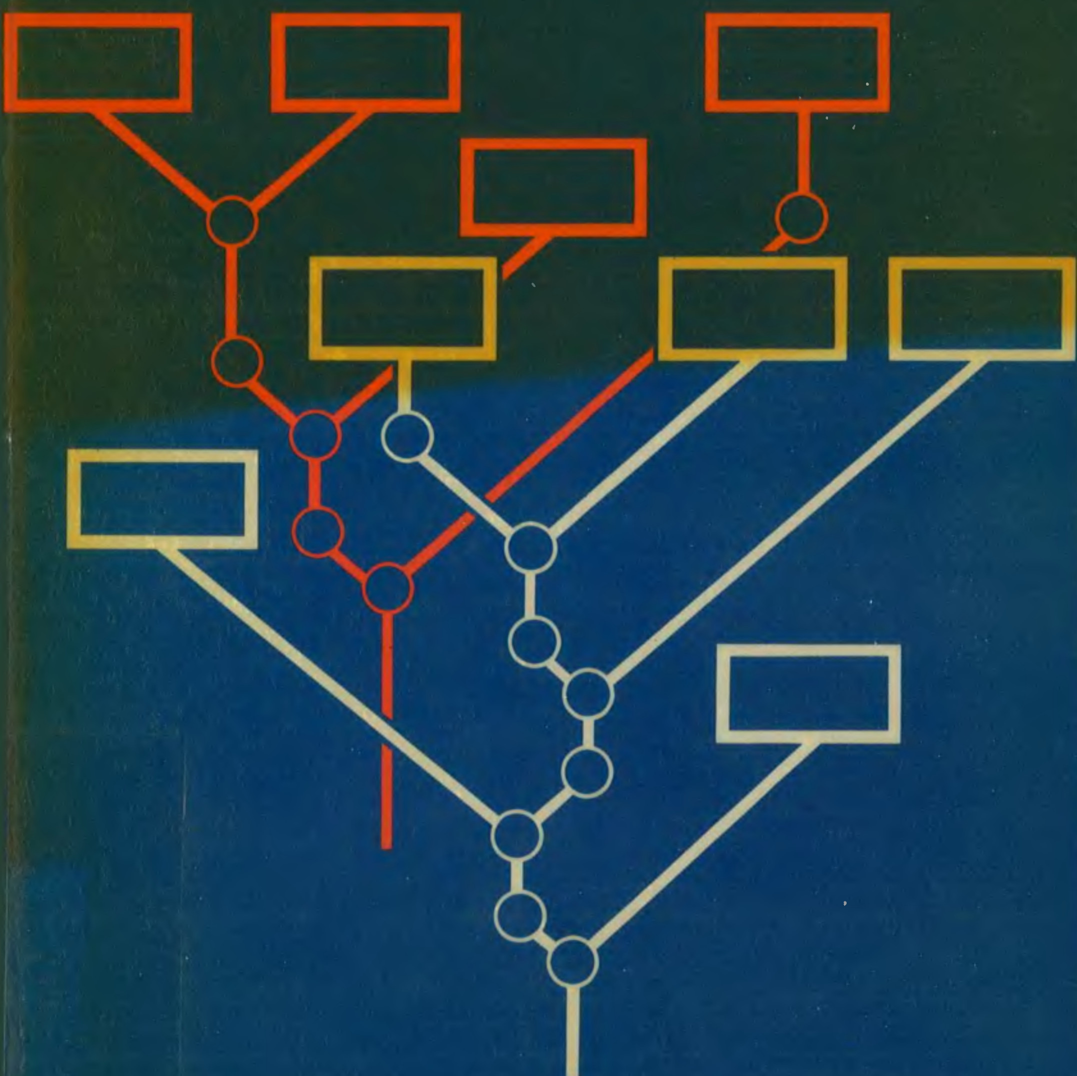
Introduction à la logique

André Delessert



Presses polytechniques romandes

Introduction à la logique

Introduction à la logique

André Delessert

Presses polytechniques romandes

La collection ***MATHÉMATIQUES***, dirigée par S.-D. Chatterji, professeur à l'Ecole polytechnique fédérale de Lausanne, propose des ouvrages qui sont nécessaires à la formation des mathématiciens et des ingénieurs théoriciens des hautes écoles. Les publications concernent aussi bien l'enseignement de base (premier cycle) que l'enseignement plus spécialisé (deuxième et troisième cycles) de mathématiques supérieures. Des publications générales touchant des aspects historiques et culturels des mathématiques sont également envisagées.

Dans la même collection:

Calcul différentiel et intégral
Jacques Douchet et Bruno Zwahlen

1 Fonctions réelles d'une variable réelle

2 Fonctions réelles de plusieurs variables réelles

3 Fonctions réelles d'une variable réelle – Exercices résolus

4 Fonctions réelles de plusieurs variables réelles – Exercices résolus (à paraître)

Analyse non standard
Alain Robert

Algèbre linéaire, tomes 1 et 2
Renzo Cairoli

Initiation aux probabilités
Sheldon M. Ross

Si vous désirez être tenu au courant des publications de l'éditeur de cet ouvrage, envoyez vos nom, prénom et adresse aux **Presses polytechniques romandes** (EPFL, Centre Midi, CH–1015 Lausanne, Suisse) qui vous enverront leur catalogue général.

Première édition
ISBN 2-88074-153-X

A Claude

Table des matières

Avertissement 5

Chapitre 0 Préambule

0.0 Origine de la logique. 7
0.1 La logique aristotélicienne 8
0.2 Le déclin de la logique aristotélicienne 10
0.3 La logique symbolique 14

Chapitre 1 Les langages du premier ordre

1.0 Définitions des langages du premier ordre 17
1.1 Commentaires généraux 26

Chapitre 2 L'idée de modèle ensembliste

2.0 Introduction 29
2.1 Conventions relatives aux ensembles 31
2.2 La notion de L-structure 34
2.3 Remarques sur les ensembles dénombrables. 45

Chapitre 3 La logique (ou calcul) des propositions
Les fonctions de vérité

3.0 Introduction 51
3.1 Définitions et propriétés élémentaires 52

Chapitre 4 Les axiomes de l'égalité ou formules de Leibniz

4.0 Conventions préalables. 65
4.1 Les axiomes de l'égalité 66

Chapitre 5 La logique des quantificateurs
La méthode de Henkin: la réduction à la logique des propositions

5.0 Introduction 69
5.1 Substitution d'un terme à une variable 70
5.2 Extension de Henkin d'un langage du premier ordre . . 73
5.3 Les axiomes de Henkin et les axiomes des quantificateurs. 74
5.4 Le lemme de réduction à la logique des propositions . . 76
5.5 Les théorèmes de compacité et de Löwenheim-Skolem 80
5.6 Appendice 83

Chapitre 6 L'idée de preuve
Le théorème de complétude de la logique du premier ordre

6.0 Introduction 89
6.1 Le système d'inférence de Hilbert 90
6.2 Quelques lemmes 93
6.3 Le théorème de complétude. 100

Chapitre 7 Extension de la logique élémentaire du premier ordre

7.0 Compléments sur les ensembles 111
7.1 Cardinal d'un langage du premier ordre 115
7.2 Théorème de Löwenheim-Skolem-Tarski 116

Chapitre 8 Quelques remarques sur la logique du premier ordre

8.0 Introduction 121
8.1 Un système formel du premier ordre pour l'arithmétique. 122
8.2 Un système formel du premier ordre pour les ensembles 131
8.3 Logique «naïve» et logique du premier ordre. Logique pratique 137
8.4 Arithmétique et logique du premier ordre. Les théorèmes d'incomplétude de Gödel (énoncés et remarques) . 141
8.5 De quelques autres théorèmes d'impossibilité 150
8.6 Le programme et la thèse de Hilbert 152

Chapitre 9 Aperçus sur d'autres logiques formelles

9.0 Introduction 157
9.1 Comment introduire simplement la finitude dans les raisonnements? 159
9.2 Logiques d'ordre supérieur 164
9.3 Sur la logique intuitionniste. 172
9.4 Sur la logique modale 175

Chapitre 10 Epilogue. 181

Exercices. 183
Index terminologique 196
Index des notations 198
Petite bibliographie 199

Avertissement

Ce modeste ouvrage a été rédigé à partir des notes d'un cours public donné à la Faculté des Sciences de l'Université de Lausanne en hiver 1982–1983. L'annonce en précisait que "les connaissances préalables requises sont celles du programme mathématique de la maturité classique", c'est-à-dire du baccalauréat littéraire. Le texte qui suit est un peu plus exigeant, en ce sens qu'il suppose une bonne pratique des notations formelles et du langage ensembliste. A partir du chapitre 7, le lecteur trouvera des développements nécessitant quelques notions supplémentaires – d'ailleurs simples – sur les ensembles, les groupes et les nombres réels. Ils ne sont pas indispensables à la compréhension du reste de l'ouvrage.

L'exposé combine des démonstrations de type mathématique, des commentaires ouvrant des perspectives plus larges sur la logique en général, des indications historiques et quelques exercices placés en fin de volume. Il ne prétend aucunement à l'originalité. Ainsi, le théorème de complétude de Gödel est-il établi en suivant de près le canevas donné par Jon Barwise dans le chapitre "An Introduction to First-Order-Logic" du Handbook of Mathematical Logic (Studies in Logic, vol. 90). Le présent ouvrage a pour seul propos de mettre à la disposition du profane des faits de logique à la fois élémentaires, non banals et peu accessibles dans l'édition en langue française.

L'établissement du texte est dû pour l'essentiel à MM. Jacques Perrinjaquet et Gérard Schibler, assistants à la Faculté des Sciences de Lausanne. Ils ont grandement amélioré sa présentation et comblé des lacunes sensibles dans certaines démonstrations. M. Perrinjaquet a en outre établi les index et corrigé le manuscrit. Je tiens à exprimer à ces deux précieux collaborateurs ma très vive reconnaissance.

Je dois encore dire l'obligation que j'ai au professeur Jean-Jacques Loeffel, président de la Commission d'histoire et de méthode des sciences de la Faculté des Sciences de l'Université de Lausanne, qui a suscité à la fois le cours public et la publication de cet ouvrage. Mes remerciements vont aussi à Madame Suzanne Assal qui a dactylographié le manuscrit avec infiniment de patience et de dévouement.

La réalisation de cet ouvrage a été rendue possible par l'aide matérielle de la Faculté des Sciences, du Fonds Landry, de la Fondation Herbette, de la Fondation Chuard-Schmidt et par la précieuse collaboration des Presses Polytechniques Romandes. A tous mes collègues, j'exprime ma très sincère gratitude.

Conventions

L'ouvrage est découpé en chapitres numérotés par un nombre arabe à partir de 0. Chaque chapitre est divisé en paragraphes; chacun d'eux est repéré par deux nombres arabes séparés par un point. 5.0 désigne le paragraphe 0 du chapitre 5, par exemple. A l'intérieur d'un paragraphe, les définitions, les propositions, les remarques, etc. sont repérées par trois nombres arabes séparés par des points. Cas échéant, les subdivisions d'une remarque, d'un exemple sont repérées par quatre nombres arabes séparés par des points.

Les équations ou formules hors texte sont numérotées par ordre dans leur chapitre. (6.4) désigne la formule numéro 4 dans le chapitre 6. Une numérotation analogue est utilisée pour les figures. Le terme ou la locution introduits spécifiquement par une définition ou une remarque y apparaissent en *italique maigre*. Un passage ou un mot important sont composés en ***italique gras.***

La fin des démonstrations est marquée par le signe □. Les passages ou paragraphes exigeant des connaissances mathématiques plus avancées ou d'une lecture plus difficile sont précédés et suivis du signe ■. Ils peuvent être laissés de côté dans une première lecture.

Servion, juin 1987.

CHAPITRE 0

Préambule

0.0 ORIGINE DE LA LOGIQUE

Le mot "logique" vient du grec *logos* qui signifie parole, verbe.

Il nous est difficile aujourd'hui de prendre conscience du pouvoir mystérieux que peut détenir la parole. Nous vivons une période d'inflation verbale. L'éther est traversé en permanence par des milliers de discours que nous sommes appelés à capter, à enregistrer et à reproduire. La presse déverse quotidiennement une logorrhée irrépressible. Les mots sombrent dans l'insignifiance. Il faut constamment en augmenter la ration journalière, à moins de recourir à des néologismes audacieux et à des expressions choquantes pour exciter artificiellement notre écoute.

Toutefois, nous pouvons observer qu'à l'occasion l'éloquence d'un avocat ou d'un homme politique peut retourner une situation. Il nous arrive d'éprouver les méfaits d'un ragot ou d'un compte rendu tendancieux. L'intrigue de certaines pièces de théâtre repose essentiellement sur la présence d'un individu – Scapin ou Iago – qui manipule les autres personnages par ses seuls discours. Le phénomène est encore plus net dans la fable du Corbeau et du Renard. La plupart des civilisations anciennes et certaines civilisations actuelles scellent les actes importants de la vie par des contrats oraux. Aujourd'hui encore, chez nous, le mariage requiert la prononciation d'un oui sacramentel. Certains individus anachroniques persistent à se sentir engagés par leur parole d'honneur.

Nous constatons que la parole peut être action directe. Mais elle est souvent chargée d'un pouvoir en quelque sorte magique. Passons sur les innombrables bénédictions et malédictions qui jalonnent l'Histoire. Nous n'évoquerons par non plus tous les enfants qui ont abîmé leurs genoux et leurs habits du dimanche juste ***après*** que leurs parents leur ont dit qu'ils allaient tomber. En revanche, nous noterons que certaines argumentations portent pour des raisons qui n'ont rien de raisonnable. Ainsi, à l'occasion d'une votation populaire, les partisans des chasseurs l'emportèrent-ils en partie grâce à l'argument selon lequel Hitler détestait la chasse. Il s'agit d'un amalgame purement verbal mais non dénué d'efficacité. Certaines analogies, purement verbales elles aussi, peuvent susciter tantôt des inventions intéressantes, tantôt d'étranges élucubrations. Cela se présente lorsqu'on compare l'esprit humain à un grenier qu'il faut meubler ou l'école à une fabrique. L'exploitation de ce genre de rapprochement s'apparente à la médecine sympathique qui soigne un mal à l'aide d'un objet qui présente avec lui certaines similitudes. Par exemple, on traitait jadis la jaunisse en faisant boire du vin où avaient macéré des pièces d'or. Nous ne sommes d'ailleurs pas tous exempts d'une espèce de crainte à l'égard du pouvoir magique de la parole. Imaginons qu'un ami nous dérange par téléphone à une heure indue et que nous nous exclamions par-devers nous: "Que ne se casse-t-il plutôt une jambe!" Si nous apprenons le lendemain qu'il s'est effectivement cassé la jambe, nous nous empresserons d'aller le trouver sur son lit de souffrance avec trois romans policiers et un kilo et demi de chocolat, soit environ trois fois plus qu'il ne serait rigoureusement nécessaire.

Il est dès lors facile de comprendre que diverses civilisations, en particulier celles dont nous descendons, aient adopté une cosmologie, des mythes d'origine faisant intervenir une Parole, un logos. "Au commencement le Verbe était et le Verbe était avec Dieu et le Verbe était Dieu" lit-on au début de l'Evangile selon Saint Jean.

Selon cette conception, on se représente le monde comme un mécanisme régi par des lois qu'un démiurge a édictées dans une langue sacrée – sanscrit, grec, hébreux, arabe, ... – connues de certains hommes. La cohérence du monde est garantie par celle de la parole. La création est donc intelligible. Cette représentation était largement répandue dans l'Antiquité. Elle apparaît explicitement chez Zénon d'Elée (V^e siècle av. J.-C.) et les Upanishads en prose (500–800 av. J.-C.). Elle n'est d'ailleurs pas entièrement étrangère aux esprits apparemment les moins attachés aux antiques superstitions puisque, aujourd'hui encore, on parle couramment des "lois scientifiques" et du "grand livre de la nature".

0.1 LA LOGIQUE ARISTOTÉLICIENNE

La logique ancienne a atteint un sommet avec Aristote. Les règles péripatéticiennes ont été reprises et développées par les auteurs grecs, latins, juifs, arabes et par les scolastiques. Le terme même de "logique" ne s'est définitivement imposé qu'au Moyen Age. Aristote n'a pas consacré expressément d'ouvrage à la seule logique. Il en a exposé les diverses parties dans l'ensemble de traités groupés sous le nom d'Organon (instrument) ainsi que dans d'autres livres tels que la Métaphysique ou la Politique. En effet, il ne la considère pas comme une discipline parmi d'autres; la logique est pour lui "la science des sciences".

Pour en présenter le mécanisme, nous ferons appel à une terminologie qui n'a été explicitée que plus tardivement. Traditionnellement, un *concept* résulte d'une série de jugements portant sur des *individus*. Par exemple, le concept Homme s'obtient en soumettant une certaine collection d'objets individuels à une grille de tests: respire-t-il? combien a-t-il de membres? peut-il rire? est-il mortel? ... L'ensemble des réponses obtenues constitue une donnée verbale appelée *compréhension* du concept Homme. L'*extension* de ce concept est la collection de tous les objets individuels – ici les hommes – satisfaisant les critères inscrits dans sa compréhension. La compréhension et l'extension d'un concept sont étroitement liées. Chacune d'elles détermine l'autre. Lorsque l'une croît, l'autre décroît. Il faut plus de propriétés pour caractériser le concept Jardinier que le concept Homme. En revanche, seuls certains hommes sont jardiniers.

Les individus et les concepts entretiennent un vaste réseau de relations d'appartenance ou d'inclusion. L'individu Socrate appartient à l'extension du concept Homme et toutes les données de la compréhension du concept Homme conviennent à Socrate, ce que l'on traduit par "Socrate est un homme". De même le concept Saule est subordonné au concept Arbre en ce sens que l'extension du premier est incluse dans celle du second et que les caractères de l'arbre s'appliquent tous au concept Saule. Et cela se dit: "tout saule est un arbre". Un assertion telle que "ce poisson est rouge" exprime que ce poisson individuel appartient à l'extension de Chose rouge. La Logique aristotélicienne exploite l'organigramme des individus et des concepts et elle produit des raisonnements tels que le syllogisme bien connu:

tout homme est mortel
Socrate est un homme
Donc Socrate est mortel.

Ce qui précède appelle trois remarques.

D'abord, les choses qui nous entourent paraissent se ranger spontanément dans les extensions de concepts bien distincts. Ce n'est pas étonnant pour les objets fabriqués par l'homme. Mais on le constate aussi pour les objets naturels. Il y a beaucoup de pommiers et beaucoup de saules. Mais il n'existe pas de famille continue d'arbres passant par variations insensibles du pommier au saule. A nos yeux, le monde se révèle conforme à un organigramme d'individus et de concepts. Par là, il nous semble intelligible et la logique aristotélicienne se présente comme l'outil de base pour l'appréhender.

On constate ensuite que, pour produire ou comprendre le syllogisme de Socrate, il est inutile de connaître le sens exact des mots employés pour désigner les individus et les concepts. Seule importe sa forme:

tout a est un b
c est un a
Donc c est un b.

D'où le nom de *logique formelle* donné généralement à la logique d'Aristote.

Enfin, les règles gouvernant l'appartenance et l'inclusion sont très simples et peu nombreuses. D'où l'opinion assez répandue selon laquelle la logique est une science banale, bonne pour les esprits bornés et dénués d'imagination. Ce n'est que dans les situations artificiellement compliquées qu'il convient d'y recourir, pour déchiffrer une loi ou un règlement, par exemple.

0.2 LE DÉCLIN DE LA LOGIQUE ARISTOTÉLICIENNE

La logique d'Aristote a été inlassablement reprise au long des siècles. D'innombrables philosophes y ont apporté des commentaires profonds ou non. D'infinies subtilités ont été développées. Mais les principes essentiels n'ont guère varié. De nos jours encore, les connaissances des profanes en matière de logique relèvent quasiment toutes de la Logique aristotélicienne. Toutefois, au cours des derniers siècles et particulièrement aux XIXe et XXe siècles, la logique classique a fait l'objet de critiques assez graves. Les logiciens, certains philosophes et divers mathématiciens – gros utilisateurs de logique – ont mis en évidence certaines insuffisances de la logique aristotélicienne. On peut parler d'un véritable déclin de cette discipline. Nous allons essayer d'évoquer trois causes, parmi d'autres, de cette désaffection.

Pour suggérer la première, nous partirons d'une remarque inspirée par le logicien John Stuart-Mill (1806–1873). Reprenons le syllogisme de Socrate. En vertu de la deuxième prémisse, celui qui affirme que "tous les hommes sont mortels" doit s'assurer au préalable que le qualificatif "mortel" s'applique effectivement à chacun des hommes au nombre desquels figure Socrate. Avec beaucoup d'indulgence, on est conduit à admettre que la conclusion n'enseigne rien qu'on ne sache au préalable. Un peu plus de sévérité incite à penser que ce syllogisme est un cercle vicieux puisque la première prémisse suppose vraie la conclusion.

Au lieu d'épiloguer sur cette remarque, essayons de comprendre comment il se fait que les Anciens n'aient pas constaté que ce raisonnement apparemment exemplaire était une opération stérile, voire une pétition de principe. Notons que la remarque de Stuart-Mill ne prend en compte que l'extension des concepts en cause. Tandis qu'Aristote joue alternativement sur la compréhension et l'extension. "Socrate est un homme" est un constat portant sur l'extension du concept Homme. Il n'en est pas de même pour "tout homme est mortel". Pour Aristote, c'est un décret divin. Le caractère "mortel" appartient par principe à la compréhension du concept Homme. Comment pourrait-on vérifier effectivement que tout homme vivant est mortel? La conclusion "Socrate est mortel" est dès lors un "jugement" au sens strict du mot. C'est une création, comme peut l'être une sentence de tribunal.

Aristote exploite la conformité de la parole au monde et il explicite les exigences du logos. En revanche, au XIXe siècle, on admet que la parole humaine obéit à des règles internes sans liens nécessaires avec un Verbe créateur. Le syllogisme ne nous apprend rien sur le monde. Il se contente d'assurer la cohérence de la langue et il nous permet de vérifier que les mots gardent le même sens au long du discours. Entre Aristote et Stuart-Mill un retournement philosophique majeur s'est produit qui appelle un renouvellement de la logique.

La deuxième cause que nous mentionnerons pour expliquer le déclin de la logique aristotélicienne est étroitement liée à l'évolution des mathématiques. Nous avons noté que la logique classique ne considère que deux relations: l'appartenance et l'inclusion. Ce sont des relations binaires puisqu'elles portent sur deux termes:

a est un élément de B, C est inclus dans D. Ces relations sont prises en compte par le langage des ensembles: $a \in B$, $C \subset D$. Mais les mathématiciens ont imaginé et utilisé bien d'autres relations. Par exemple:

• des relations unaires:	16 est un nombre pair
	sinus est une fonction périodique
• des relations binaires:	a égale b
	a est parallèle à b
	a est perpendiculaire à b
	x divise y
• des relations ternaires:	x est la somme de y et z
	a, b et c passent par un même point

etc, etc...

Les propriétés de ces relations s'écartent sensiblement de celles de l'appartenance et de l'inclusion. Il a fallu imaginer une logique capable en permanence de prendre en compte de nouvelles relations.

Mais il y a plus. La logique d'Aristote, bien que d'essence métaphysique, était destinée à donner prise sur l'univers accessible à l'homme. C'était une logique de la finitude, l'infini restant un attribut de la divinité situé au-delà de notre intelligence et ne se manifestant à nous que sous une forme virtuelle. L'infini était proprement in-fini, autrement dit indéfini et, partant, inutilisable. Dans le domaine du fini, il est naturel d'adopter, par exemple, le principe selon lequel "le tout est, sous tous les rapports, plus grand que la partie". Mais les géomètres grecs – à leur insu sans doute –, Archimède, puis les créateurs du calcul infinitésimal se sont graduellement accoutumés à employer ***effectivement*** des collections infinies.

Donnons un exemple de ce qu'on entend par là. Considérons les deux nombres décimaux:

$$a = 9{,}9999 \ldots 999 \ldots$$
$$b = 99{,}9999 \ldots 999 \ldots$$

où la décimale 9 se répète indéfiniment. Visiblement, b égale a augmenté de 90. Mais c'est aussi le nombre 10 fois plus grand que a, obtenu en décalant la virgule d'un rang vers la droite dans l'expression décimale de a. Donc $a+90=10\,a$, et a égale 10. Ce raisonnement ne vaut qu'à condition de prendre effectivement en compte l'infinité des décimales de a.

Les mathématiciens ont dû apprendre à éviter les apparences trompeuses et introduire de nouvelles règles logiques permettant de maîtriser certaines collections infinies. Ainsi est née, par exemple, l'induction complète ou démonstration par récurrence. En contrepartie, il a fallu renoncer à certains principes, tels que celui du "tout et de la partie". Ainsi, en décalant la virgule d'un rang vers la droite, on a ôté réellement un 9 de la suite des décimales de a; mais cette suite n'a pas changé pour autant.

La troisième cause qui a mobilisé les contempteurs de la logique d'Aristote est liée à l'existence des paradoxes et des antinomies.

La conception du monde où s'enracine la logique aristotélicienne conduit à admettre que la justesse d'un raisonnement est garantie par l'usage correct de la langue. C'est une pensée simple et naturelle à laquelle il semble facile de souscrire. Elle explique sans doute, au moins en partie, la pérennité de la logique classique. Très tôt cependant, quelques doutes se sont manifestés sur la cohérence de la langue elle-même. Les sophistes grecs produisaient déjà des "raisonnements" tels que celui-ci:

Connais-tu l'homme qui s'avance au loin?
Non!
Cet homme est ton père. Donc tu ne connais pas ton père!

L'impertinence de la conclusion repose sur l'ambiguïté du verbe "connaître". Un autre paradoxe, celui du Menteur, était connu d'Aristote et a retenu l'attention jusqu'au Moyen Age:

Epiménide, le Crétois, dit: "Tous les Crétois sont menteurs"
Epiménide, étant Crétois, ment.
Donc, les Crétois ne mentent pas, et Epiménide non plus.
Donc, tous les Crétois sont menteurs, ...

Remarquons en passant qu'il est facile de sortir de ce cercle vicieux. Il suffit d'observer que la négation de "Tous les Crétois sont menteurs" est: "Il existe un Crétois qui n'est pas menteur". On peut alors conclure que ce n'est certainement pas Epiménide, mais guère plus.

On trouve encore dans certains ouvrages de logique des "syllogismes" tels que celui-ci:

J'ai mis mes lunettes dans mon étui.
Mon étui est dans l'armoire.
Donc mes lunettes sont dans l'armoire.

qui passe pour un modèle à suivre. Formellement, il est du type:

J'ai mis A dans B
B est dans C
Donc A est dans C.

On constate alors qu'on s'est laissé prendre à un piège lorsqu'on remplace A par "ma confiance", B par "mon neveu Paul" et C par "la lune". Pour rectifier le "raisonnement" précédent, il faudrait écrire:

Quels que soient A, B et C, si j'ai mis A dans B et si B est dans C, alors A est dans C.
Or j'ai mis A dans B et B dans C.
Donc A est dans C.

Mais alors la première assertion est fausse si on prend en compte tout le champ sémantique – c'est-à-dire toute l'étendue du sens – du mot "dans".

L'exemple qui précède nous montre que des assertions qui sont banales dans le domaine matériel deviennent sujettes à caution quand on les transporte à des objets de pensée. Or les fonctions elliptiques, l'entropie, la propriété intellectuelle ou le produit national brut sont des objets de pensée et on peut désirer appliquer la logique aux mathématiques, à la physique, au droit ou aux sciences économiques. Il semble donc difficile de raisonner à l'aide d'une langue naturelle sans faire intervenir le contenu sémantique des termes employés.

Mais d'autres antinomies révèlent que le danger est encore plus profond. Le paradoxe d'Epiménide peut être présenté sous des formes plus frappantes: "Je mens actuellement", "La présente affirmation est fausse", "Il est défendu de lire la présente interdiction". Ces assertions nous enferment dans des contradictions dont il est plus difficile de sortir que de celle du paradoxe du Menteur. Elles nous montrent qu'il est possible de former des propositions fortement suspectes, bien qu'elles soient grammaticalement correctes et que le sens exact de chaque terme y soit connu. Les trois phrases mentionnées ont en commun la propriété d'être "auto-référentielles". Il faudrait les avoir lues entièrement avant de les lire!

Cette référence d'un discours à lui-même peut être créatrice comme on peut l'observer dans l'exemple d'un dictionnaire de la langue française écrit en français. Mais elle peut aussi engendrer des absurdités et elle est parfois difficile à déceler. Ainsi, on peut confectionner des catalogues de tout ce qu'on veut et particulièrement des catalogues de catalogues. Est-il possible d'établir le catalogue des catalogues qui ne se mentionnent pas eux-mêmes? Doit-il se mentionner lui-même? Grelling a proposé une antinomie assez agaçante. Il suggère de qualifier d'"hétérologue" tout adjectif qui ne s'applique pas à lui-même. Par exemple, "long" est hétérologue, mais "polysyllabique" ne l'est pas. "Hétérologue" est-il hétérologue? Si oui, il ne l'est pas car il ne s'applique pas à lui-même. Si non, il ne s'applique pas à lui-même et, par suite, il est hétérologue.

Une autre antinomie, empruntée à Berry, soulève des difficultés du même ordre, bien que sous une forme plus cachée. Prenons un bon dictionnaire français. L'ensemble des mots, éventuellement conjugués ou déclinés, qu'il comporte est grand mais fini. La collection des suites de vingt mots qu'on peut extraire de ce dictionnaire est donc elle aussi finie. Il existe par suite un nombre naturel (et même une infinité de nombres naturels) qu'on ne peut pas caractériser en moins de vingt mots pris dans ce dictionnaire. "Le plus petit nombre naturel qu'on ne peut pas caractériser en moins de vingt mots de ce dictionnaire" est justement caractérisé en moins de vingt mots qui figurent certainement dans le dictionnaire considéré.

Bien d'autres antinomies ont été imaginées. Elles ont provoqué une abondante littérature de valeur inégale. Pourtant certaines d'entre elles lancent de graves défis à la logique classique. Elles montrent en tous cas qu'une langue naturelle – le grec, le français, etc. – n'est pas en mesure de nous mettre formellement à l'abri de graves accidents sémantiques. Il devient dès lors difficile d'admettre que l'ordre du monde puisse être garanti par la parole. Notons en passant qu'en proscrivant les sophistes, les philosophes classiques grecs ont peut-être enfermé pour longtemps la pensée occidentale dans un carcan.

0.3 LA LOGIQUE SYMBOLIQUE

L'évolution des conceptions philosophiques, les besoins des mathématiques et les antinomies ont remis en cause les acquisitions de la logique classique. Le logicien Bertrand Russell, auteur avec Whitehead des *Principia Mathematica* (3 volumes, 1910–1913) ne déclara-t-il pas: "La logique d'Aristote n'est rien d'autre qu'un charlatanisme solennel" et "quiconque désire de nos jours apprendre la logique perd son temps s'il lit Aristote ou l'un quelconque de ses disciples"? On conçoit dès lors que les logiciens aient formé le projet de décrire une logique véritablement formelle qui permette de circonscrire le rôle de l'intuition. Ce plan ne s'est pas réalisé en un jour. Il a fallu concevoir des langages artificiels, obéissant à des règles simples, peu nombreuses, vérifiables mécaniquement et qui bannissent les expressions auto-référentielles. Le symbolisme mathématique a servi de patron. Une idée aussi vieille que Pythagore, reprise à leur compte par Raymond Lulle (1235–1315) et surtout par Leibniz (1646–1716) a conduit à considérer la logique comme une sorte d'algèbre. Mais les règles de ce genre de calcul n'ont été dégagées que peu à peu. Les travaux de A. de Morgan (1806–1871) et de G. Boole (1815–1864) y ont beaucoup contribué. Enfin, G. Peano (1858–1932), G. Frege (1848–1925), Russell (1872–1970) et Whitehead (1861–1947) sont parvenus à décrire des langages formels dignes de ce nom. Ainsi est née la logique *symbolique,* dite aussi *théorique* ou *mathématique*. Elle est capable de former une multitude de systèmes logiques dont certains conviennent admirablement aux mathématiques et d'autres se prêtent avec assez de bonheur à l'analyse des discours philosophiques, éthiques ou déontologiques, par exemple.

Considérée globalement, la logique ne se réduit pas à la logique symbolique. Elle pose à la philosophie des problèmes majeurs. Elle est étroitement liée à la théorie de la connaissance et, en particulier, à l'épistémologie générale et à la méthodologie des sciences. Il est indiqué de l'étendre à une théorie plus vaste de l'argumentation et de l'intégrer à la linguistique. On peut l'aborder sous l'angle de la psychologie ou de l'histoire des idées. Mais il est difficile aujourd'hui de parler raisonnablement de logique sans connaître quelques faits touchant la logique théorique. Certains penseurs, qui s'y sont essayés, se sont exposés ainsi à de graves critiques. Ils auraient pu les éviter par la connaissance de quelques résultats importants, mais élémentaires, de logique théorique.

Nous nous proposons ici de présenter une partie de la logique symbolique qu'on appelle logique *du premier ordre*. Nous établirons essentiellement un résultat non banal: le théorème de complétude de Gödel. Ce fait, que l'on peut découvrir par des moyens somme toute assez élémentaires, montre que la logique du premier ordre est justement celle qui permet de formaliser les mathématiques classiques. Mais nous verrons aussi qu'il projette un éclairage surprenant sur des notions apparemment familières comme le fini et l'infini. Nous ne serions pas étonnés si ces considérations suscitaient chez le lecteur des réflexions enrichissantes. Nous terminerons ce modeste exposé par quelques indications sur d'autres systèmes logiques qui permettent d'imaginer des domaines non mathématiques où la logique théorique ouvre des perspectives intéressantes.

Ce texte est conçu pour un lecteur qui ne dispose que de notions mathématiques très rudimentaires: une certaine familiarité avec le calcul littéral, les notations et le langage des ensembles. A celui qui connaît un peu plus d'algèbre, d'analyse et de théorie des ensembles, des paragraphes ou des alinéas placés entre deux signes ■ apportent quelques compléments que nous croyons intéressants. Ces passages ne sont pas indispensables pour comprendre l'objet principal de cet exposé.

CHAPITRE 1

Les langages du premier ordre

1.0 DÉFINITIONS DES LANGAGES DU PREMIER ORDRE

1.0.0 Préambule

Dans ce chapitre, nous allons présenter la notion de langage (formel) du premier ordre. Il s'agit d'une étape essentiellement descriptive, où il y a "tout à raconter et rien à comprendre".

Un langage du premier ordre est essentiellement la donnée:

- de *symboles*;
- de *règles de formation* qui, à partir des symboles, permettent d'écrire les *formules* du langage considéré.

1.0.1 Définition

Les *symboles d'un langage du premier ordre L* sont donnés par les collections suivantes:

- une collection de huit *symboles logiques*, à savoir:
  six connecteurs
  $\neg \quad \wedge \quad \vee \quad = \quad \rightarrow \quad \leftrightarrow$
  qu'on lit respectivement
  "non" "et" "ou" "égale" "implique" "est équivalent à"
  deux *quantificateurs*
  $\forall \quad \exists$
  lus respectivement
  "pour tout" (ou "quel que soit") et "il existe";
- une collection de trois *symboles de ponctuation*:
  ( ) ,
  soit le début de parenthèse, la fin de parenthèse et la virgule, respectivement;
- une collection de *symboles de variables*, notée Var:
  $x \quad x' \quad x'' \quad x''' \ldots;$
- une collection de *symboles de constantes*, notée Cst(L):
  $c \quad c' \quad c'' \quad c''' \ldots;$

- une collection de *symboles de fonctions*, notée Fct(L):
  $f_n \quad f'_{n'} \quad f''_{n''} \quad f'''_{n'''} \quad \ldots$
  où n, n', n'', n''', ... sont des entiers naturels strictement positifs;
- une collection de *symboles de relations*, notée Rel(L):
  $R_m \quad R'_{m'} \quad R''_{m''} \quad R'''_{m'''} \ldots$
  où m, m', m'', m''', ... sont des entiers naturels strictement positifs.

1.0.2 Remarque

Tous ces symboles sont *a priori* dénués de sens. Il faut les considérer comme des lettres d'un alphabet inconnu. La seule chose qui importe est qu'une machine puisse les distinguer et reconnaître s'ils sont des symboles de variables, ou de fonctions, etc.

1.0.3 Remarque

Certains de ces symboles sont empruntés à l'algèbre élémentaire. Il conviendra de distinguer entre l'utilisation ordinaire de ces signes et leur emploi dans un langage formel.

1.0.4 Remarque

Les symboles logiques, les symboles de ponctuation et de variables appartiennent à tous les langages du premier ordre. Ce sont donc les collections Cst(L), Fct(L) et Rel(L) qui caractérisent le langage L. Pratiquement, elles ne comportent que peu d'éléments. Il arrive que l'une ou l'autre d'entre elles soit vide.

1.0.5 Remarque

Les symboles de fonctions sont numérotés par des "accents": , $'$, $''$, ... L'indice inférieur indique un "nombre de places" ou, si l'on préfère, un nombre d'arguments. $f'_{n'}$ est un symbole de fonction unaire, binaire, ternaire, ... , p-aire suivant que n' égale 1, 2, 3, ... p, respectivement.

Une convention analogue vaut pour les symboles de relations.

1.0.6 Définition

Nous avons comparé les symboles d'un langage du premier ordre L à un alphabet. Nous allons donner des règles permettant de construire ce qu'on pourrait considérer comme des substantifs.

Supposons donnés les symboles d'un langage du premier ordre L. La collection des *termes* de L, notée Ter(L), est déterminée par les règles suivantes:

- tout symbole de variable ou de constante est un terme;
- si f_n est un symbole de fonction n-aire et si $t_1, t_2, \ldots, t_n$ désignent des termes (distincts ou non), $f_n(t_1, t_2, \ldots, t_n)$ est un terme;
- il n'y a pas d'autres termes que ceux qu'on obtient à l'aide des règles précédentes.

1.0.7 Remarque

Tout terme est un agrégat de symboles de L, comme par exemple $f_2(x, x')$. Dans la définition 1.0.6, $t_1, t_2, \ldots$ ne sont pas des symboles de L, mais des signes typographiques pour désigner de tels agrégats.

Si les termes peuvent être regardés comme des substantifs, les règles suivantes vont permettre de construire ce qu'on peut comparer à des phrases.

1.0.8 Définition

Supposons donnés les symboles d'un langage du premier ordre L.

Les *formules atomiques* de L sont données par les règles suivantes:

- si t_1 et t_2 désignent des termes de L, $(t_1 = t_2)$ est une formule atomique de L;
- si R_n est un symbole de relation n-aire de L et si $t_1, t_2, \ldots, t_n$ désignent des termes (distincts ou non) de L, $R(t_1, t_2, \ldots, t_n)$ est une formule atomique de L.

La collection des *formules* de L, notée For(L), est déterminée par les règles suivantes:

- toute formule atomique de L est une formule de L;
- si φ et ψ désignent des formules de L,
  $(\neg\varphi)$ $(\varphi \wedge \psi)$ $(\varphi \vee \psi)$ $(\varphi \rightarrow \psi)$ $(\varphi \leftrightarrow \psi)$
  sont des formules de L;
- si φ désigne une formule de L et si y désigne un symbole de variable, $(\forall y \varphi)$ et $(\exists y \varphi)$ sont des formules de L;
- il n'y a pas d'autres formules de L que celles qu'on obtient à l'aide des règles précédentes.

La formule $(\varphi \rightarrow \psi)$ se lit "φ implique ψ" ou parfois encore "si φ, alors ψ".

1.0.9 Exemple

Considérons le langage du premier ordre L_1 ne comportant qu'un symbole de constante, c, qu'un symbole de fonction binaire, f_2, et qu'un symbole de relation unaire, R_1. Autrement dit:

$$\mathrm{Cst}(L_1) = \{c\} \quad \mathrm{Fct}(L_1) = \{f_2\} \quad \mathrm{Rel}(L_1) = \{R_1\}$$

(Les notations ensemblistes utilisées ici seront rappelées au début du chapitre 2.)

Alors:

- x; x'; x''; ... ; c; $f_2(x, c)$; $f_2(x, x')$; $f_2(x, x)$; $f_2(c, f_2(x, x''))$; $f_2(f_2(x, c), f_2(f_2(x, x), x))$; ...
  sont des termes de L_1.
- $(x=x)$; $(x=c)$; $(f_2(x, c)=c)$; $R_1(c)$; $R_1(f_2(x, c))$; ...
  sont des formules atomiques de L_1.
- $(x=x)$; $(f_2(x, x)=c)$; $(\neg(x=c))$; $((f_2(c, x)=x')\leftrightarrow(x=x'))$; $(R_1(x)\wedge(\neg R_1(x')))$; $(\exists x''((f_2(x'', c)=c)\vee(f_2(c, x'')=c)))$; $((\forall x((f_2(x, c)=x)\wedge(f_2(c, x)=x)))\wedge(\exists x(\neg(R_1(x)))))$; ...
  sont des formules de L_1.

1.0.10 Contre-exemples

Dans le même langage L_1, les agrégats de symboles suivants ne sont pas des formules:

$x' = f_2)xc$; $c=(x, c)$; $(\neg(\forall x((x=c)$; $(f_2(x, x)=c)))$;
$(R_1(x))$; $(\exists f_2(f_2(x, x)=c))$; ...

1.0.11 Remarque

Dans les définitions 1.0.6 et 1.0.8, il est sous-entendu que les agrégats de symboles – termes ou formules – sont écrits en ligne, de la gauche vers la droite. On suppose que le lecteur est familiarisé avec les principes de l'écriture ordinaire. Il serait d'ailleurs difficile de les décrire, sans cercle vicieux, dans un livre ordinaire!

1.0.12 Remarques

Les termes de L sont construits de proche en proche – on dit: *par récurrence* – à partir des symboles de constantes, de variables et de fonctions. De leur côté, les formules de L sont aussi construites par récurrence à partir des formules atomiques. Nous serons amenés à utiliser ces deux récurrences pour prouver certaines propriétés des termes et des formules.

1.0.13 Remarque

Le fait qu'un langage formel est du premier ordre tient à la fois à la collection de ces symboles et aux règles de formation des formules. Au chapitre 9, nous évoquerons des langages comportant des symboles étrangers à la logique du premier ordre. D'autre part, dans un langage du premier ordre, tout symbole de variable est un terme et les quantificateurs précèdent nécessairement un symbole de variable.

1.0.14 Remarque

Pour tout langage du premier ordre L, on pourrait se borner à l'étude des formules qui ne contiennent pas le symbole logique $=$. Cela constituerait la "logique du premier ordre sans égalité", ce que certains appellent parfois la "logique du premier ordre des prédicats". Bien entendu, il faut que $\mathrm{Rel}(L)$ soit non-vide, faute de quoi $\mathrm{For}(L)$ serait elle-même vide.

Réciproquement, à partir d'un langage du premier ordre sans égalité, on peut reconstituer un langage du premier ordre en introduisant un nouveau symbole de relation binaire noté $=$. On verrait alors apparaître des formules de la forme $=(t_1, t_2)$ au lieu de $(t_1 = t_2)$.

1.0.15 Remarque

Dans le langage du premier ordre L_1 introduit à l'occasion des exemples précédant ces remarques, considérons la formule:

$$((\forall x((f_2(x, c) = x) \wedge R_1(x))) \rightarrow (\exists x'(\neg(f_2(x', x') = c)))) \tag{1.0}$$

Il est facile d'y repérer les constituantes atomiques: il y en a exactement une par symbole $=$ et une par symbole de relation. Disposons-les sur une ligne horizontale dans l'ordre où elles apparaissent dans la formule considérée. Les formules non atomiques construites à partir d'elles s'obtiennent de proche en proche selon deux sortes de règles: dans l'une figure l'emploi du connecteur $\neg$ et des deux quantificateurs; l'ancienne et la nouvelle formules sont alors reliées par une arête verticale descendante; dans l'autre, on range l'emploi des connecteurs $\wedge$, $\vee$, $\rightarrow$ et $\leftrightarrow$; deux anciennes formules sont reliées chacune par une arête descendante oblique à une nouvelle formule. On voit apparaître un ensemble de sommets et d'arêtes d'un seul tenant et sans circuit, autrement dit un arbre. C'est l'*arbre de formation* de la formule (1.0):

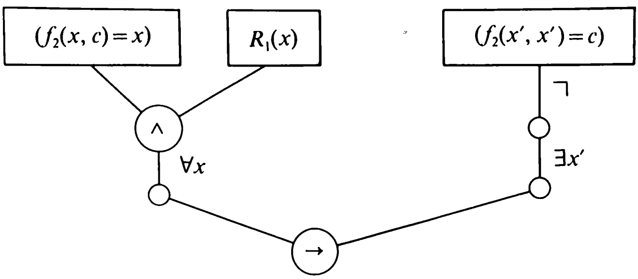


Fig. 1.0

A chaque sommet correspond une formule. L'emplacement des arêtes dans l'arbre est déterminé par celui des parenthèses dans la formule considérée.

Pour être complet, l'arbre de formation de la formule étudiée doit en outre comporter trois genres d'indications:

- aux extrémités libres supérieures, les formules atomiques dans l'ordre où elles apparaissent dans la formule étudiée;
- aux sommets où aboutissent deux arêtes descendantes obliques, les connecteurs respectivement utilisés;
- sur les arêtes verticales, le connecteur $\neg$ ou le quantificateur convenable accompagné de son symbole de variable, suivant le cas.

La donnée d'un arbre de formation permet évidemment de trouver la formule finale; on peut présumer que, réciproquement, la donnée de la formule détermine son arbre de formation, abstraction faite de la longueur des arêtes et de la direction des arêtes obliques descendantes. C'est bien le cas et nous allons le montrer.

1.0.16 Lemme

Soit L un langage du premier ordre.

Soit T un terme de L comportant n symboles.

Désignons par $P(T, p)$ le nombre de "(" diminué du nombre de ")" dans les p premiers symboles de T.

Alors:

a) si $p=1, 2, \dots, n$, $P(T, p)\geqslant 0$

b) si $p=2, 3, \dots, n-1$, $P(T, p)\geqslant 1$

c) $P(T, n)=0$

1.0.17 Démonstration

Nous allons procéder par récurrence sur le nombre n.

- Lorsque $n=1$, a) et c) sont évidentes. Quant à b), elle est satisfaite parce qu'il n'existe pas de valeur de p qui la mette en défaut.
- Lorsque $n>1$, supposons le lemme vrai pour les termes de L ayant moins de n symboles. Soit T un terme de L comportant n symboles. T est de la forme $f_q(t_1, t_2, \dots, t_q)$, où f_q est un symbole de fonction q-aire et $t_1, t_2, \dots, t_q$ sont des termes ayant moins de n symboles. On constate successivement que:

$P(T, 1)=0$ car le premier symbole de T est f_q.

$P(T, 2)=1$ car le deuxième symbole de T est (.

$P(T, p)\geqslant 1$ si $p=3, 4, \dots, n-1$, à cause de l'hypothèse de récurrence appliquée à $t_1, t_2, \dots, t_q$.

$P(T, n-1)=1$ pour la même raison.

Donc $P(T, n)=0$ car le dernier symbole de T est). □

1.0.18 Corollaire

Convenons d'appeler *section commençante* d'un terme l'agrégat de symboles obtenus en biffant un ou plusieurs symboles à partir de la fin de ce terme. Alors une section commençante d'un terme n'est jamais un terme.

1.0.19 Lemme

Soit L un langage du premier ordre.

Soit φ une formule de L comportant n symboles.

Désignons par $P(\varphi, p)$ le nombre de "(" diminué du nombre de ")" dans les p premiers symboles de φ.

Alors:

a) si $p=1, 2, \ldots, n$, $P(\varphi, p) \geqslant 0$

b) si $p=2, 3, \ldots, n-1$, $P(\varphi, p) \geqslant 1$

c) $P(\varphi, n)=0$.

1.0.20 Démonstration

Nous allons à nouveau procéder par une sorte de récurrence, mais cette fois sur la complexité de la formule φ.

1^er^ cas: φ est une formule atomique de L.

- Si φ est de la forme $(t_1=t_2)$ avec $t_1, t_2 \in \mathrm{Ter}(L)$, il est clair que $P(\varphi, 1)=1$. En vertu du lemme 1.0.16, $P(\varphi, p) \geqslant 1$ pour $2, 3, \ldots, n-1$. De même $P(\varphi, n-1)=1$ et par suite $P(\varphi, n)=0$.
- Si φ est de la forme $R_q(t_1, t_2, \ldots, t_q)$ où R_q est un symbole de relation q-aire et $t_1, t_2, \ldots, t_q \in \mathrm{Ter}(L)$, $P(\varphi, 1)=0$ et $P(\varphi, 2)=1$. En vertu du lemme 1.0.16, $P(\varphi, p) \geqslant 1$ pour $p=2, 3, \ldots, n-1$. De même $P(\varphi, n-1)=1$ et par suite $P(\varphi, n)=0$.

2^e^ cas: soit φ une formule de L vérifiant le lemme 1.0.19.

- $P((\neg\varphi), 1)=1$. $P((\neg\varphi), 2)=1$. En vertu de l'hypothèse faite sur φ, $P((\neg\varphi), p) \geqslant 1$ pour $p=3, 4, \ldots, n-1$; $P((\neg\varphi), n-1)=1$ et $P((\neg\varphi), n)=0$.
- Si on désigne par Q l'un quelconque des quantificateurs et par y un symbole de variable, on a:
  $P((Qy\varphi), 1)=\mathrm{P}((Qy\varphi), 2)=P((Qy\varphi), 3)=1$. En vertu de l'hypothèse faite sur φ, $P((Qy\varphi), p) \geqslant 1$ pour $4, 5, \ldots, n-1$; $P((Qy\varphi), n-1)=1$ et $P((Qy\varphi), n)=0$.

3^e^ cas: Soit φ et ψ deux formules de L vérifiant le lemme 1.0.19.

Désignons par $*$ l'un quelconque des connecteurs $\wedge$, $\vee$, $\rightarrow$ ou $\leftrightarrow$. On a $P((\varphi*\psi), 1)=1$. En vertu de l'hypothèse faite sur φ et ψ, $P((\varphi*\psi), p) \geqslant 1$ pour $p=2, 3, \ldots, n-1$; $P((\varphi*\psi), n-1)=1$ et, par suite, $P((\varphi*\psi), n)=0$. □

1.0.21 Corollaire

Moyennant une convention analogue à celle du corollaire 1.0.18, une section commençante d'une formule n'est jamais une formule.

1.0.22 Remarque

Il n'est pas difficile d'imaginer une machine capable de calculer la fonction (de p), $P(A, p)$ pour un agrégat A de symboles de L quelconque. On pourrait donner à cette machine la consigne de rejeter tout agrégat A de n symboles de L tel que $P(A, p)$ ne vérifie pas les conclusions du lemme 1.0.19. En introduisant des critères analogues mais un peu plus fins, on pourrait faire en sorte que la machine ne conserve que les formules de L. Il existe donc une procédure mécanique permettant de décider si un agrégat de symboles de L est une formule de L ou non.

1.0.23 Proposition

Soit L un langage du premier ordre et α, β, φ, ψ, $\in \mathrm{For}(L)$.

Alors:

a) Si $(\neg\alpha)$ et $(\neg\varphi)$ désignent une même formule, il en est de même de α et φ.

b) Soit y un symbole de variable et Q l'un quelconque des quantificateurs. Si $(Qy\alpha)$ et $(Qy\varphi)$ désignent une même formule, il en est de même de α et φ.

c) Soit $*$ l'un quelconque des connecteurs $\wedge$, $\vee$, $\rightarrow$ ou $\leftrightarrow$. Si $(\alpha*\beta)$ et $(\varphi*\psi)$ désignent une même formule, il en est de même de α et φ d'une part, de β et ψ d'autre part.

1.0.24 Démonstration

a) Si $(\neg\alpha)$ et $(\neg\varphi)$ désignent un même agrégat de symboles de L, il en est évidemment de même de α et φ.

b) Même argumentation que pour a).

c) Si $(\alpha*\beta)$ et $(\varphi*\psi)$ désignent une même formule de L, $\alpha*\beta)$ et $\varphi*\psi)$ désignent le même agrégat de symboles de L. Alors de trois choses l'une:

ou α est une section commençante de φ

ou φ est une section commençante de α

ou α et φ désignent une même formule de L.

Le corollaire 1.0.21 exclut les deux premières éventualités. Donc α et φ désignent une même formule. Il s'ensuit que $*\beta)$ et $*\psi)$ désignent le même agrégat de symboles. Par conséquent, β et φ désignent une même formule. □

1.0.25 Commentaire

La proposition 1.0.23 ainsi que les lemmes 1.0.16 et 1.0.19 ont pour conséquence immédiate que l'arbre de composition d'une formule de L est essentiellement unique. On exprime aussi ce fait en disant que les formules de L ont la propriété d'*unique lisibilité*. Par opposition, si α, β, $\gamma \in \mathrm{For}(L)$, l'agrégat $(\alpha \wedge \beta \wedge \gamma)$, qui n'est pas une formule de L, pourrait être lu de deux manières distinctes: $((\alpha \wedge \beta) \wedge \gamma)$ et $(\alpha \wedge (\beta \wedge \gamma))$, qui sont deux formules de L différentes.

1.0.26 Commentaire

Le corollaire 1.0.18 énonce une propriété analogue pour les termes. Tout terme de L est construit de proche en proche à partir des symboles de constantes et de variables par l'introduction de symboles de fonctions. L'ordre d'intervention de ces derniers est déterminé par les parenthèses. Par opposition, en algèbre ordinaire, $a+b+c$ peut être lu de deux façons différentes: $((a+b)+c)$ ou $(a+(b+c))$; les symboles $+$ s'y succèdent dans des ordres différents; on remarque d'autre part que $a+b$ est une section commençante de $a+b+c$ et qu'elle a un sens (en algèbre élémentaire). Une telle éventualité est exclue en ce qui concerne les termes de L. On parle aussi de l'*unique lisibilité des termes* de L.

1.0.27 Convention

A plusieurs reprises, nous avons désigné des symboles isolés ou plus généralement des agrégats de symboles d'un langage du premier ordre L par une lettre ou une abréviation étrangère à L: α, φ, y, Q, t_1 ... Par la suite, nous écrirons: $A \equiv B$ pour exprimer que A et B sont des signes pour le même agrégat de symboles.

Par exemple, si y désigne un symbole de variable, x''' pour fixer les idées, nous écrirons $y \equiv x'''$. Relevons que $\equiv$ n'est pas un symbole logique.

1.0.28 Définition

Soit L un langage du premier ordre et $\varphi \in \mathrm{For}(L)$.

- L'*ensemble des* (symboles de) *variables libres* de φ, noté $\mathrm{VL}(\varphi)$ est défini de la manière suivante:

  Si φ est atomique, $\mathrm{VL}(\varphi)$ est la collection des symboles de variables figurant dans φ

  $\mathrm{VL}((\neg\varphi)) = \mathrm{VL}(\varphi)$

  Si φ, $\psi \in \mathrm{For}(L)$,

  $\mathrm{VL}((\varphi \wedge \psi)) = \mathrm{VL}((\varphi \vee \psi)) = \mathrm{VL}((\varphi \rightarrow \psi)) = \mathrm{VL}((\varphi \leftrightarrow \psi)) = \mathrm{VL}(\varphi) \cup \mathrm{VL}(\psi)$.

  Si y est un symbole de variables,

  $\mathrm{VL}((\forall y \varphi)) = \mathrm{VL}((\exists y \varphi)) = \mathrm{VL}(\varphi) - \{y\}$

  (i.e. l'ensemble $\mathrm{VL}(\varphi)$ privé de y, s'il s'y trouve).

- Un *énoncé* de L est une formule de L dont l'ensemble des variables libres est vide, c'est-à-dire ne comporte aucun élément.

1.0.29 Exemples

Reprenons le langage L_1 des exemples précédents.

1.0.29.1 Déterminons VL(φ), où:
$\varphi \equiv ((\exists x'(f_2(x, x') = c)) \vee (\forall x(R_1(x) \to (x'' = c))))$

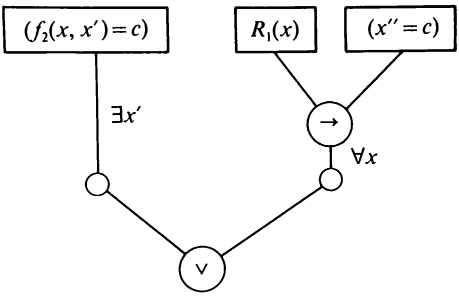


Fig. 1.1

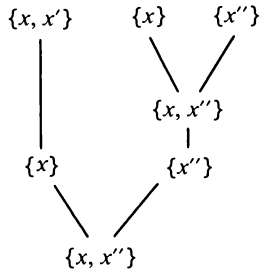


Fig. 1.2

Nous avons représenté à gauche l'arbre de formation de φ. A droite, en parallèle, nous avons déterminé les ensembles de variables libres des formules figurant aux sommets de l'arbre suivant les règles de la définition 1.0.28. Par suite: $\mathrm{VL}(\varphi) = \{x, x''\}$.

1.0.29.2 Par un procédé analogue, on vérifie que la formule (1.0) est un énoncé de L_1.

1.0.29.3 Si $\varphi \in \mathrm{For}(L_1)$ et si $\mathrm{VL}(\varphi) = \{x, x'\}$, $(\forall x'(\forall x\alpha))$ est un énoncé de L_1.

1.1 COMMENTAIRES GÉNÉRAUX

1.1.0 Du choix et de l'économie des symboles logiques

Pour l'instant, les symboles logiques que nous avons considérés sont absolument dénués de signification, même si nous les avons munis d'étiquettes qui permettent de les lire. Mais, comme nous le constaterons bientôt, ils recevront des interprétations assez proches de ce que suggèrent leurs dénominations. Les remarques qui suivent anticipent sur le paragraphe suivant.

Ainsi, nous verrons que $\wedge$ se comporte à peu près comme le mot "et"; et que $\neg$, qui se lit "non", évoque la locution "il est faux que...". Si α et β sont des formules, $(\alpha\leftrightarrow\beta)$ aura la même interprétation que $((\alpha\rightarrow\beta)\wedge(\beta\rightarrow\alpha))$. On pourrait donc faire l'économie du symbole $\leftrightarrow$ qui apparaît dès lors comme une abréviation. Certains auteurs procèdent de la sorte. Les langages qu'ils définissent diffèrent des nôtres, mais pas essentiellement. Pour faire une comparaison, imaginons deux auteurs présentant formellement les nombres naturels, l'un dans le système décimal, l'autre dans le système binaire. Le premier a besoin de dix symboles, le second de deux seulement. Leurs jeux de construction sont différents. Mais il est facile de passer de l'un à l'autre et, à des détails secondaires près, ils jouissent finalement des mêmes propriétés. Les langages du premier ordre sont dans une situation comparable suivant qu'on accepte ou qu'on rejette le symbole $\leftrightarrow$. Nous avons choisi une collection de symboles logiques assez familiers en mathématiques. Elle a l'avantage de s'adapter sans trop de mal au langage ordinaire.

On peut encore aller plus loin sur le chemin de l'économie. Par exemple, $(\alpha\vee\beta)$ recevra la même interprétation que $(\neg((\neg\alpha)\wedge(\neg\beta)))$. Intuitivement, "$\alpha$ ou β" a le même sens que "il est faux que l'on n'ait ni α, ni β". On pourrait donc se passer du symbole $\vee$, à condition de garder $\wedge$. D'autre part, "α et β" a la même signification intuitive que "il est faux que l'on ait (non α) ou (non β)". On conçoit que $(\alpha\wedge\beta)$ aura la même interprétation que $(\neg((\neg\alpha)\vee(\neg\beta)))$. Cela permettrait d'économiser $\wedge$ au dépens de $\vee$. Il existe des partisans des deux éventualités. Ainsi, non seulement on peut réduire le nombre des symboles logiques, mais on peut s'y prendre de plusieurs manières distinctes.

Ce n'est pas tout. Nous constaterons que $(\alpha\rightarrow\beta)$ a la même interprétation que $(\beta\vee(\neg\alpha))$. Intuitivement, "si Socrate est un homme, alors Socrate est mortel" a le même sens que "Socrate est mortel ou Socrate n'est pas un homme". Ayant $\vee$ (ou $\wedge$) on pourrait donc économiser $\rightarrow$. De même on pourrait abandonner l'un des quantificateurs. Si α est une formule et y un symbole de variable, $(\exists y\varphi)$ peut être interprété comme $(\neg(\forall y(\neg\varphi)))$. Par exemple, "il existe un triangle rectangle" équivaut à "il est faux que tout triangle soit non rectangle". Symétriquement, $(\forall y\varphi)$ peut être interprété comme $(\neg(\exists y(\neg\varphi)))$: "tout homme est mortel" équivaut à "il est faux qu'il existe un homme immortel". Finalement, on pourrait réduire les symboles logiques à quatre: $\neg$ $\wedge$ $=$ $\forall$, par exemple.

D'autre part, les symboles de constantes se comportent exactement comme des symboles de fonctions o-aires (cf. déf. 1.0.6). Certains auteurs les introduisent comme tels. Dans ce cas, si f_n désigne un symbole de fonction, n peut prendre toutes les valeurs naturelles, 0, 1, 2, ...

1.1.1 De l'économie des signes typographiques

Nous avons introduit les symboles de fonctions f_n, $f'_{n'}$, $f''_{n''}$, ... et de relations R_m, $R'_{m'}$, $R''_{m''}$, ... , où n, n', n'', ... , m, m', m'', ... sont des entiers strictement positifs. Supposons que $n'=5$ et que $m=3$ pour fixer les idées; nous pourrions convenir de noter $f'_{n'}$ sous la forme $f', '''''$ et R_m sous la forme $R, '''$. D'une part, tous les signes typographiques s'écriraient en ligne; de l'autre, nous renoncerions à noter les indices sous forme décimale ou binaire. Compte tenu de tout ce qui précède, nous pourrions réduire à onze le stock des signes typographiques suffisants pour écrire n'importe quelle formule du premier ordre:

$$\neg \quad \wedge \quad = \quad \forall \quad (\quad) \quad , \quad ' \quad x \quad f \quad R$$

par exemple.

1.1.2 De l'usage des parenthèses

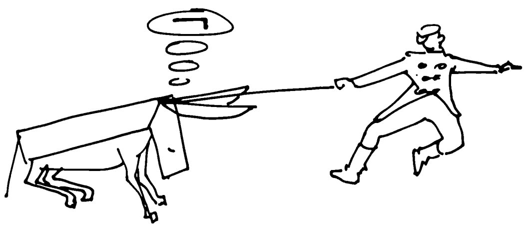
Nous avons constaté que les parenthèses assurent l'unique lisibilité des formules. Malheureusement, elles alourdissent l'écriture et il est bien rare qu'on n'en oublie pas une. On pourrait essayer de remplacer les règles de formation des termes et des formules (cf. déf. 1.0.6 et 1.0.8) par d'autres. Par exemple, on écrirait:

$f'_{n'}\ t_1\ t_2 \ldots t_{n'}$	au lieu de	$f'_{n'}(t_1, t_2, \ldots t_{n'})$
$R''_{m''}\ t_1\ t_2 \ldots t_{m''}$	au lieu de	$R''_{m''}(t_1, t_2, \ldots t_{m''})$
$=t_1\ t_2$	au lieu de	$(t_1 = t_2)$
$\neg\varphi$	au lieu de	$(\neg\varphi)$
$*\varphi\psi$	au lieu de	$(\varphi * \psi)$ où $*$ désigne $\wedge$, $\vee$, $\rightarrow$ ou $\leftrightarrow$
$\forall y\varphi$	au lieu de	$(\forall y\varphi)$
$\exists y\varphi$	au lieu de	$(\exists y\varphi)$

Il faut évidemment s'assurer que, dans ce nouveau système, les termes jouissent encore de la propriété d'unique lisibilité. La chose est possible: on peut montrer qu'aucune section commençante d'un terme n'est un terme, qu'aucune section commençante d'une formule n'est une formule. Ainsi, moyennant d'autres règles de formation, on pourrait faire l'économie des parenthèses. L'écritude des formules obtenues s'écarte à la fois de la langue parlée et des habitudes de l'algèbre élémentaire. Aussi renoncerons-nous à cette "simplification". Néanmoins, elle présente un grand intérêt théorique et pratique. Elle a été introduite par Łukasiewicz et elle est connue sous le nom de "notation polonaise". Elle permet de réduire à neuf le nombre des signes typographiques suffisants pour écrire effectivement n'importe quelle formule du premier ordre:

$$\neg \quad \wedge \quad = \quad \forall \quad , \quad ' \quad x \quad f \quad R$$

Elle est utilisée dans le traitement automatique des langages du premier ordre.



L'idée de modèle ensembliste

2.0 INTRODUCTION

Au paragraphe précédent, nous avons défini ce qu'il faut entendre par un "langage du premier ordre" L. Nous avons comparé les formules de L à des phrases. Dans une langue ordinaire, une phrase ou, plus généralement, un discours peuvent être considérés sous deux angles au moins. On peut d'abord examiner s'ils sont conformes aux lois de la grammaire: c'est ce que nous appellerons leur aspect *syntaxique*. On peut ensuite les étudier selon leur capacité de porter un sens et c'est alors leur aspect *sémantique*. Dans une langue ordinaire toujours, ces deux aspects sont étroitement dépendants. Une modification de la forme grammaticale d'une phrase change généralement son sens. Réciproquement, le contenu sémantique d'un discours permet souvent d'éclairer sa syntaxe. "On apporte une citrouille à la fée; elle la transforme en carrosse": il est clair que le pronom "elle" s'applique à la fée parce qu'il n'est pas dans les habitudes des citrouilles de transformer les fées en carrosses. "Je pleus", qui apparemment n'est pas correct du point de vue syntaxique, peut le devenir dans la bouche d'un professeur de géographie armé d'un arrosoir et démontrant les effets de l'érosion dans un bac à sable.

Les langages du premier ordre présentent aussi un aspect syntaxique et un potentiel sémantique. Nous n'avons envisagé que le premier jusqu'ici. Ce que nous en avons vu permet d'affirmer que, contrairement à ce qui se passe pour les langages ordinaires, on peut étudier l'aspect syntaxique d'un langage du premier ordre L sans référence à ses capacités sémantiques éventuelles. Une machine convenablement préparée peut déterminer si un assemblage de signes est une formule de L ou non. Dès le paragraphe suivant, nous reprendrons l'étude syntaxique des langages du premier ordre. Pour l'heure, nous nous attacherons à définir une certaine classe de contenus sémantiques qui peuvent leur être affectés.

Afin de mieux étudier le point où nous sommes, introduisons une comparaison. Par des règles un peu semblables à celles que donnent les définitions 1.0.6 et 1.0.8, on peut définir d'une manière purement formelle les *polynômes* en x à coefficients naturels, tels que $4x^2+12x$, $3x^3+2x+1$, x^2+5 (ou $1x^2+5$), par exemple. On peut ensuite édicter des consignes permettant d'additionner et de multiplier ces objets. Voilà pour l'aspect syntaxique de ces polynômes. Pour évoquer un de leurs aspects sémantiques, considérons l'aire d'une bordure de 3 mètres de large encadrant un bassin carré de 3 mètres de côté. Elle s'exprime par le nombre $4 \cdot 3^2 + 12 \cdot 3$, c'est-à-dire par le polynôme $4x^2 + 12x$ où on a substitué 3 à x. Si on désigne par $P(x)$ le polynôme $4x^2 + 12x$, l'aire considérée peut être notée $P(3)$. Plus généralement, on peut remplacer x par n'importe quel nombre naturel a; on voit apparaître une *fonction polynômiale* définie sur les nombres naturels, à valeurs naturelles et qui fait correspondre à a le nombre $P(a)$. On peut procéder de même avec n'importe quel autre polynôme en x à coefficients naturels et examiner comment se comportent les fonctions polynômiales respectivement attachées à deux polynômes, à leur somme et à leur produit. Rien n'empêcherait de recommencer en remplaçant x par des nombres réels, des nombres complexes, des polynômes en x, des matrices, etc. On obtiendrait autant d'interprétations différentes du même système de polynômes. Il est intéressant d'étudier les attributs de ces interprétations qui découlent uniquement des propriétés formelles – ou, si l'on préfère, algébriques – des polynômes en x à coefficients naturels.

Le cas des langages du premier ordre est tout à fait analogue. Pour l'instant, seul leur aspect syntaxique nous est connu. Toutefois ils ont été constitués en vue de décrire certaines situations. Par exemple, considérons la population d'un village V^{***}. Proposons-nous de mettre en évidence les relations familiales qui y existent. Introduisons un symbole de relation binaire R_2 et convenons que $R_2(x, x')$ signifie "x est père de x'". L'énoncé $(\forall x(\neg R_2(x, x)))$ se lit: "quel que soit x, non $R_2(x, x)$" qu'en français on peut traduire par "quel que soit l'individu x du village V^{***}, il n'est pas son propre père". Il est facile d'interpréter des formules telles que $(R_2(x, x') \wedge R_2(x', x''))$ ou $(\forall x(\exists x' R_2(x', x)))$. L'introduction d'autres symboles permettrait de traduire des assertions telles que "c est du sexe masculin", "c' est du sexe féminin", "x est la mère de x'", "x' et x ont le droit de se marier", etc. Nous disposerions alors d'un langage du premier ordre permettant une description assez poussée de la population de V^{***}. Celle-ci serait en quelque sorte une interprétation sociologique du langage considéré.

Pour les langages du premier ordre pris en général, nous allons envisager des interprétations à la fois plus simples et plus abstraites. Les collections considérées seront des *ensembles* et non plus des groupements d'objets compliquées tels que des livres, des doctrines ou encore des êtres humains comme dans le cas du village V^{***}. Des individus – ou éléments – composant ces ensembles, on ne saura faire que deux choses: les distinguer et reconnaître s'ils appartiennent ou non à un ensemble donné. Quant aux ensembles eux-mêmes, ils pourront être arbitrairement grands, voire inépuisables.

La notion d'*ensemble* est assez intuitive. Nous n'en utiliserons que les propriétés les plus élémentaires. Nous parlerons à ce propos de la *notion naïve d'ensemble*. Pour le profane, cela signifie que le terme d'ensemble sera utilisé comme dans la langue ordinaire, moyennant quelques précautions que nous rappellerons ci-dessous. Pour le lecteur averti, cela veut dire que nous ne nous appuierons pas sur une théorie mathématique des ensembles. Nous verrons ultérieurement ce qu'il conviendrait d'entendre par là.

2.1 CONVENTIONS RELATIVES AUX ENSEMBLES

2.1.1 Convention

Un ensemble est susceptible de comporter des *éléments*. Si a est un élément de l'ensemble E, on note $a \in E$. Si a n'est pas un élément de E, on note $a \notin E$.

2.1.2 Convention

Si A et E sont des ensembles et si tout élément de A appartient à E, on dit que A est une *partie* ou un *sous-ensemble* de E, et on note $A \subset E$; cette expression se lit: "A est *inclus* dans E". Si $A \subset E$ et $E \subset A$, on dit que A et E sont *égaux* et on note $A = E$.

2.1.3 Convention

Il existe un *ensemble vide* noté $\emptyset$. Il est caractérisé par le fait que, pour tout élément a, $a \notin \emptyset$. D'après 2.1.2., quel que soit l'ensemble E, $\emptyset \subset E$.

2.1.4 Convention

Si $x_1, x_2, \dots, x_n$, pris dans cet ordre, désignent des éléments distincts ou non, $(x_1, x_2, \dots, x_n)$ est une notation pour ce qu'on appelle un *n-uple*. On parle de *singleton*, de *couple*, de *triple* lorsque $n = 1, 2, 3$ respectivement.

2.1.5 Convention

Si $E, F, G, \dots$ sont des ensembles distincts ou non:

- $E \times F$ est l'ensemble des couples (x, y) avec $x \in E$ et $y \in F$. C'est le *produit cartésien* de E et de F.
- $E \times F \times G$ est l'ensemble des triples (x, y, z) avec $x \in E$, $y \in F$ et $z \in G$. C'est le *produit cartésien* de E, F et G.
- Plus généralement, si $E_1, E_2, \dots, E_n$ sont des ensembles distincts ou non, le *produit cartésien* $E_1 \times E_2 \times \dots \times E_n$ est l'ensemble des n-uples $(x_1, x_2, \dots, x_n)$ où $x_1 \in E_1, x_2 \in E_2, \dots x_n \in E_n$. Dans le cas particulier où $E_1 = E_2 = \dots = E_n = E$, ce produit cartésien se note E^n.

2.1.6 Convention

Si E et F sont deux ensembles, l'ensemble des éléments appartenant à l'un des deux au moins est l'*union* ou la *réunion* de E et F; on le note $E \cup F$.

Plus généralement, si E_1, E_2, ... , E_n, ... sont des ensembles, leur *union* ou *réunion*, notée $\bigcup_n E_n$, est l'ensemble des éléments appartenant à l'un au moins de ces ensembles.

2.1.7 Convention

Si E et F sont deux ensembles, l'ensemble des éléments communs à E et F est l'intersection de E et F; on le note $E \cap F$. Lorsque $E \cap F$ est vide, on dit que E et F sont *disjoints*.

Plus généralement, si E_1, E_2, ... , E_n, ... sont des ensembles, leur *intersection*, notée $\bigcap_n E_n$ est l'ensemble des éléments appartenant à la fois à tous ces ensembles.

2.1.8 Convention

Si A et B sont deux ensembles, on note $A-B$ l'ensemble des éléments de A qui n'appartiennent pas à B.

2.1.9 Convention

Une application ou fonction f d'un ensemble E dans (ou vers) un ensemble F, notée:

$$\begin{aligned} f:\ & E \to F \\ & x \mapsto f(x) \end{aligned}$$

est un ensemble de couples $(x, y) \in E \times F$, aussi appelé *graphe de f*, tel que:

- pour tout $x \in E$, il existe un couple (x, y) dans cet ensemble f;
- si (x, y) et (x, z) appartiennent à l'ensemble f, alors y et z coïncident.

Pour tout $x \in E$, on note $f(x)$ le seul élément $y \in F$ tel que (x, y) appartient à l'ensemble f; $f(x)$ est appelé *valeur* de f pour l'*argument* x. Nous préciserons parfois que f est une fonction (ou application) *unaire* de E dans F.

Une fonction *binaire* de E dans F est une application de E^2 dans F. Soit g une telle fonction binaire de E dans F. On note:

$$\begin{aligned} g:\ & E^2 \quad\quad \to F \\ & (x_1, x_2) \mapsto g(x_1, x_2) \end{aligned}$$

$g(x_1, x_2)$ désigne la valeur de g pour les *arguments* x_1 et x_2. Une fonction *ternaire*, respectivement *n-aire*, de E dans F est une application de E^3, respectivement E^n dans F. Elle comporte 3, respectivement n arguments.

Soit $f: E \to F$ une application et soit A une partie de E; on note $f|_A$ l'application de A dans F déterminée par la condition: $f|_A(x)$ coïncide avec $f(x)$ pour tout $x \in A$. $f|_A$ est appelée *restriction de f à A*.

2.1.10 Remarque importante

Il ne faut pas confondre la flèche apparaissant dans $f\colon E \to F$ avec le symbole logique $\to$. Le contexte permet toujours de décider.

2.1.11 La notion de relation

Une relation *unaire* dans un ensemble E est une partie R_1 de E. Si $x \in R_1$, on note $R_1(x)$ et on dit que x satisfait la relation R_1.

Une relation *n-aire* dans un ensemble E est une partie R_n de E^n. Lorsque $(x_1, x_2, \ldots, x_n) \in R_n$, on note $R_n(x_1, x_2, \ldots, x_n)$; ces deux notations sont équivalentes.

2.1.12 Un exemple de relation: l'égalité

L'*égalité* dans un ensemble E est la relation binaire donnée par la diagonale Δ de E^2, c'est-à-dire par l'ensemble de couples $(x, x) \in E^2$, où x parcourt E. Lorsque $(x_1, x_2) \in \Delta$, en bonne doctrine on devrait écrire $\Delta(x_1, x_2)$; mais habituellement, on note $x_1 = x_2$ et nous ferons ainsi.

2.1.13 Autres exemples: les idées d'ordre, d'ordre total, de bon ordre

Un *ordre* dans un ensemble E est une relation binaire donnée par une partie $\mathcal{O}$ de E^2 telle que:

la diagonale Δ de E^2 est incluse dans $\mathcal{O}$

si $(x, y) \in \mathcal{O}$ et $(y, x) \in \mathcal{O}$, alors $x = y$

si $(x, y) \in \mathcal{O}$ et $(y, z) \in \mathcal{O}$, alors $(x, z) \in \mathcal{O}$.

Lorsqu'on ne considère qu'un ordre $\mathcal{O}$ dans E, $\mathcal{O}(x, y)$ se note habituellement $x \leqq y$. Lorsqu'on considère simultanément plusieurs ordres dans E, il convient d'adopter des signes différents pour les distinguer.

Un ordre $\mathcal{O}$ dans E est dit *total* si, pour tout $x \in E$ et tout $y \in E$, on a $(x, y) \in \mathcal{O}$ ou $(y, x) \in \mathcal{O}$. Un tel ordre est dit *bon* et E est dit *bien ordonné* par $\mathcal{O}$, si, de surcroît, pour toute partie non vide A de E il existe $a \in A$ tel que $x \in A$ entraîne $(a, x) \in \mathcal{O}$.

2.1.14 Remarque importante

La notion d'ensemble est abstraite, en ce sens qu'il faut faire la distinction entre chaque élément d'un ensemble et le signe – ou les signes – qu'on emploie éventuellement pour le nommer. Un même élément peut être désigné par plusieurs signes différents; $1+1$ et 2 sont des signes pour le même nombre naturel, par exemple. Un élément peut fort bien ne pas avoir de désignation, comme c'est le cas pour presque tous les points du plan muni d'une figure donnée.

2.1.15 Remarque importante

Au cours du rappel ci-dessus, ainsi qu'au chap. 1 (lemmes 1.0.16 et 1.0.19, déf. 1.0.28), nous avons employé à plusieurs reprises un signe "égale". D'une façon générale, dans le texte ordinaire, "$a=b$" est une abréviation pour "a et b sont des notations pour le même objet". Par principe, il faut distinguer ce signe = du symbole logique =; ils ne seront cependant pas figurés par des caractères typographiques différents.

Par un surcroît de précaution, nous avons introduit au chapitre 1 le signe ≡ pour indiquer que deux notations désignent le même agrégat de symboles d'un langage du premier ordre L. Ainsi, si t_1 et t_2 désignent des termes de L, $t_1 \equiv t_2$ signifie qu'ils sont attachés à un seul et même terme de L; tandis que $(t_1 = t_2)$ est une formule de L qui ne donne aucun renseignement sur les termes désignés par t_1 et t_2.

2.1.16 Remarque importante

Dans le même ordre d'idée, nous aurons souvent à exprimer qu'une condition C_1 a pour conséquence nécessaire une condition C_2. Nous le noterons $C_1 \Rightarrow C_2$. Par exemple, $(a \in A$ *et* $A \subset E) \Rightarrow (a \in E)$. Lorsque $C_1 \Rightarrow C_2$ *et* $C_2 \Rightarrow C_1$, nous noterons $C_1 \Leftrightarrow C_2$, ce qui peut se lire "C_1 est valide *si et seulement si* C_2 est valide". Cette phrase s'abrège parfois en "C_1 *ssi* C_2". Il importe de ne pas confondre $\Rightarrow$ (resp. $\Leftrightarrow$) avec $\rightarrow$ (resp. $\leftrightarrow$). Les deux premiers sont des abréviations pour des locutions de la langue ordinaire; ils relèvent de ce qu'on peut considérer comme la "logique naïve". Les deux derniers sont des symboles logiques dénués de signification *a priori.*

2.2 LA NOTION DE *L*-STRUCTURE

2.2.0 Préambule

Soit L un langage du premier ordre. Outre les huit symboles logiques, les trois symboles de ponctuation et une collection de symboles de variables, il comporte des collections de symboles propres: Cst(L), Fct(L) et Rel(L). Nous admettrons, sans autre forme de procès, que ***toutes ces collections sont des ensembles***, pour tous les langages du premier ordre considérés. Il existe des collections qui ne sont pas des ensembles. Toutefois elles sont si complexes ou si peu maniables que la restriction convenue ne devrait provoquer aucune nostalgie. Nous constaterons d'ailleurs que nous plaçons dans une situation extrêmement générale.

2.2.1 Définition

Soit L un langage du premier ordre.

Une structure ensembliste pour L, ou *L-structure*, est la donnée d'un couple (E, J) où:

- E est un ensemble non vide
- J, que nous appellerons *interprétation*, est une application, autrement dit un ensemble de couples, dont les premières composantes appartiennent à:

$$\mathrm{Cst}(L) \cup \mathrm{Fct}(L) \cup \mathrm{Rel}(L)$$

et telle que:

i) si $c \in \mathrm{Cst}(L)$, $J(c)$, aussi noté $\tilde{c}$, est un élément de E

ii) si $f_n \in \mathrm{Fct}(L)$, $J(f_n)$, aussi noté $\tilde{f}_n$, est une fonction de E^n dans E

iii) si $R_m \in \mathrm{Rel}(L)$, $J(R_m)$, aussi noté $\tilde{R}_m$, est une partie de E^m

Cette définition justifie *a posteriori* les locutions: “symboles de constante, de fonction et de relation” introduites au chapitre 1. Relevons aussi qu'une L-structure ne permet pas de “traduire” les symboles logiques, les symboles de variables ni les symboles de ponctuations.

2.2.2 Exemple

Soit L un langage du premier ordre. Soit $E = \{e\}$ un ensemble réduit à un seul élément. Posons alors:

- pour tout $c \in \mathrm{Cst}(L)$, $J(c) := e$
- pour tout symbole de fonction n-aire $f_n \in \mathrm{Fct}(L)$, $J(f_n)$ égale l'unique fonction n-aire sur E à valeurs dans E: $J(f_n)\colon E^n \to E$
- pour tout symbole de relation m-aire $R_m \in \mathrm{Rel}(L)$, $J(R_m) := \emptyset \subset E^m$.

(“$J(c) := e$” se lit: “$J(c)$ égale, par définition, e”.)

Cet exemple montre que tout langage du premier ordre L admet au moins une L-structure.

2.2.3 Exemples

Donnons un langage du premier ordre L_2 par:

$$\mathrm{Cst}(L_2) := \{c\},\ \mathrm{Fct}(L_2) := \{f_2\},\ \mathrm{Rel}(L_2) := \{R_2\}$$

2.2.3.0 1^er^ exemple de L_2-structure

Prenons l'ensemble à trois éléments $E_1 := \{u, v, w\}$ et déterminons l'interprétation J_1 par:

- $J_1(c) = \tilde{c} := u$
- $J_1(f_2) = \tilde{f}_2$ égale, par définition, l'application binaire $\tilde{f}_2\colon E_1^2 \to E_1$ donnée par l'ensemble:

$\{((u, u), u), ((u, v), v), ((u, w), w), ((v, u), v), ((v, v), w), ((v, w), u), ((w, u), w),$

$((w, v), u), ((w, w), v)\}$

qu'on peut aussi représenter dans un tableau à double entrée:

$$E_l \left\{ \begin{array}{c} w \\ v \\ u \end{array} \right. \quad \begin{array}{|c|c|c|} \hline w & u & v \\ \hline v & w & u \\ \hline u & v & w \\ \hline \end{array} \quad \tilde{f}_2\,(w, v)$$
$$\underbrace{u \quad v \quad w}_{E_l}$$

Fig. 2.0

- $J_1(R_2) = \tilde{R}_2 := \{(u, u), (u, v), (u, w), (v, v), (v, w), (w, w)\} \subset E_1^2$
qu'on peut illustrer dans une présentation graphique du produit cartésien E_1^2:

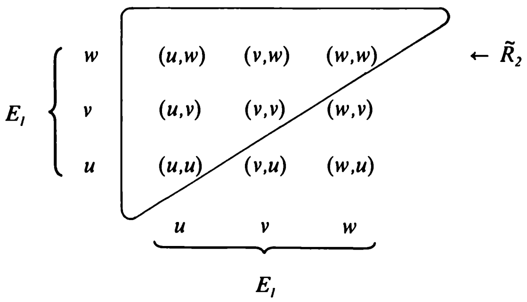


Fig. 2.1

2.2.3.1 2[e] exemple de L_2-structure:

posons $E_2 := \mathbb{N} := \{0, 1, 2, 3, \dots, n, \dots\}$ et déterminons l'interprétation J_2 par:

$J_2(c) := \tilde{c} := 0$
$J_2(f_2) := \tilde{f}_2 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
$(x, y) \to$ maximum de x et y
$J_2(R_2) = \tilde{R}_2 := \{(x, y) \in \mathbb{N}^2 | x$ divise y dans $\mathbb{N}\}$
(x divise y dans $\mathbb{N}$ s'il existe $z \in \mathbb{N}$ tel que $y = xz$).

2.2.4 Définition

Soit L un langage du premier ordre et soit (E, J) une L-structure.
Une *spécialisation* s de (E, J) est une application

s: $\mathrm{Ter}(L) \to E$

soumise aux deux conditions suivantes:

i) si $t \in \mathrm{Cst}(L)$, $s(t) = J(t)$

ii) si $f_n \in \mathrm{Fct}(L)$ et si $t_1, t_2, \ldots, t_2 \in \mathrm{Ter}(L)$
$s(f_n(t_1, t_2. \ldots, t_n)) = J(f_n)(s(t_1), s(t_2), \ldots, s(t_n))$

2.2.5 Remarque

La condition i) exprime que s et J coïncident sur Cst(L).

2.2.6 Remarque

Les symboles de variables sont des termes; autrement dit: $\mathrm{Var} \subset \mathrm{Ter}(L)$. En vertu de la condition ii) et de l'unique lisibilité des termes, s est entièrement déterminée par les valeurs qu'elle prend sur $\mathrm{Cst}(L) \cup \mathrm{Var}$.

2.2.7 Remarque

Pour les mêmes raisons, si σ: $\mathrm{Var} \to E$ est une application quelconque, il existe une spécialisation (et une seule) s de (E, J) telle que la restriction de s à Var soit σ. Nous dirons que la spécialisation s est *déterminée par* σ.

2.2.8 Exemple

Reprenons le langage L_2 des exemples 2.2.3 et la L_2-structure (E_1, J_1) de l'exemple 2.2.3.0. Soit s_1 la spécialisation de (E_1, J_1) déterminée par:

$s_1(x) = u$, $s_1(x') = v$, $s_1(x'') = s_1(x''') = \ldots = w$.

Calculons les images par s_1 des termes:

c; $f_2(c, x)$; $f_2(x, c)$; $f_2(x, x')$; $f_2(x, f_2(x, x'))$.

- $s_1(c) = J_1(c) = u$
- $s_1(f_2(c, x)) = J_1(f_2)(s(c), s(x)) = \tilde{f}_2(u, u) = u$
- $s_1(f_2(x, c)) = J_1(f_2)(s(x), s(c)) = \tilde{f}_2(u, u) = u$
- $s_1(f_2(x, x')) = J_1(f_2)(s(x), s(x')) = \tilde{f}_2(u, v) = v$
- $s_1(f_2(x, f_2(x, x')) = J_1(f_2)(s(x), J_1(f_2)(s(x), s(x'))) = \tilde{f}_2(u, \tilde{f}_2(u, v)) = \tilde{f}_2(u,v) = v$.

2.2.9 Convention

Lorsque $P(x)$ est un polynôme en x, l'usage est de désigner par $P(a)$ la valeur de la fonction polynômiale associée à $P(x)$ quand on y spécialise x en a. Par analogie, si s est une spécialisation de (E, J) et t un terme, ce que nous avons désigné par $s(t)$ ***se notera plutôt*** $t(s)$; cette écriture fait penser à la "valeur" des termes t quand on y interprète les symboles de constantes selon J et quand on y spécialise les symboles de variables selon s.

2.2.10 Convention

Soit s une spécialisation de la L-structure (E, J); soit x un symbole de variable et soit a un élément de E. On notera $s\left(\frac{x}{a}\right)$ la spécialisation s' de (E, J) qui coïncide avec s sur tous les symboles de variables, sauf éventuellement en x, et qui envoie x sur a.

Nous sommes maintenant en mesure d'attribuer aux formules du premier ordre un contenu sémantique.

2.2.11 Définition

Soit L un langage du premier ordre, (E, J) une L-structure et s une spécialisation de (E, J). Si φ est une formule de L, le sens de la phrase "*(E, J) satisfait la formule φ pour la spécialisation s*", qui s'abrège en $(E, J)\vDash\varphi[s]$, est déterminé par les règles suivantes (où $\alpha,\beta\in\mathrm{For}(L)$, $t_1, t_2, \dots, t_m\in\mathrm{Ter}(L)$ et $R_m\in\mathrm{Rel}(L)$):

Quand φ est:	*$(E, J)\vDash\varphi[s]$* ***signifie que:***
1) $(t_1=t_2)$	$t_1(s)$ est le même élément que $t_2(s)$
2) $R_m(t_1, t_2, \dots, t_m)$	$(t_1(s), t_2(s), \dots, t_m(s))\in J(R_m)$
3) $(\neg\alpha)$	il est faux que $(E, J)\vDash\alpha[s]$
4) $(\alpha\wedge\beta)$	$(E, J)\vDash\alpha[s]$ *et* $(E, J)\vDash\beta[s]$
5) $(\alpha\vee\beta)$	$(E, J)\vDash\alpha[s]$ *ou* $(E, J)\vDash\beta[s]$
6) $(\alpha\rightarrow\beta)$	$(E, J)\vDash\beta[s]$ *ou* $(E, J)\vDash(\neg\alpha)[s]$
7) $(\alpha\leftrightarrow\beta)$	$(E, J)\vDash(\alpha\rightarrow\beta)[s]$ *et* $(E, J)\vDash(\beta\rightarrow\alpha)[s]$
8) $(\exists x\alpha)$	il existe a dans E tel que $(E, J)\vDash\alpha[s\left(\frac{x}{a}\right)]$
9) $(\forall x\alpha)$	pour tout a dans E, $(E, J)\vDash\alpha[s\left(\frac{x}{a}\right)]$.

2.2.12 Remarque

La définition ci-dessus s'appuie sur la récurrence propre à la construction des formules de L. Elle n'a de sens qu'en vertu de l'unique lisibilité des formules de L.

2.2.13 Remarque

Quelle que soit la formule $\varphi \in \mathrm{For}(L)$, pour reconnaître si $(E, J) \models \varphi[s]$, le test ultime consiste à examiner si des éléments appartiennent ou n'appartiennent pas à certains ensembles. Or, ou bien un élément appartient à un ensemble ou bien il ne lui appartient pas; l'une des éventualités exactement est réalisée. Par conséquent, ou bien $(E, J) \models \varphi[s]$, ou bien $(E, J) \models (\neg\varphi)[s]$.

2.2.14 Remarque

Le mot "ou" figurant dans les règles 5) et 6) est ***disjonctif*** et ***non exclusif***. Placé entre deux éventualités, il exprime que l'une au moins d'entre elles est réalisée. Nous aurons l'occasion de revenir sur le sens des mots "et" et "ou" dans la langue ordinaire.

2.2.15 Remarque

Les seuls symboles qui soient traduits par des verbes sont $=$ et les symboles de relations.

2.2.16 Remarque

En particulier, $(\alpha \rightarrow \beta)$ et $(\beta \vee (\neg\alpha))$ ont la même traduction. Comme nous l'avons annoncé au Chap. 1, on pourrait se passer du symbole $\rightarrow$. On vérifie de la même manière qu'on pourrait faire l'économie des symboles $\vee$, $\leftrightarrow$ et $\exists$.

Cette remarque nous place dans la situation suivante:

D'une part, le système de symboles logiques que nous avons introduit est redondant. Mais il est pratiquement prêt à l'emploi: il permet de traduire presque mot à mot les assertions des mathématiques ordinaires, tout au moins. D'autre part, on pourrait considérer un système de symboles logiques réduit à : $\neg$, $\wedge$, $=$ et $\forall$. Pour établir les faits de la logique du premier ordre, il faut généralement traiter séparément chaque symbole logique. En les ramenant à quatre, on allège d'autant les démonstrations. En revanche, un tel système est pratiquement malcommode.

Nous allons donc passer la ***convention suivante***:

2.2.17 Convention

- les définitions, les propositions, les exemples concerneront toujours des langages du premier ordre comportant notre système de huit symboles logiques.
- En règle générale, nos démonstrations seront "économiques". Elles ne feront intervenir, dans la plupart des cas, que les symboles $\neg$, $\wedge$, $=$ et $\forall$.

Cette commodité exige une contrepartie. A chaque définition nouvelle, nous devrons nous assurer qu'elle est compatible avec le fait que $\vee$, $\rightarrow$, $\leftrightarrow$ et $\exists$ sont des abréviations. Plus précisément:

- $(\alpha \vee \beta)$ est une abréviation pour $(\neg((\neg\alpha)\wedge(\neg\beta)))$; intuitivement "$\alpha$ ou β" équivaut à "il est faux que ni α, ni β"
- $(\alpha\rightarrow\beta)$ est une abréviation pour $(\beta\vee(\neg\alpha))$, donc une abréviation pour $(\neg((\neg\beta)\wedge(\neg(\neg\alpha))))$
- $(\alpha\leftrightarrow\beta)$ est une abréviation pour $((\alpha\rightarrow\beta)\wedge(\beta\rightarrow\alpha))$, donc pour $((\neg((\neg\beta)\wedge(\neg(\neg\alpha))))\wedge(\neg((\neg\alpha)\wedge(\neg(\neg\beta)))))$
- $(\exists x\alpha)$ est une abréviation pour $(\neg(\forall x(\neg\alpha)))$; intuitivement "il existe x tel que α" équivaut à "il est faux que pour tout x, (non α)".

Les vérifications sont généralement tout à fait banales. Nous les confierons au lecteur qui n'aura aucune peine à les effectuer à titre d'exercices. Il pourra aussi reconnaître s'il a compris une démonstration en rédigeant la preuve concernant l'un des symboles logiques laissés de côté. Cela le conduira à paraphraser la preuve donnée dans le texte.

Revenons à la définition 2.2.11 que nous allons illustrer par des exemples.

2.2.18 Exemples

Considérons le langage L_2, la L_2-structure (E_1, J_1) de l'exemple 2.2.3.0 et la spécialisation s_1 de l'exemple 2.2.8. Introduisons les formules suivantes:

$$\alpha\equiv R_2(x, c);\ \beta\equiv(f_2(x, c)=x);\ \gamma\equiv(x'=c)$$
$$\delta\equiv((f_2(x', x')=x')\rightarrow(x'=c));\ \varepsilon\equiv(\forall x'(\forall x(f_2(x, x')=f_2(x', x))))$$

Nous allons examiner si (E_1, J_1) satisfait certaines de ces formules pour la spécialisation s_1.

2.2.18.0 Est-ce que $(E_1, J_1)\models\alpha[s_1]$?

La réponse est oui *ssi* $(s_1(x), s_1(c))\in\tilde{R}_2$. Dans ce cas, $(s_1(x), s_1(c))=(u, u)\in\tilde{R}_2$. La réponse est donc oui.

2.2.18.1 Est-ce que $(E_1, J_1)\models\beta[s_1]$?

La réponse est oui *ssi* $\tilde{f}_2(s_1(x), s_1(c))=s_1(x)$.
Ici, $\tilde{f}_2(s_1(x), s_1(c))=\tilde{f}_2(u, u)=u$ et $s_1(x)=u$. La réponse est oui.

2.2.18.2 Est-ce que $(E_1, J_1)\models\gamma[s_1]$?

La réponse est oui *ssi* $s_1(x')=s_1(c)$.
Or $s_1(x')=v$ et $s_1(c)=u$. La réponse est donc non. Autrement dit, $(E_1, J_1)\models(\neg\gamma)[s_1]$.

2.2.18.3 Est-ce que $(E_1, J_1)\models\delta[s_1]$?

La réponse est oui *ssi* $s_1(x')=s_1(c)$ *ou* $\tilde{f}_2(s_1(x'), s_1(x'))\neq s_1(x')$.
Or, $\tilde{f}_2(s_1(x'), s_1(x'))=\tilde{f}(v, v)=w$ et $s_1(x')=v$. Donc la deuxième éventualité est vérifiée; la réponse est oui.

2.2.18.4 Est-ce que $(E_1, J_1) \models \varepsilon[s_1]$?

La réponse est oui *ssi*, pour tout a dans E_1:

$(E_1, J_1) \models (\forall x(f_2(x, x') = f_2(x', x))[s_1 \left(\frac{x'}{a}\right)]$. Cela a lieu *ssi*, pour tout b dans E_1 et tout a dans E_1:

$$(E_1, J_1) \models (f_2(x, x') = f_2(x', x))[s_1 \left(\frac{x}{a}\right) \left(\frac{x'}{b}\right)].$$

Notons s^* la spécialisation $s_1\left(\frac{x}{b}\right) \left(\frac{x'}{a}\right)$ (ou mieux $(s_1\left(\frac{x}{b}\right)) (\left(\frac{x'}{a}\right))$)

$$\tilde{f}_2(s^*(x), s^*(x')) = \tilde{f}_2(b, a) \text{ et } \tilde{f}_2(s^*(x'), s^*(x)) = \tilde{f}_2(a, b).$$

Il suffit d'examiner le tableau donnant $\tilde{f}_2$ pour constater que, pour tout a et tout b dans E, $\tilde{f}_2(b, a) = \tilde{f}_2(a, b)$. La réponse est donc oui.

Dans ce dernier exemple, ε est un énoncé. De plus, le choix de la spécialisation s_1 ne joue aucun rôle. Il s'agit là d'un fait général qui découle de la proposition suivante:

2.2.19 Proposition

Soit L un langage du premier ordre, (E, J) une L-structure et φ une formule de L. Soit s_1 et s_2 deux spécialisations de (E, J) qui coïncident sur $VL(\varphi)$. Alors

$$(E, J) \models \varphi[s_1] \text{ si et seulement si } (E, J) \models \varphi[s_2].$$

2.2.20 Démonstration

Elle repose sur la récurrence selon laquelle sont formées les formules de L. Désignons par A l'ensemble des formules de L qui satisfont la conclusion de la proposition. Nous allons montrer que:

2.2.20.0 A contient les formules atomiques de L

2.2.20.1 Si $\alpha, \beta \in A$ et si $x \in \mathrm{Var}$, alors $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\forall x \alpha) \in A$.

Donc $A = \mathrm{For}(L)$, ce qu'il faut établir.

2.2.20.0 A contient les formules atomiques de L.

Remarquons d'abord que si $t \in \mathrm{Ter}(L)$ et si s_1, s_2 sont deux spécialisations qui coïncident sur l'ensemble des symboles de variables apparaissant dans t, alors $t(s_1)$ et $t(s_2)$ désignent un même élément de E.

i) Si $\varphi \equiv (t_1 = t_2)$, avec $t_1, t_2 \in \mathrm{Ter}(L)$, comme s_1 et s_2 coïncident sur $VL(\varphi)$ par hypothèse, s_1 et s_2 coïncident sur les symboles de variables de t_1 et t_2. Donc $t_1(s_1) = t_1(s_2)$ et $t_2(s_1) = t_2(s_2)$. Par suite, si $t_1(s_1) = t_2(s_1)$, alors $t_1(s_2) = t_2(s_2)$ et réciproquement. D'où: $(E, J) \models \varphi[s_1] \Leftrightarrow (E, J) \models \varphi[s_2]$.

ii) Soit R_m un symbole de relation de L et $t_1, t_2, \ldots, t_m \in \mathrm{Ter}(L)$. Si $\varphi \equiv R_m(t_1, t_2, \ldots, t_m)$, comme s_1 et s_2 coïncident sur $VL(\varphi)$ par hypothèse, elles coïncident sur les symboles de variables de $t_1, t_2, \ldots, t_m$. Donc $(t_1,(s_1), t_2(s_1), \ldots, t_m(s_1)) = (t_1(s_2), t_2(s_2), \ldots, t_m(s_2))$.
Si l'un des membres de cette égalité désigne un élément de $\tilde{R}_m$, il en est de même de l'autre. D'où: $(E, J) \models \varphi[s_1] \Leftrightarrow (E, J) \models \varphi[s_2]$.

2.2.20.1 Si $\alpha, \beta \in A$ et si $x \in \mathrm{Var}$, alors $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\forall x\alpha) \in A$.

i) $\alpha \in A \Rightarrow (\neg\alpha) \in A$
Supposons que les spécialisations s_1 et s_2 coïncident sur $VL((\neg\alpha))$. Elles coïncident donc sur $VL(\alpha)$. Comme $\alpha \in A$, $(E, J) \models \alpha[s_1] \Leftrightarrow (E, J) \models \alpha[s_2]$. Cette dernière assertion est équivalente à: (il est faux que $(E, J) \models \alpha[s_1] \Leftrightarrow$ (il est faux que $(E, J) \models \alpha[s_2]$). Ce qui peut encore s'écrire:
$(E, J) \models (\neg\alpha)[s_1] \Leftrightarrow (E, J) \models (\neg\alpha)[s_2]$.
Donc: $(\neg\alpha) \in A$.

ii) $\alpha, \beta \in A \Rightarrow (\alpha \wedge \beta) \in A$.
Supposons que les spécialisations s_1 et s_2 coïncident sur $VL((\alpha \wedge \beta))$, c'est-à-dire sur $VL(\alpha) \cup VL(\beta)$. Elles coïncident donc sur $VL(\alpha)$ et sur $VL(\beta)$. Comme $\alpha, \beta \in A$, on a:
$\{(E, J) \models \alpha[s_1] \Leftrightarrow (E, J) \models \alpha[s_2]\}$ *et* $\{(E, J) \models \beta[s_1] \Leftrightarrow (E, J) \models \beta[s_2]\}$.
on en déduit immédiatement que:
$\{(E, J) \models \alpha[s_1]$ *et* $(E, J) \models \beta[s_1]\} \Leftrightarrow \{(E, J) \models \alpha[s_2]$ *et* $(E, J) \models \beta[s_2]\}$,
ce qui se note aussi: $(E, J) \models (\alpha \wedge \beta)[s_1] \Leftrightarrow (E, J) \models (\alpha \wedge \beta)[s_2]$.
D'où: $(\alpha \wedge \beta) \in A$.

iii) $(\alpha \in A$ et $x \in \mathrm{Var}) \Rightarrow (\forall x\alpha) \in A$.
Supposons que les spécialisations s_1 et s_2 coïncident sur $VL((\forall x\alpha))$, c'est-à-dire sur $VL(\alpha) - \{x\}$. Alors pour tout $a \in E$, $s_1\left(\dfrac{x}{a}\right)$ et $s_2\left(\dfrac{x}{a}\right)$ coïncident sur $VL(\alpha)$.
Comme $\alpha \in A$, on a, pour tout $a \in E$,
$(E, J) \models \alpha[s_1\left(\dfrac{x}{a}\right)] \Leftrightarrow (E, J) \models \alpha[s_2\left(\dfrac{x}{a}\right)]$.
Ce qui équivaut à: $(E, J) \models (\forall x\alpha)[s_1] \Leftrightarrow (E, J) \models (\forall x\alpha)[s_2]$.
D'où: $(\forall x\alpha) \in A$. □

2.2.21 Corollaire

Les notations étant celles de la proposition 2.2.19, supposons de plus que φ est un énoncé de L. S'il existe une spécialisation s_1 de (E, J) telle que $(E, J) \models \alpha[s_1]$, alors pour toute spécialisation s de (E, J), on a $(E, J) \models \varphi[s]$. Sinon, pour toute spécialisation s de (E, J), $(E, J) \models (\neg\alpha)[s]$.

2.2.22 Convention

Ce corollaire justifie la convention suivante: Si $\varphi \in \mathrm{For}(L)$ est un énoncé, si s est une spécialisation d'une L-structure (E, J) telle que $(E, J) \models \varphi[s]$, on note:

$$(E, J) \models \varphi.$$

2.2.23 Définition

Soit L un langage du premier ordre et (E, J) une L-structure. Soit S un ensemble d'énoncés de L. On dit que (E, J) est *un modèle pour* S si, pour tout énoncé $\varphi \in S$: $(E, J) \models \varphi$.

2.2.24 Exemple

Soit L_3 un langage du premier ordre donné par:

$\mathrm{Cst}(L_3) := \{c\}$; $\mathrm{Fct}(L_3) := \{f_2\}$; $\mathrm{Rel}(L_3) := \emptyset$.

Soit (E_3, J_3) une L_3-structure donnée par:

- $E_3 := \{u, v, w\}$
- $J_3(c) := u$
- $J_3(f_2) := \bar{f}_2 : E_3^2 \to E_3$, fonction exprimée par le tableau suivant:

$$E_3\left\{\begin{array}{c} w \\ v \\ u \end{array}\right. \quad \begin{array}{|c|c|c|} \hline w & u & v \\ \hline v & w & u \\ \hline u & v & w \\ \hline \multicolumn{3}{c}{\underbrace{u \quad v \quad w}_{E_3}} \end{array}$$

Fig. 2.2

Considérons l'ensemble $S = \{\varphi_1, \varphi_2, \varphi_3\}$ d'énoncés de L_3, où:

$$\varphi_1 \equiv (\forall x''(\forall x'(\forall x(f_2(x, f_2(x', x'')) = f_2(f_2(x, x'), x'')))))$$
$$\varphi_2 \equiv (\forall x((f_2(x, c) = x) \wedge (f_2(c, x) = x)))$$
$$\varphi_3 \equiv (\forall x(\exists x'((f_2(x, x') = c) \wedge (f_2(x', x) = c)))).$$

Il est facile de vérifier que $(E_3, J_3) \models \varphi_i$, $i = 1, 2, 3$. (cf. exercices). Donc (E_3, J_3) est un modèle pour S. On dit qu'un modèle de S est un *groupe*; S est formé des *axiomes des groupes*. Plus généralement, on appelle *groupe* tout modèle de S dans un langage du premier ordre comportant un symbole de constante c et un symbole de fonction binaire f_2 (cf. exemple 2.2.3.0).

2.2.25 Exemple

Dans le langage L_2 et avec la L_2-structure (E_1, J_1) de l'exemple 2.2.3.0, considérons l'ensemble d'énoncés $T=\{\psi_1, \psi_2\}$, où

$$\psi_1 \equiv (\forall x'(\forall x((R_2(x, x') \wedge R_2(x', x)) \leftrightarrow (x=x'))))$$
$$\psi_2 \equiv (\forall x''(\forall x'(\forall x((R_2(x, x') \wedge R_2(x', x'')) \rightarrow R_2(x, x'')))))$$

A nouveau on vérifie aisément que $(E_1, J_1) \models \psi_i$, $i=1, 2$. (cf. exercices). Donc (E_1, J_1) est un modèle pour T. Tout modèle de T dans un langage du premier ordre comportant un symbole de relation binaire R_2 est appelé *ensemble ordonné*.

2.2.26 Exemple

Reprenons le cas du village V^{***} évoqué au paragraphe 2.0. Supposons qu'on veuille formaliser la généalogie des hommes de V^{***}; celle-ci pourrait être schématisée dans un diagramme dont voici un fragment:

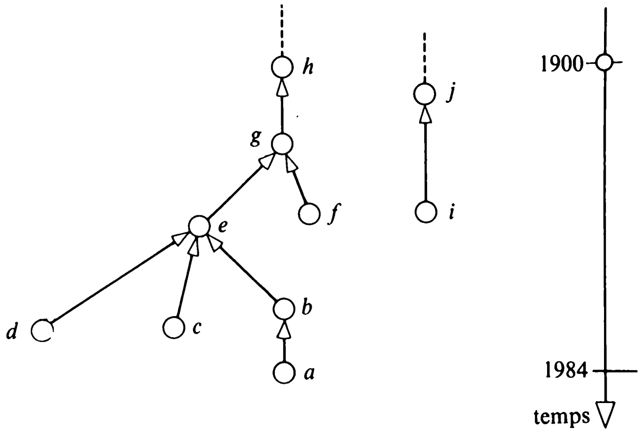


Fig. 2.3

Nous voyons apparaître un graphe orienté. Les sommets forment un ensemble $E_4 := \{a, b, c, d, e, f, g, h, i, j, \ldots\}$ représentant les hommes de V^{***}. Chaque arête orientée figure la correspondance entre un homme de V^{***} et son père (qui appartient aussi à V^{***}, car il s'agit d'un village très isolé). Nous aimerions disposer d'un langage du premier ordre et des énoncés dans ce langage pour lequel le graphe de la figure 2.3 fournisse un modèle.

Proposons-nous de formaliser des phrases telles que: "x est père de y". Chacun n'ayant qu'un seul père, il est assez naturel d'introduire un langage L_4 comportant un symbole de fonction unaire: f_1. Posons alors:

$$J_4(f_1) = \tilde{f}_1 = \{(a, b), (b, e), (c, e), (d, e), (e, g), (f, g), (g, h), (i, j), \ldots\}.$$

En se reportant à la figure 2.3, on constate que pour toute spécialisation s de J_4 et pour tout $x \in \mathrm{Var}$, $s(f_1(x))$ désigne le père de $s(x)$. Le graphe de la figure 2.3 illustre la L_4-structure (E_4, J_4). (E_4, J_4) est aussi un modèle pour l'ensemble vide d'énoncés de L_4.

L'énoncé $\alpha_1 \equiv (\forall x(\neg(f_1(x)=x)))$ s'interprète en disant que personne n'est son propre père. Comme il est facile de le vérifier, α_1 est satisfait dans (E_4, J_4). Donc (E_4, J_4) est un modèle pour $\{\alpha_1\}$.

Toutefois, comme nous l'avons fait dans le § 2.0, nous pourrions préférer avoir à disposition un symbole de relation binaire susceptible d'être interprété par "... est père de ...". Introduisons donc un langage du premier ordre L'_4 comportant un symbole de relation binaire R_2. Posons alors:

$J'_4(R_2) = \{(b, a), (e, b), (e, c), (e, d), (g, e), (g, f), (h, g), (j, i), \ldots\}$. Considérons alors les énoncés:

$\beta_1 \equiv (\forall x(\exists x' R_2(x', x)))$ ("chacun a un père")

$\beta_2 \equiv (\forall x''(\forall x'(\forall x((R_2(x, x'') \wedge R_2(x', x'')) \to (x = x')))))$
("chacun n'a au plus qu'un seul père")

$\beta_3 \equiv (\forall x(\neg R_2(x, x)))$ ("personne n'est son propre père")

Nous laissons au lecteur le soin de vérifier en détail que (E_4, J'_4) est bien un modèle pour $\{\beta_1, \beta_2, \beta_3\}$. Ce modèle est illustré par le graphe de la figure 2.3.

L'énoncé β_3 a la même signification que α_1.

Les énoncés $\{\beta_1, \beta_2\}$ expriment que R_2 a "un caractère fonctionnel". Plus précisément, dans chaque modèle (E, J) de $\{\beta_1, \beta_2\}$, $\tilde{R}_2 \subset E^2$ est le symétrique du graphe d'une fonction. Moyennant l'introduction des énoncés $\{\beta_1, \beta_2\}$, nous pouvons supprimer un symbole de fonction au profit d'un symbole de relation. On constate par là qu'en ce qui concerne les interprétations ensemblistes tout au moins, on pourrait toujours se borner à des langages du premier ordre sans symbole de fonction. C'est ce que font certains auteurs.

2.3 REMARQUES SUR LES ENSEMBLES DÉNOMBRABLES

2.3.0 Considérations élémentaires sur les ensembles

La notion naïve d'ensemble joue un rôle essentiel dans l'idée de structure. Mais elle intervient déjà dans l'étude des formules d'un langage du premier ordre L. Nous savons que toute formule de L est un agrégat fini de signes typographiques. Nous entendons pas là que cette succession de signes peut être effectivement, matériellement écrite. En revanche, il n'est pas possible d'écrire effectivement toutes les formules de L, même quand l'ensemble des symboles propres à L est très réduit. Pour poursuivre notre étude nous devons faire un effort d'imagination et admettre que la totalité des formules de L existe actuellement. C'est ce qu'on traduit en disant que For(L) est un ensemble.

Une situation analogue se présente avec les nombres naturels. On peut commencer à écrire la suite des nombres naturels sous la forme:

( ); (|); (| |); (| | |); (| | | |); ...

chaque parenthèse comportant un bâton de moins que la suivante. On peut aussi employer la notation décimale:

0; 1; 2; 3; 4; ...

Dans les deux cas, chaque nombre naturel se présente comme un agrégat fini de signes typographiques; mais il est impossible d'écrire effectivement tous ces agrégats. Nous admettrons cependant que leur totalité existe. Elle constitue un ensemble que nous noterons $\mathbb{N}$. La notion mathématique d'ensemble a été introduite pour faire face à de telles situations.

Une application $f{:}E \to F$ d'un ensemble E vers un ensemble F est dite

- *injective* si, quels que soient x et y dans E, $(f(x)=f(y))$ implique $x=y$.
- *surjective* si, quel que soit z dans F, il existe x dans E tel que $f(x)=z$.
- *bijective* si elle est à la fois injective et surjective.

Dans ce dernier cas, on dit aussi que f établit une *correspondance biunivoque* entre E et F. L'application réciproque $f^{-1}{:}F \to E$ qui, à tout z dans F, attache le seul élément x de E tel que $f(x)= z$ est aussi bijective.

Un ensemble E est dit *dénombrable* lorsqu'il existe une bijection de $\mathbb{N}$ vers E (ou, ce qui revient au même, de E vers $\mathbb{N}$). Un ensemble E est dit *fini* quand il existe une bijection de E vers une partie effectivement écrite de $\mathbb{N}$. Nous admettrons sans autre forme de procès que toute partie de $\mathbb{N}$ est soit finie, soit dénombrable, ce qu'on exprime aussi en disant qu'elle est *au plus dénombrable.*

N est un ensemble *bien ordonné* en ce sens que l'ordre naturel sur $\mathbb{N}$ est total et que toute partie non vide de $\mathbb{N}$ admet un plus petit élément. On en déduit que s'il existe une application surjective $f{:}\mathbb{N} \to E$ de $\mathbb{N}$ sur un ensemble E, E est au plus dénombrable. En effet, définissons une application

$$\begin{aligned} g:\ & E \to \mathbb{N} \\ & x \mapsto g(x) \end{aligned}$$

où $g(x)$ désigne le plus petit élément de l'ensemble (non vide, par hypothèse) des éléments de $\mathbb{N}$ que f applique sur x. Il est clair que g est injective. Il existe donc une correspondance biunivoque entre E et l'ensemble des valeurs de g, qui est une partie au plus dénombrable de $\mathbb{N}$.

La réunion d'une famille dénombrable d'ensembles dénombrables est dénombrable. Considérons en effet les ensembles dénombrables $(E_i)_{i \in \mathbb{N}}$:

$$
\begin{array}{l}
E_0 = \{a_0^0,\ a_0^1,\ a_0^2,\ a_0^3,\ldots.,a_0^n,\ldots\} \\
E_1 = \{a_1^0,\ a_1^1,\ a_1^2,\ a_1^3,\ldots.,a_1^n,\ldots\} \\
E_2 = \{a_2^0,\ a_2^1,\ a_2^2,\ a_2^3,\ldots.,a_2^n,\ldots\} \\
\vdots \\
E_i = \{a_i^0,\ a_i^1,\ a_i^2,\ a_i^3,\ldots.,a_i^n,\ldots\} \\
\vdots \qquad \vdots \qquad\qquad \vdots
\end{array}
$$

On peut facilement déterminer une surjection de $\mathbb{N}$ sur $\bigcup\limits_{i\in\mathbb{N}} E_i$: il suffit de numéroter les a_i^n selon le diagramme suivant:

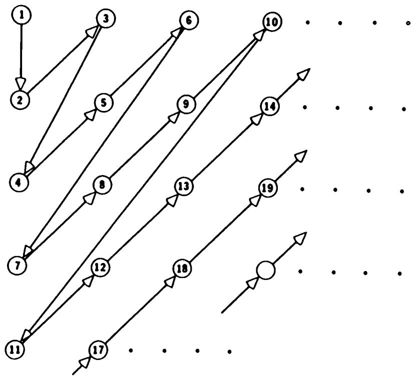


Fig. 2.4

en suivant les flèches. Donc $\bigcup\limits_{i\in\mathbb{N}} E_i$ est au plus dénombrable. Mais comme il contient E_0, il n'est pas fini. Il est donc dénombrable. On déduit immédiatement de là que la réunion d'une famille finie non vide d'ensembles dénombrables est dénombrable.

Un raisonnement analogue montre que la réunion d'une famille dénombrable d'ensembles finis non vides et disjoints est dénombrable:

$$
\begin{array}{llllll}
a_0^0 & a_0^1 & a_0^2 & & & \\
a_1^0 & a_1^1 & a_1^2 & a_1^3 & & \\
a_2^0 & & & & & \\
a_3^0 & a_3^1 & a_3^2 & a_3^3 & a_3^4 & a_3^5 \\
a_4^0 & a_4^1 & a_4^2 & a_4^3 & & \\
a_5^0 & \ldots & & & & \\
\vdots & & & & &
\end{array}
$$

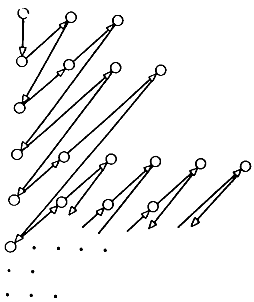


Fig. 2.5

2.3.1 Langages du premier ordre "élémentaires"

Revenons aux langages du premier ordre.

La logique élémentaire, qui est l'objet principal de cet exposé, ne s'intéresse qu'aux formules qu'on peut – ou qu'une machine peut – effectivement écrire. Cela impose quelques restrictions à l'ensemble des symboles utilisés.

Prenons un langage du premier ordre L, "élémentaire" au sens qui vient d'être évoqué. Il comporte un nombre fini de symboles logiques et de symboles de ponctuation. Les symboles de variables peuvent s'écrire:

$$x \quad x' \quad x'' \quad x''' \quad \ldots$$

ce qui revient à les numéroter. Ils constituent donc un ensemble dénombrable.

Passons aux symboles propres à L. Cst(L) peut éventuellement être fini. Lorsqu'il ne l'est pas, on doit pouvoir écrire chaque symbole de constante. Leur suite se présente alors ainsi:

$$c \quad c' \quad c'' \quad c''' \quad \ldots$$

Donc, Cst(L) est au plus dénombrable.

En ce qui concerne les symboles de fonctions, nous avons vu que nous pouvions faire l'économie des indices numériques décimaux et noter par exemple $f'',{}'''$ au lieu de f_3''(cf. fin du Chap. 1). Les symboles de fonctions peuvent dès lors être rangés dans un tableau:

$$\begin{array}{lllll}
f,' & f',' & f'',' & f''',' & \ldots\ldots. \\
f,'' & f','' & f'','' & f''','' & \ldots\ldots. \\
f,''' & f',''' & f'',''' & \ldots\ldots. & \\
\ldots\ldots. & & & &
\end{array}$$

qui fait apparaître une famille finie ou dénombrable d'ensembles disjoints finis ou dénombrables. Donc Fct(L) est au plus dénombrable. On montre de la même manière que Rel(L) est au plus dénombrable.

Par suite, l'ensemble des symboles propres à L est fini ou dénombrable et l'***ensemble de tous les symboles de L est toujours dénombrable***.

Cela vaut pour tous les langages du premier ordre "élémentaires", c'est-à-dire pour lesquels chaque formule peut être effectivement écrite, éventuellement par une machine assez puissante. ***C'est dans ce cas que nous placerons par la suite***, sauf mention expresse du contraire. Nous réserverons toutefois un chapitre ultérieur à des langages du premier ordre moins élémentaires dont l'ensemble des symboles pourrait ne pas être dénombrable.

Revenons, comme convenu, aux langages du premier ordre "élémentaires". Nous pouvons établir une proposition utile:

2.3.2 Proposition

Soit L un langage du premier ordre. L'ensemble For(L) des formules de L est dénombrable.

2.3.3 Démonstration

Lorsqu'on fait usage des notations rappelées ci-dessus, tous les symboles et, partant, toutes les formules de L peuvent s'écrire à l'aide de seize signes:

$$\neg \quad \wedge \quad \vee \quad \rightarrow \quad \leftrightarrow \quad = \quad (\quad , \quad) \quad \forall \quad \exists \quad c \quad x \quad f \quad R \quad '$$

Par exemple, le symbole de relation $R'','''$ est un agrégat de sept signes.

Appelons For(n, L) l'ensemble des formules comportant exactement n signes. Il est facile de s'assurer que For(1, L), For(2, L), For(3, L) et For(4, L) sont vides.
En revanche:

- $\{(x=x)\}\subset \text{For}(5, L)\subset\{(x=x), (c=x); (x=c); (c=c)\}$
- $\{(x'=x); (x=x'); R,'(x)\}\subset \text{For}(6, L)\subset$
  $\subset\{(x'=x); (x=x'); (x'=c); (c=x'); (x=c'), (c'=x); (c'=c); (c=c'); R,'(x); R,'(c)\}$

Pour $n>4$, For(n, L) n'est pas vide; il contient au moins la formule $(x=x\underbrace{'''' \cdots '}_{n-5})$.
De plus, il est fini, car l'ensemble des agrégats de n de nos seize signes comporte 16^n éléments; For(n, L), étant une partie de cet ensemble, est *a fortiori* fini. Ainsi, For(L) est la réunion $\bigcup_{n>4}\text{For}(n, L)$ d'une famille dénombrable d'ensembles finis disjoints non vides: c'est un ensemble dénombrable. □

2.3.4 Corollaire

For(L) peut être muni d'un bon ordre.

2.3.5 Démonstration

For(L) étant dénombrable, on peut établir une bijection de $\mathbb{N}$ sur For(L). Désignons par α_n la formule ainsi attachée au nombre naturel n. Donc:

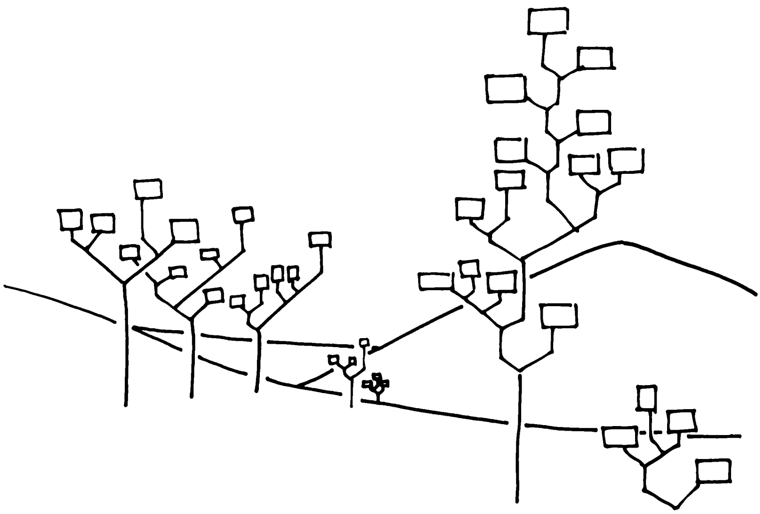
$$\text{For}(L)=\{\alpha_0, \alpha_1, \alpha_2, \ldots \alpha_n, \ldots\}.$$

Transportons à For(L) le bon ordre naturel sur $\mathbb{N}$ en posant: $\alpha_p \leqq \alpha_q$ *ssi* $p \leqq q$. Il est clair que For(L) est bien ordonné par cette relation. □

La présence d'un bon ordre sur For(L) permet d'y effectuer des démonstrations et des constructions par *induction complète* ou, comme on dit aussi, par *récurrence*, à l'instar de ce qui se fait sur $\mathbb{N}$. Si on veut attacher à chaque formule α_n de L une opération $\Omega(\alpha_n)$ – démonstration ou construction – il convient:

1° de décrire $\Omega(\alpha_0)$
2° de décrire $\Omega(\alpha_p)$ dans l'hypothèse où on dispose de $\Omega(\alpha_k)$ pour tout $k<p$.

Cette procédure apparaîtra par la suite.



CHAPITRE 3

La logique (ou calcul) des propositions. Les fonctions de vérité

3.0 INTRODUCTION

Revenons maintenant à l'étude syntaxique des langages du premier ordre. Soit L l'un d'eux. Nous savons reconnaître, en principe, si un agrégat de signes est une formule de L, c'est-à-dire un élément de For(L). Mais nous n'en savons guère plus.

Faisons une comparaison. Il est facile de discerner si un agrégat de signes appartient ou non à l'ensemble $R[x]$ des polynômes en x à coefficients réels. Mais la notion même de polynôme en x apparaît beaucoup plus clairement quand on sait comment les éléments de $R[x]$ se comportent vis-à-vis de l'addition, de la multiplication ou d'autres opérations encore. Le calcul élémentaire des polynômes en x est l'étude de $(R[x], +, \cdot)$, c'est-à-dire de l'ensemble des polynômes en x à coefficients réels, muni de l'addition et de la multiplication.

Il existe de même une sorte de calcul dans For(L). Mais nous ne considérons d'abord qu'une partie des opérations possibles: celles qui sont déterminées par les *connecteurs*, à l'exception du symbole $=$. Si α et β sont des formules de L, $(\neg\alpha)$, $(\alpha\wedge\beta)$, $(\alpha\to(\neg\beta))$ sont aussi des formules de L. Cette algèbre présente de grandes analogies avec la combinaison des phrases ou propositions de la langue courante. Si A désigne "il pleut" et si B désigne "nous allons à bicyclette", $(\neg A)$, $(A\wedge B)$, $(A\to(\neg B))$ – qui se lisent (non A), (A *et* B), (si A alors non B)) – désignent dans l'ordre: "il ne pleut pas", "il pleut et nous allons à bicyclette", "s'il pleut, alors nous n'allons pas à bicyclette". C'est pourquoi la logique des connecteurs s'appelle aussi *logique* ou *calcul* des *propositions*.

Cette partie de la logique s'applique à tout langage formel comportant les connecteurs $\neg$, $\wedge$, $\vee$, $\to$ et $\leftrightarrow$, pour autant qu'ils soient gouvernés par les règles de formation que nous avons posées au Chap. 1. Elle ne prend pas en compte le symbole $=$ ni les quantificateurs, lorsqu'il y en a. La logique des propositions n'est donc pas partie intégrante de la seule logique du premier ordre. Néanmoins, c'est aux langages du premier ordre que nous comptons l'appliquer et nous nous intéresserons à (For(L), $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$).

3.1 DÉFINITIONS ET PROPRIÉTÉS ÉLÉMENTAIRES

3.1.0 Préambule

Dans ce paragraphe, L désigne un langage du premier ordre donné une fois pour toutes.

Lorsqu'on combine les formules atomiques de L à l'aide des connecteurs, on n'obtient pas de formule comportant un ou plusieurs quantificateurs. Si on désire obtenir toutes les formules de L, il faut partir d'un ensemble de "générateurs" plus grand, qui fait l'objet de la définition suivante:

3.1.1 Définition

Les formules premières de L sont:

i) les formules atomiques de L

ii) les formules de L commençant par $(\forall$ ou $(\exists$.

Nous noterons $P(L)$ l'ensemble des formules premières de L.

Pour préciser comment les formules de L sont engendrées à partir des formules premières de L, posons la définition suivante qui a une portée très générale:

3.1.2 Définition

Soit E un ensemble non vide quelconque.

On appelle *forme propositionnelle* sur E (ou construite à partir de E) toute expression obtenue selon les règles suivantes:

i) Si $A \in E$, A est une forme propositionnelle sur E.

ii) Si A et B sont des formes propositionnelles sur E $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ et $(A \leftrightarrow B)$ aussi.

iii) Il n'y a pas d'autres formes propositionnelles sur E que celles qui découlent des règles i) et ii).

Nous noterons $\Phi(E)$ l'ensemble des formes propositionnelles sur E.

La définition 1.0.8 permet d'énoncer immédiatement:

3.1.3 Proposition

Les formules de L sont les formes propositionnelles construites à partir de l'ensemble des formules premières de L. Autrement dit:

$$\mathrm{For}(L) = \Phi(P(L))$$

3.1.4 Remarque

La définition 3.1.2 s'appuie sur la remarque 2.1.14. Lorsqu'on considère les formes propositionnelles sur un ensemble E, les éléments de E n'admettent *a priori* aucune désignation spéciale. Si on veut en choisir une, elle ne doit engendrer aucune confusion avec les règles de la définition 3.1.2. Par exemple, si E comporte au moins deux éléments, on ne choisirait pas de les noter a et $(\neg a)$. On ne pourrait plus distinguer entre l'élément "premier" $(\neg a)$ et la forme propositionnelle $(\neg a)$ construite selon la règle ii) à partir de l'élément "premier" a. Les expressions fabriquées de la sorte n'obéiraient plus à la condition d'unique lisibilité.

3.1.5 Remarque

Soit E un ensemble non vide et A une forme propositionnelle sur E. En spéculant sur les parenthèses comme nous l'avons fait pour les termes et les formules de L (cf. prop. 1.0.23), on peut affirmer l'existence d'un unique "*arbre de composition*" de A à partir d'éléments de E. En particulier, toute formule φ de L admet un unique *arbre de composition* à partir de formules premières de L, appelées *composantes premières* de φ.

3.1.6 Exemple

Soit α, β, γ, δ des formules atomiques de L et soit $\varphi \in \mathrm{For}(L)$ donnée par:

$$\varphi :\equiv ((\exists x(\alpha \wedge \beta)) \vee ((\neg(\forall x'\gamma)) \rightarrow \delta))$$

avec $x, x' \in \mathrm{Var}$. Son arbre de formation est représenté par la figure 3.0, et son arbre de composition par la figure 3.1:

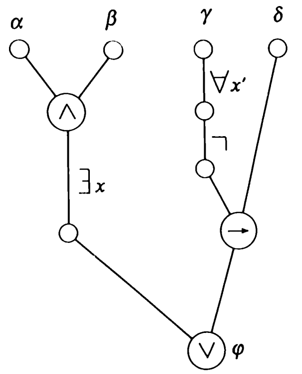


Fig. 3.0

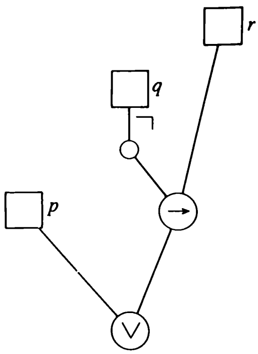


Fig. 3.1

où $p :\equiv (\exists x(\alpha \wedge \beta))$, $q :\equiv (\forall x'\gamma)$ et $r :\equiv \delta$ sont les composantes premières de φ.

3.1.7 Motivation

Passons maintenant à la notion de “fonction de vérité” que nous allons essayer de motiver. Soit (E, J) une L-structure et s une spécialisation de (E, J). φ étant une formule de L, ou bien $(E, J)\models\varphi[s]$, ou bien il est faux que $(E, J)\models\varphi[s]$. Décidons d'associer à φ le nombre $V_s(\varphi)$ déterminé par:

$$V_s(\varphi) := \begin{cases} 1 \text{ si } (E, J)\models\varphi \\ 0 \text{ sinon.} \end{cases}$$

Les propriétés suivantes de la fonction V_s:For$(L)\to\{0, 1\}$ découlent immédiatement de la définition 2.2.11:

a) $V_s((\neg\varphi)) \neq V_s(\varphi)$
b) $V_s((\varphi\wedge\psi)) = 1$ *ssi* $V_s(\varphi) = V_s(\psi) = 1$
c) $V_s((\varphi\vee\psi)) = 0$ *ssi* $V_s(\varphi) = V_s(\varphi) = 0$
d) $V_s((\varphi\to\psi)) = 1$ *ssi* $\{V_s(\varphi) = 0$ *ou* $V_s(\psi) = 1\}$
e) $V_s((\varphi\leftrightarrow\psi)) = 1$ *ssi* $V_s(\varphi) = V_s(\psi)$

quelles que soient φ, $\psi\in$For(L).

Vérifions d) par exemple:

$$\begin{aligned} V_s((\varphi\to\psi)) = 1 &\Leftrightarrow (E, J)\models(\varphi\to\psi)[s] \Leftrightarrow \\ &\Leftrightarrow \{(E, J)\models\psi[s] \text{ ou il est faux que } (E, J)\models\varphi[s]\} \Leftrightarrow \\ &\Leftrightarrow \{V_s(\psi) = 1 \text{ ou } V_s(\varphi = 0\} \Leftrightarrow \\ &\Leftrightarrow \{V_s(\varphi) = 0 \text{ ou } V_s(\psi) = 1\}. \end{aligned}$$

Ainsi, il suffit de connaître $V_s(\varphi)$ et $V_s(\psi)$ pour savoir évaluer V_s en $(\neg\varphi)$, $(\varphi\wedge\psi)$, $(\varphi\vee\psi)$, $(\varphi\to\psi)$ et $(\varphi\leftrightarrow\psi)$. Nous sommes conduits à la définition suivante:

3.1.8 Définition

Soit E un ensemble non vide. Une *fonction de vérité* V_s sur l'ensemble $\Phi(E)$ des formes propositionnelles sur E est une application V:$\Phi(E)\to\{0; 1\}$ satisfaisant les conditions portées dans le tableau suivant:

$V(A)$	$V(B)$	$V((\neg A))$	$V((A\wedge B))$	$V((A\vee B))$	$V((A\to B))$	$V((A\leftrightarrow B))$
0	0	1	0	0	1	1
0	1		0	1	1	0
1	0	0	0	1	0	0
1	1		1	1	1	1

Fig. 3.2

où A et B sont des éléments quelconques de $\Phi(E)$.

3.1.9 Remarque

Il résulte de l'unique lisibilité de chaque forme propositionnelle sur E que toute fonction de vérité sur $\Phi(E)$ est essentiellement déterminée par ses valeurs sur E; plus précisément, pour toute application $\mu:E\to\{0;\ 1\}$, il existe une unique fonction de vérité $V:\Phi(E)\to\{0;1\}$ telle que $V|_E=\mu$.

Par exemple, si $E=\{a, b, c\}$, si $\mu(a)=1$ et $\mu(b)=\mu(c)=0$, et si $F:\equiv(a\wedge((\neg b)\to c))\in\Phi(E)$, on obtient successivement:

$$V((\neg b))=1;\ V(((\neg b)\to c))=0 \text{ et } V(F)=0.$$

La proposition suivante est presque immédiate:

3.1.10 Proposition

Soit s une spécialisation d'une L-structure (E, J). Il existe une unique fonction de vérité V_s sur For(L), dite "associée à s", telle que, pour toute formule φ de L:

$$(E, J)\models\varphi[s] \quad ssi \quad V_s(\varphi)=1.$$

3.1.11 Démonstration

Considérons la fonction:

$$V_s:\mathrm{For}(L)\to \{0;\ 1\}$$
$$\varphi \mapsto \begin{cases} 1 \text{ si } (E, J)\models\varphi[s] \\ 0 \text{ sinon.} \end{cases}$$

V_s est bien une fonction de vérité sur For(L) comme nous l'avons montré en 3.1.7. Cela prouve à la fois l'existence et l'unicité de la fonction de vérité associée à s. □

3.1.12 Calcul des valeurs d'une fonction de vérité

Considérons maintenant un ensemble $E=\{A, B, ...\}$ et une forme propositionnelle $C:\equiv((A\wedge(\neg B))\to B)$; si V est une fonction de vérité sur $\Phi(E)$, on sait déterminer le nombre $V(C)$ à partir des nombres $V(A)$ et $V(B)$ à l'aide de la table de la figure 3.2. Mais on peut aussi se proposer de le trouver par des calculs numériques.

Sur l'ensemble $\{0;\ 1\}$, définissons les deux lois internes $+$ et $\cdot$ suivantes:
$0+0=0;\ 0+1=1+0=1;\ 1+1=0$
$0\cdot 0=0\cdot 1=1\cdot 0=0;\ 1\cdot 1=1.$
Cela revient à calculer avec les nombres entiers ordinaires en ne s'occupant que de leur parité; "pair" est noté 0 et "impair" est noté 1. On reconnaît aussi le corps F_2.

Remarquons que pour tout $a \in \{0;\ 1\}$, $a+a=0$ et $a \cdot a=a$.
On vérifie alors facilement les relations suivantes:
a) $V((\neg A))=1+V(A)$
b) $V((A \wedge B))=V(A) \cdot V(B)$
c) $V((A \vee B))=V(A)+V(B)+V(A) \cdot V(B)$
d) $V((A \rightarrow B))=1+V(A)+V(A) \cdot V(B)$
e) $V((A \leftrightarrow B))=1+V(A)+V(B)$

Vérifions d) par exemple:

- si $V(A)=0$, $V((A \rightarrow B))=1$ et $1+V(A)+V(A) \cdot V(B)=1+0+0=1$
- si $V(A)=1$ et $V(B)=0$, $V((A \rightarrow B))=0$ et $1+V(A)+V(B)=1+1+0=0$
- si $V(A)=V(B)=1$, $V((A \rightarrow B))=1$ et $1+V(A)+V(A) \cdot V(B)=1+1+1=1$.

Lorsqu'on applique ces règles à $C \equiv ((A \wedge (\neg B)) \rightarrow B)$, on constate que: $V(C)=1+V(A)+V(A) \cdot V(B)$. Quelle qu'elle soit, la fonction de vérité V prend les mêmes valeurs en C et en $(A \rightarrow B)$. Ce genre de calcul va apparaître dans l'exemple suivant:

3.1.13 Exemple

Soit $E=\{A,\ B,\ ...\}$ un ensemble quelconque; soit V une fonction de vérité quelconque sur $\varphi(E)$. Calculer $V(D)$ où

$$D:\equiv((A \rightarrow B) \rightarrow (((\neg A) \rightarrow B) \rightarrow B)). \tag{3.0}$$

Pour simplifier l'écriture, posons:

$F:\equiv(A \rightarrow B)$, $G:\equiv((\neg A) \rightarrow B)$, $H:\equiv(G \rightarrow B)$
$a:=V(A)$ et $b:=V(B)$.

Alors
$$\begin{aligned} V(F)&=1+a+a \cdot b \\ V(G)&=1+(1+a)+(1+a) \cdot b=a+b+a \cdot b \\ V(H)&=1+(a+b+a \cdot b)+(a+b+a \cdot b)b=1+a+a \cdot b. \end{aligned}$$

D'où
$$\begin{aligned} V(D)&=1+V(F)+V(F) \cdot V(H) \\ &=1+(1+a+a \cdot b)+(1+a+a \cdot b)(1+a+a \cdot b) \\ &=1+(1+a+a \cdot b)+(1+a+a \cdot b)=1. \end{aligned}$$

Ainsi, $V(D)=1$ quelle que soit la fonction de vérité V sur $\Phi(E)$. Cela justifie la définition suivante:

3.1.14 Définition

Soit E un ensemble non vide. On dit qu'une forme propositionnelle A sur E est une *tautologie* si, pour toute fonction de vérité V sur $\Phi(E)$, $V(A)=1$.

3.1.15 Remarque

La définition 3.1.14 s'applique en particulier au cas où $E=P(L)$ et $\Phi(E)=$ For(L).

3.1.16 Remarque

Si A est un élément de E, A n'est certainement pas une tautologie, car il existe une fonction de vérité V_0 telle que $V_0(A)=0$, ne fût-ce que celle qui est identiquement nulle sur E.

3.1.17 Remarque

Si, en particulier, x est un symbole de variable du langage du premier ordre L, $(x=x)$ est une formule première de L. Il existe donc au moins une fonction de vérité V_0 sur For(L) telle que $V_0((x=x))=0$. Or pour toute spécialisation s d'une L-structure (F, J), on a: $(F, J)\models(x=x)[s]$, et par conséquent $V_s((x=x))=1$, si V_s est la fonction de vérité associée à s. Ainsi, d'une part $(x=x)$ n'est pas une tautologie de L; d'autre part, la fonction de vérité V_0 attribue la valeur 0 à une formule de L qui est manifestement satisfaite – ou "vraie" – dans toute interprétation. Autrement dit, les V_s n'épuisent pas les fonctions de vérité sur For(L) et la notion de fonction de vérité est trop fruste pour décrire ce qu'on appelle intuitivement la "vérité".

3.1.17 Proposition

Soit E un ensemble non vide. Alors, quelles que soient A et B dans $\Phi(E)$, les formes propositionnelles:

1) $(A \vee (\neg A))$
2) $(\neg(A \wedge (\neg A)))$
3) $((\neg(A \vee B))\leftrightarrow((\neg A) \wedge (\neg B)))$
4) $((\neg(A \wedge B))\leftrightarrow((\neg A) \vee (\neg B)))$
5) $((\neg(\neg A))\leftrightarrow A)$
6) $((A\rightarrow B)\leftrightarrow((\neg B)\rightarrow(\neg A)))$

sont des tautologies.

3.1.18 Démonstration

Soit V une fonction de vérité quelconque sur $\Phi(E)$. Pour alléger l'écriture, posons $a:=V(A)$ et $b:=V(B)$; pour tout entier naturel $n\geqq 1$, $na = \underbrace{a+a+\ldots+a}_{\text{n fois}}$.

En vertu des règles de calcul que nous avons vues:

1) $V((A \vee (\neg A))=a+(1+a)+a\cdot(1+a)=1+4a=1$

2) $V((\neg(A \wedge (\neg A)))) = 1 + a \cdot (1+a) = 1 + 2a = 1$

3) $V(((\neg(A \vee B)) \leftrightarrow ((\neg A) \vee (\neg B)))) = 1 + (1 + a + b + a \cdot b) + (1+a) \cdot (1+b) =$
$= 1 + 2(1 + a + b + a \cdot b) = 1$

4) $V(((\neg(A \wedge B)) \leftrightarrow ((\neg A) \vee (\neg B)))) = 1 + (1 + a \cdot b) +$
$+ (1+a) + (1+b) + (1+a) \cdot (1+b) =$
$= a \cdot b + a + b + (1 + a + b + a \cdot b) = 1$

5) $V(((\neg(\neg A)) \leftrightarrow A)) = 1 + (1 + (1+a)) + a = 1$

6) $(((A \rightarrow B) \leftrightarrow ((\neg B) \leftrightarrow (\neg A)))) = 1 + (1 + a + a \cdot b) + (1 + (1+b) + (1+b) \cdot (1+a)) =$
$= (a + a \cdot b) + b + (1 + a + b + a \cdot b) = 1.$ □

3.1.19 Nomenclature

Les assertions selon lesquelles les formes propositionnelles 1) à 6) sont des tautologies sont traditionnellement désignées ainsi:
1) est le “principe du tiers exclu”
2) est le “principe de non-contradiction”
3) et 4) sont les “lois de De Morgan”
5) est le “principe de la double négation”
6) est le “principe de contraposition”.

3.1.20 Remarque

Remarquons en passant que la définition des fonctions de vérité a été posée en accord avec la définition 2.2.11. A son tour celle-ci, qui régit la satisfaction d'une formule dans une spécialisation d'une L-structure, est compatible avec le fait que $\vee$, $\rightarrow$ et $\leftrightarrow$ peuvent être considérées comme des abréviations. Il en est donc de même des propriétés des fonctions de vérité. Cela apparaît au travers des tautologies 3) et 5).

3.1.21 Remarque

Malgré leur nom, les fonctions de vérité ne permettent pas de savoir si une formule est “vraie”, comme nous l'avons déjà remarqué. En revanche, quelle que soit la formule $\alpha \in \mathrm{For}(L)$, aucune fonction de vérité sur $\mathrm{For}(L)$ ne prend la valeur 1 ***à la fois*** sur α et sur $(\neg\alpha)$. D'une manière purement formelle, α et $(\neg\alpha)$ sont incompatibles. Lorsque deux formules α et β de L sont telles qu'il existe une fonction de vérité sur $\mathrm{For}(L)$ valant 1 sur α et sur β, on peut dire qu'elles ne sont pas formellement incompatibles. C'est là une condition assez faible qui fait l'objet de la définition suivante:

3.1.22 Définition

Soit E un ensemble non vide et $S \subset \Phi(E)$ un ensemble de formes propositionnelles sur E. On dit que S est *consistant pour la logique des propositions* ou

LP-consistant s'il existe une fonction de vérité sur $\Phi(E)$ valant 1 sur chaque élément de S. Une forme propositionnelle $A \in \Phi(E)$ est dite *LP-consistante* si $\{A\}$ est LP-consistant.

3.1.23 Exemple

Soit A, $B \in \Phi(E)$ et V une fonction de vérité sur $\Phi(E)$ telle que $V(A)=1$ et $V((A \rightarrow B))=1$. Alors $V(B)=1$ en vertu de la définition 3.1.8. Donc, si $\{A, (A \rightarrow B)\}$ est LP-consistant, $\{A, (A \rightarrow B), B\}$ l'est aussi.

3.1.24 Exemple

Soit un ensemble de formules $S \subset \Phi(P(L)) = \mathrm{For}(L)$; s'il existe une spécialisation s d'une L-structure (E, J) telle que $(E, J) \models \varphi[s]$ pour chaque φ de S, alors S est LP-consistant. En effet, si V_s est la fonction de vérité à S, $V_s(\varphi)=1$ pour chaque φ de S.

3.1.25 Proposition

La proposition suivante n'est qu'un cas particulier de l'exemple 3.1.24:

Soit L un langage du premier ordre et soit S un ensemble d'énoncés de L. Si S admet un modèle (E, J), alors S est LP-consistant.

3.1.26 Démonstration

Soit s une spécialisation quelconque de (E, J) et V_s la fonction de vérité associée à s. Comme S est constitué par des énoncés de L, $(E, J) \models \varphi[s]$ pour tout $\varphi \in S$. Donc $V_s(\varphi)=1$ pour tout $\varphi \in S$. □

3.1.27 Remarque

La réciproque de la proposition 3.1.26 est fausse. Ainsi, l'énoncé $(\exists x(\neg(x=x)))$ est une formule première de L. Il est donc LP-consistant; toutefois, il n'admet aucun modèle.

3.1.28 Remarque

Soit E un ensemble non vide quelconque. Si S est une partie LP-consistante de $\Phi(E)$, toute partie S' de S l'est aussi. En particulier, toute partie *finie* de S est LP-consistante. La proposition qui va suivre exprime que la réciproque est vraie dans le cas où $E=P(L)$.

Pour abréger, nous dirons que $S \subset \Phi(E)$ est de *LP-consistance finie* lorsque toute partie finie de S est LP-consistante.

3.1.29 Proposition: théorème de compacité de la logique des propositions

Soit L un langage du premier ordre et soit S une partie de For(L). S est LP-consistante si et seulement si S est de LP-consistance finie.

3.1.30 Démonstration

La nécessité de la condition découle de la remarque 3.1.28 ci-dessus. Pour démontrer la suffisance de cette condition, nous allons établir un résultat apparemment plus fort: si S est de LP-consistance finie, alors elle est contenue dans une partie $T \subset$ For(L) qui est LP-consistante. Nous allons procéder en trois étapes.

3.1.31 Lemme

Soit $S \subset$ For(L) de LP-consistance finie. Pour toute formule $\varphi \in$ For(L), l'un au moins des deux ensembles $S \cup \{\varphi\}$ et $S \cup \{(\neg\alpha)\}$ est de LP-consistance finie.

3.1.32 Démonstration du lemme 3.1.31

Supposons que $S \cup \{\varphi\}$ et $S \cup \{(\neg\varphi)\}$ ne sont ni l'une ni l'autre de LP-consistance finie et montrons que cette hypothèse conduit à une contradiction. En effet, S étant elle-même de LP-consistance finie, il existe $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_p$ dans S tels que:

$$\{\alpha_1, \alpha_2, \ldots, \alpha_n, \varphi\} \text{ et } \{\beta_1, \beta_2, \ldots, \beta_p, (\neg\varphi)\} \text{ ne sont pas } LP\text{-consistants} \quad (3.1)$$

Comme $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_p\}$ est LP-consistant en tant que partie finie de S, il existe une fonction de vérité V sur For(L) telle que: $V(\alpha_i)=1$ pour $i=1, 2, \ldots, n$ et $V(\beta_k)=1$ pour $k=1, 2, \ldots, p$. Comme $V(\varphi) \neq V(\neg\varphi)$, l'un de ces deux membres égale 1 et, par suite, l'un des deux ensembles $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \varphi\}$, $\{\beta_1, \beta_2, \ldots, \beta_p, (\neg\varphi)\}$ est LP-consistant: cela contredit (3.1). □

3.1.33 Lemme

Soit $S \subset$ For(L) de LP-consistance finie. Alors S est contenue dans un ensemble $T \subset$ For(L) tel que:

a) T est de LP-consistance finie.

b) T est maximal en ce sens que pour tout $\varphi \in$ For(L), soit $\varphi \in T$, soit $(\neg\varphi) \in T$.

3.1.34 Démonstration du lemme 3.1.33

En vertu du corollaire 2.3.4, munissons For(L) d'un bon ordre noté $\leqq$. Si $\alpha, \beta \in$For(L), nous noterons $\beta < \alpha$ lorsque $\beta \leqq \alpha$ et $\beta \neq \alpha$. Construisons par induction une partie T_α de For(L) pour chaque formule α de L.

Soit α_0 le plus petit élément de For(L). Si $S \cup \{\alpha_0\}$ est de LP-consistance finie, posons: $T_{\alpha_0} := S \cup \{\alpha_0\}$. Sinon $S \cup \{(\neg \alpha_0)\}$ est de LP-consistance finie en vertu du lemme 3.1.31 et nous posons: $T_{\alpha_0} := S \cup \{(\neg \alpha_0)\}$.

Soit $\alpha \in$For(L) telle que:

i) pour tout $\beta \in$For(L) telle que $\beta < \alpha$, T_β soit construit

ii) pour tout $\beta \in$For(L) telle que $\beta < \alpha$, T_β soit de LP-consistance finie.

iii) pour toutes β, $\gamma \in$For(L) telles que $\beta < \gamma < \alpha$, $T_\beta \subset T_\gamma$.

Ces conditions sont banalement satisfaites quand $\alpha \equiv \alpha_0$.

L'ensemble $\bigcup\limits_{\beta<\alpha} T_\beta$ est de LP-consistance finie. Sinon il existerait $\{\delta_1, \delta_2, \dots, \delta_p\} \subset \bigcup\limits_{\beta<\alpha} T_\beta$ qui ne serait pas LP-consistant, avec $\delta_1 \in T_{\beta_1}$, $\delta_2 \in T_{\beta_2}, \dots, \delta_p \in T_{\beta_p}$; si β_m est le plus grand des éléments $\beta_1, \beta_2, \dots, \beta_p$, $\{\delta_1, \delta_2, \dots, \delta_p\}$ serait inclus dans T_{β_m} en vertu de iii) et T_{β_m} ne serait pas de LP-consistance finie, ce qui contredirait ii).

Si $(\bigcup\limits_{\beta<\alpha} T_\beta) \cup \{\alpha\}$ est de LP-consistance finie, nous posons: $T_\alpha := (\bigcup\limits_{\beta<\alpha} T_\beta) \cup \{\alpha\}$. Sinon, nous posons $T_\alpha := (\bigcup\limits_{\beta<\alpha} T_\beta) \cup \{(\neg \alpha)\}$ qui est de LP-consistance finie. Il est manifeste que si α^* désigne le successeur immédiat de α, les conditions i), ii) et iii) sont satisfaites quand on y remplace α par α^*.

Posons enfin: $T := \bigcup\limits_{\alpha \in \mathrm{For}(L)} T_\alpha$. On a bien $S \subset T$. Vérifions alors que T satisfait les conditions a) et b).

a) Soit $\beta_1, \beta_2, \dots, \beta_m$ dans T. Comme les ensembles T_α sont emboîtés en vertu de iii) – c'est-à-dire que $\beta < \gamma$ implique $T_\beta < T_\gamma$ – il existe $\delta \in$For(L) tel que $\{\beta_1, \beta_2, \dots, \beta_m\} \subset T_\delta$. Comme T_δ est de LP-consistance finie par construction, $\{\beta_1, \beta_2, \dots, \beta_m\}$ est LP-consistant.

b) Pour tout $\varphi \in$For(L), on a par construction $\varphi \in T_\varphi \subset T$ ou $(\neg \varphi) \in T_\varphi \subset T$. Comme $\{\varphi, (\neg \varphi)\}$ n'est pas LP-consistant, chacune de ces éventualités exclut l'autre.

□

3.1.35 Lemme

Soit $S \subset$For(L) de LP-consistance finie. Si $T \subset$For(L) est un ensemble contenant S et satisfaisant les conditions a) et b) du lemme 3.1.33, alors T est LP-consistant.

3.1.36 Démonstration du lemme 3.1.35

Nous allons même montrer qu'il existe une fonction de vérité V sur For(L) qui vaut 1 pour toutes les formules de L appartenant à T et pour celles-là seulement. Comme nous l'avons remarqué à la suite de la définition 3.1.8, V est déterminé lorsqu'on donne ses valeurs sur l'ensemble $P(L)$ des formules premières de L.

Posons donc:

$$V(\alpha) := \begin{cases} 1 \text{ si } \alpha \in P(L) \cap T \\ 0 \text{ si } \alpha \in P(L) \textit{ et } \alpha \notin T. \end{cases}$$

Montrons que $V(\varphi)=1$ si et seulement si $\varphi \in T$. C'est vrai lorsque φ est première en vertu de la définition de V. Pour obtenir le résultat général, nous procéderons par récurrence sur la "longueur" de φ en tant que forme proportionnelle sur $P(L)$. Conformément à nos conventions d'économie, nous nous bornerons aux connecteurs $\neg$ et $\vee$ (cf. remarque 2.2.16 et convention 2.2.17). Admettons donc qu'on a prouvé $V(\psi)=1 \Leftrightarrow \psi \in T$ pour toutes les formules ψ "plus courtes" que φ.

a) *Cas où* $\varphi \equiv (\neg\alpha)$. Si $(\neg\alpha) \in T$, alors $\alpha \notin T$ (cf. lemme 3.1.33); comme α est plus courte que φ, on a $V(\alpha)=0$. Donc $V((\neg\alpha))=1$. Réciproquement, si $V((\neg\alpha))=1$, alors $V(\alpha)=0$; comme α est plus courte que φ, on a $\alpha \notin T$. Donc $(\neg\varphi) \in T$.

b) *Cas où* $\varphi \equiv (\alpha \wedge \beta)$. Si $(\alpha \wedge \beta) \in T$, alors $\alpha \in T$ *et* $\beta \in T$; sans quoi $\{(\neg\alpha), (\alpha \wedge \beta)\} \subset T$ *ou* $\{(\neg\beta), (\alpha \wedge \beta)\} \subset T$ ce qui est impossible car aucun de ces deux ensembles n'est LP-consistant.Comme α et β sont plus courtes que φ, on a $V(\alpha)=V(\beta)=1$ et, par suite, $V((\alpha \wedge \beta))=1$. Réciproquement, si $V((\alpha \wedge \beta))=1$, alors $V(\alpha)=V(\beta)=1$; comme α et β sont plus courtes que φ, on a $\alpha \in T$ *et* $\beta \in T$. On en déduit que $(\alpha \wedge \beta) \in T$ car $\{\alpha, \beta, (\neg(\alpha \wedge \beta))\}$ n'est pas LP-consistant. □

Avec le lemme 3.1.35 s'achève la démonstration de la proposition 3.1.29. □

■ 3.1.37 Remarque

Il résulte de la remarque 3.1.9 que l'ensemble Λ des fonctions de vérité sur $\mathrm{For}(L)$ peut être identifié à l'ensemble $\{0; 1\}^{P(L)}$ des applications $P(L) \to \{0; 1\}$. $\{0; 1\}$ étant muni de la topologie discrète, munissons Λ de la topologie produit. En vertu du théorème de Tychonoff, Λ est compact.

Pour toute formule $\varphi \in \mathrm{For}(L)$, posons:

$$\Omega_\varphi := \{V \in \Lambda \mid V(\varphi)=1\}.$$

Montrons que Ω_φ est fermé dans Λ.

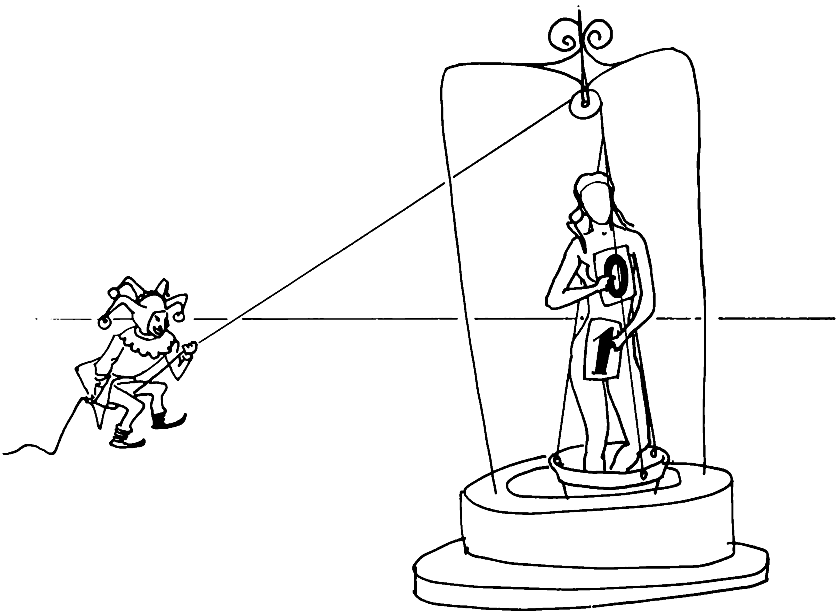
On a: $\Lambda - \Omega_\varphi = \{V \in \Lambda \mid V(\varphi)=0\} = \Omega_{(\neg\varphi)}$. Si φ est première Ω_φ et $\Lambda - \Omega_\varphi$ sont des ouverts élémentaires de Λ. Donc Ω_φ et $\Omega_{\neg\varphi}$ sont fermés. D'autre part, si $\alpha, \beta \in \mathrm{For}(L)$, on a par définition:

$$\Omega_{(\alpha \wedge \beta)} = \Omega_\alpha \cap \Omega_\beta$$
$$\Omega_{(\alpha \vee \beta)} = \Omega_\alpha \cup \Omega_\beta$$
$$\Omega_{(\alpha \rightarrow \beta)} = \Omega_\beta \cup \Omega_{(\neg\alpha)}$$
$$\Omega_{(\alpha \leftrightarrow \beta)} = (\Omega_\beta \cup \Omega_{(\neg\alpha)}) \cap (\Omega_\alpha \cup \Omega_{(\neg\beta)}$$

Donc pour toute formule $\varphi \in \mathrm{For}(L)$, Ω_φ s'obtient par une collection finie de réunions et d'intersections de fermés de Λ. Par suite, Ω_φ est fermé.

Cette observation permet de donner une autre démonstration de la proposition 3.1.29 et de justifier le nom de "théorème de compacité". En effet, soit $S \subset \mathrm{For}(L)$. Dire que S n'est pas LP-consistant revient à dire que $\bigcap_{\varphi \in S} \Omega_\varphi = \emptyset$. Comme Λ est compact, il existe une partie *finie* non vide $F \subset S$ telle que $\bigcap_{\varphi \in F} \Omega_\varphi = \emptyset$, c'est-à-dire telle que F n'est pas LP-consistante.

Il en résulte que S n'est pas de LP-consistance finie. ■



CHAPITRE 4

Les axiomes de l'égalité ou formules de Leibniz

4.0 CONVENTIONS PRÉALABLES

4.0.0 Préambule

Afin d'alléger un peu l'exposé, nous allons adopter dès maintenant quelques simplifications d'écriture. Le principe en est simple. Nous remplacerons certains agrégats de signes par des notations typographiques qui les évoquent sans ambiguïté. Nous avons déjà utilisé ce procédé sans le mentionner expressément. Dire, comme nous l'avons souvent fait, que "α est une formule" est, à proprement parler, abusif. Il faudrait dire que "α est un signe évoquant une certaine formule". La distinction est plus subtile ici que dans d'autres domaines puisque les objets que nous considérons sont eux-mêmes des agrégats de signes.

C'est ainsi que:

4.0.1 Convention

Nous désignerons les symboles de variables x, x', x'', ... par les lettres x, y, z, ... , voire par x_1, x_2, x_3, ...

4.0.2 Convention

Si α, β désignent des formules de L, t_1, t_2 des termes de L, $*$ l'un des symboles $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ et x un symbole de variable, nous désignerons

$(\alpha*\beta)$ par $\alpha*\beta$
$(t_1=t_2)$ par $t_1=t_2$
$(\forall x\alpha)$ par $\forall x\alpha$
$(\exists x\alpha)$ par $\exists x\alpha$

pour autant qu'aucune confusion n'en résulte.

4.0.3 Convention

Si α_1, α_2, α_3, ... , α_n sont des formules de L,
$((\ldots((\alpha_1 \wedge \alpha_2) \wedge \alpha_3) \wedge \ldots) \wedge \alpha_n)$ sera abrégé en $\alpha_1 \wedge \alpha_2 \wedge \alpha_3 \wedge \ldots \wedge \alpha_n$
$((\ldots((\alpha_1 \vee \alpha_2) \vee \alpha_3) \vee \ldots) \vee \alpha_n)$ sera abrégé en $\alpha_1 \vee \alpha_2 \vee \alpha_3 \vee \ldots \vee \alpha_n$.

Ces abus d'écriture seront d'autant moins périlleux que les formules $((\alpha_1 \wedge \alpha_2) \wedge \alpha_3)$ et $(\alpha_1 \wedge (\alpha_2 \wedge \alpha_3))$ – qui sont distinctes dans For(L) – vont se révéler interchangeables. Comme on le vérifie sans peine, elles sont satisfaites ou non satisfaites simultanément dans toute spécialisation d'une L-structure quelconque. D'autre part, $(((\alpha_1 \wedge \alpha_2) \wedge \alpha_3) \leftrightarrow (\alpha_1 \wedge (\alpha_2 \wedge \alpha_3)))$ est une tautologie dans For(L). On peut en dire autant de $((\alpha_1 \vee \alpha_2) \vee \alpha_3)$ et $(\alpha_1 \vee (\alpha_2 \vee \alpha_3))$.

Relevons que ces omissions de parenthèses n'interviennent que pour les ***notations*** relatives à des formules et non pas dans ces formules elles-mêmes. Rien n'est changé aux règles des définitions 1.0.6 et 1.0.8. Bien entendu ces simplifications d'écriture ne sont pas obligatoires.

En outre, nous nous autoriserons à parler de "constantes", de "variables", de "fonctions" et de "relations" au lieu de "symboles de constantes", de "symboles de variables", etc. Ce sont là de véritables abus et nous nous réservons de revenir à la terminologie orthodoxe en cas de besoin.

4.1 LES AXIOMES DE L'ÉGALITÉ

4.1.0 Définition

Soit L un langage du premier ordre.

On appelle *axiomes de l'égalité* ou *formules de Leibniz* (pour L) les formules:

1) $t_1 = t_1$
2) $(t_1 = t_2) \leftrightarrow (t_2 = t_1)$
3) $((t_1 = t_2) \wedge (t_2 = t_3)) \rightarrow (t_1 = t_3)$
4) $((t_1 = t'_1) \wedge (t_2 = t'_2) \wedge \ldots \wedge (t_n = t'_n)) \rightarrow (f_n(t_1, t_2, \ldots, t_n) = f_n(t'_1, t'_2, \ldots, t'_n))$
5) $((t_1 = t'_1) \wedge (t_2 = t'_2) \wedge \ldots \wedge (t_m = t'_m) \wedge R_m(t_1, t_2, \ldots, t_m)) \rightarrow R_m(t'_1, t'_2, \ldots, t'_m)$

où t_1, t'_1, t_2, t'_2, ..., t_p, t'_p, ... parcourent Ter(L), f_n parcourt Fct(L) et R_m parcourt Rel(L).

Nous désignerons l'ensemble de ces formules par Leib(L).

4.1.1 Proposition

La proposition suivante résulte immédiatement de ce qui précède ainsi que des définitions d'une spécialisation s d'une L-structure et de la satisfaction d'une formule pour s (cf. déf. 2.2.1, 2.2.4 et 2.2.11).

Soit L un langage du premier ordre. Pour toute L-structure (E, J), toute spécialisation s de (E, J) et toute formule λ dans Leib(L), on a:

$(E, J) \models \lambda[s]$. □

4.1.2 Commentaire

La dénomination adoptée pour Leib(L) est un hommage rendu à Gottfried Wilhelm Leibniz (1646–1716). Ce philosophe, mathématicien et logicien se situe à une charnière entre la pensée traditionnelle et les conceptions qui allaient s'épanouir dès la fin du 17[e] siècle. Ses préoccupations logiques le conduisirent à préciser l'idée d'égalité qui se trouve au carrefour de trois perspectives.

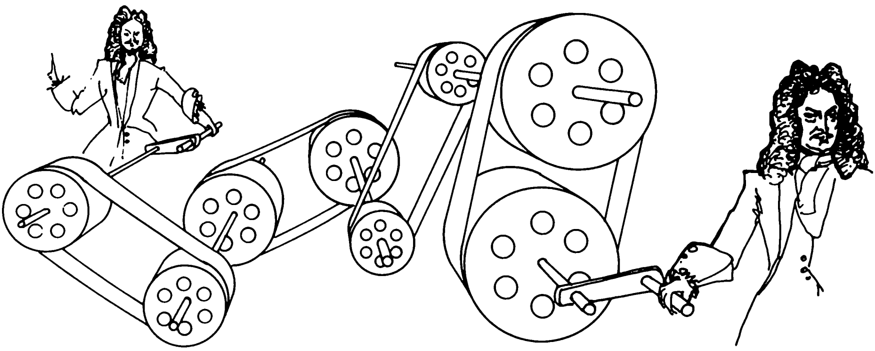
a) Traditionnellement, on parlait de "triangles égaux", de "figures égales" pour désigner ce qu'on appelle aujourd'hui triangles et figures isométriques ou congruentes. Dans ce sens "a égale b" signifie que a et b sont des objets occasionnellement confondus, mais plus généralement distincts, ayant un ou plusieurs caractères en commun. Ce genre de relation binaire est aujourd'hui appelé *équivalence*. Il est défini formellement par les formules de Leibniz des types 1), 2) et 3). Notons que les axiomes du type 1) soulèvent une petite difficulté d'origine grammaticale. Il est naturel de dire "a et b sont égaux"; il l'est moins de dire "a et a sont égaux" ("a et a est égal" ou "a est égal" sont décidément exécrables).

b) "Socrate est un homme" était considéré comme une sorte d'égalité du type "a est b", qui se notera ultérieurement (et passagèrement, par chance) $a=b$. Ce genre de relations satisfait les formules de Leibniz des types 1) et 3), mais pas 2). Les axiomes 3) expriment le *principe du syllogisme*: si "Socrate est homme" et si "homme est mortel", alors "Socrate est mortel", que Leibniz appelait la "conséquence vraie par elle-même".

De telles considérations conduisirent Leibniz à établir des rapprochements entre la langue ordinaire d'une part, l'arithmétique et l'algèbre de l'autre. Remplacer "le lion est un animal" et "le lion est sauvage" par "le lion est un animal sauvage" peut se schématiser en"a est b" et "a est c", "a est bc". Cela ressemble beaucoup à "12 est divisible par 2" et "12 est divisible par 3", donc "12 est divisible par $2 \cdot 3$". Les propriétés de la négation peuvent être traduites par celles du signe $-$ de l'algèbre. Leibniz conçut alors le projet général d'expliciter un dictionnaire des notions premières et un calcul de type algébrique capable de schématiser tout ou partie de l'art de penser. Il comptait ainsi "arriver à quelque certitude pour finir une bonne partie des disputes et pour avancer l'art d'inventer". Ce programme ambitieux ne fut pas accompli par Leibniz, ni par personne d'autre. Mais il reste une obsession secrète de beaucoup de penseurs. Et on peut estimer que les travaux de Gödel que nous évoquerons au chapitre 8 en ont achevé une partie raisonnable.

c) Le troisième point de vue sur l'égalité, que Leibniz évoquait par les termes d'***identité*** ou d'***égalité logique***, fait penser à la conception actuelle de l'égalité mathématique: aux termes de celle-ci, "$a=b$" exprime que a et b sont des signes pour un même objet. On peut alors remplacer a par b et réciproquement dans tout raisonnement. Ainsi Leibniz déclarait-il que a est identique à b quand il est possible de substituer l'un à l'autre sans altérer la vérité. Cet aspect de l'égalité est partiellement traduit par les formules de Leibniz des types 4) et 5), ainsi que par 3).

La définition donnée par Leibniz de l'identité montre qu'il prenait essentiellement en compte la compréhension des concepts. C'est ce qui lui rendit difficile l'élaboration d'un calcul des propositions. En spéculant sur l'extension des concepts, Georges Boole (1815–1864) parvint à créer une véritable algèbre logique, dont nous avons fait usage au chapitre 3, par le truchement des fonctions de vérité.



CHAPITRE 5

La logique des quantificateurs. La méthode de Henkin: la réduction à la logique des propositions

5.0 INTRODUCTION

Les deux paragraphes précédents nous ont familiarisés avec l'emploi des divers connecteurs dans un langage du premier ordre L. Il convient d'en faire autant avec les autres symboles logiques et particulièrement avec les quantificateurs.

Dans les assertions "6 est pair" et "Socrate est mortel", "pair" et "mortel" sont grammaticalement des prédicats. On peut considérer qu'en disant "6 est pair", on exprime que 6 appartient à l'ensemble des nombres pairs.

Considérons maintenant un symbole de relation unaire R_1 et une constante c dans L. La formule $R_1(c)$ est traduite dans toute L-structure (E, J) par: $J(c)$ appartient au sous-ensemble $J(R_1)$ de E. On peut donc regarder R_1 comme un prédicat formel. En fait, certains auteurs donnent le nom de prédicat à tout symbole de relation. Il existe dès lors des prédicats unaires, binaires, ternaires, etc. Le symbole $=$ apparaît aussi comme un prédicat binaire.

A partir du symbole $=$ et de symboles de relations R_1, R'_1, R_2, ... on peut construire de nouveaux prédicats. Considérons en particulier les quatre procédés suivants:

1. *L'emploi du symbole* $=$: si $f_1 \in \mathrm{Fct}(L)$ et $c \in \mathrm{Cst}(L)$, $f_1(x)=c$ est une formule déterminant un prédicat unaire portant sur la variable x.
2. *L'emploi des autres connecteurs*: $(\neg(R_1(x)))$ et $R_1(x) \wedge R'_1(x)$ sont des formules qui déterminent de nouveaux prédicats unaires portant sur la variable x.
3. *L'emploi des substitutions*: $R_2(x, x)$ et $R_2(c, x)$, où $c \in \mathrm{Cst}(L)$, nous montrent des prédicats unaires portant sur la variable x et construits à partir d'un prédicat binaire. Si $f_2 \in \mathrm{Fct}(L)$, $R_1(f_2(x, y))$ est un prédicat binaire portant sur les variables x et y, construit à partir d'une relation unaire et d'une fonction binaire.
4. *L'emploi des quantificateurs*: $\forall x R_2(x, y)$ et $\exists x R_2(x, y)$ sont interprétées dans chaque spécialisation s d'une L-structure (E, J) comme des conditions imposées à $s(y)$, où y est la seule variable libre dans ces deux formules. Elles font donc apparaître des prédicats unaires portant sur y, construits à partir d'un prédicat binaire. Observons à ce propos que "6 est pair" signifie "il existe un nombre naturel x tel que 6 égale $2 \cdot x$".

Il est clair qu'on peut combiner entre eux ces quatre procédés.

Le procédé 1 nous renvoie aux formules de Leibniz et le procédé 2 au calcul des propositions. Il nous faut examiner de plus près les procédés 3 et 4 qui relèvent de ce qu'on appelle parfois le *calcul des prédicats*.

Le calcul des prédicats, particulièrement ce qui touche aux quantificateurs, semble très éloigné du calcul des propositions. Pourtant le logicien Henkin est parvenu, en 1949, à ramener le premier au second. C'est à ce beau résultat qu'est consacré le présent paragraphe. Le lemme de réduction de la logique du premier ordre à celle des propositions en est le pivot. Il a un caractère un peu technique. Mais il permet d'établir immédiatement deux théorèmes intéressants: le théorème de compacité de la logique du premier ordre et celui de Löwenheim-Skolem. En outre, il deviendra l'outil essentiel de la preuve du théorème de complétude que nous démontrerons au paragraphe suivant.

5.1 SUBSTITUTION D'UN TERME À UNE VARIABLE

5.1.0 Préambule

Soit L un langage du premier ordre, x une variable, t un terme de L et φ une formule de L. Le remplacement purement typographique de x par t dans φ ne conduit généralement par à une formule de L. Il suffit de penser au cas où $t \equiv c \in \mathrm{Cst}(L)$ et $\varphi \equiv \forall x \alpha$, avec $\alpha \in \mathrm{For}(L)$. Nous allons définir par récurrence sur la formation de φ la propriété pour t d'être *substituable à x dans φ* et, le cas échéant, la formule φ^x_t obtenue en substituant t à x dans φ.

5.1.1 Définition

Soit L un langage du premier ordre; soit $x \in \mathrm{Var}$, $t \in \mathrm{Ter}(L)$ et $\varphi \in \mathrm{For}(L)$.

- Si φ est atomique, t est *substituable* à x dans φ. φ^x_t est alors la formule obtenue en remplaçant typographiquement x par t dans φ. En particulier, si x ne figure pas dans φ, $\varphi^x_t \equiv \varphi$.
- Si $\varphi \equiv \neg \psi \in \mathrm{For}(L)$, t est *substituable* à x dans φ *ssi* t est substituable à x dans ψ. Dans ce cas: $\varphi^x_t :\equiv \neg \psi^x_t$
- Si $\varphi \equiv \alpha * \beta$, avec α, $\beta \in \mathrm{For}(L)$, et où $*$ désigne l'un des symboles $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, t est *substituable* à x dans φ *ssi* t est substituable à x à la fois dans α et dans β. Dans ce cas: $\varphi^x_t :\equiv \alpha^x_t * \beta^x_t$
- Si $\varphi \equiv \forall y \psi$ (resp. $\exists y \psi$), avec $y \in \mathrm{Var}$ et $\psi \in \mathrm{For}(L)$, il faut distinguer deux cas:
  1° Si $x \equiv y$, t est *substituable* à x dans φ, et $\varphi^x_t :\equiv \varphi$.
  2° Si $x \not\equiv y$, t est *substituable* à x dans φ *ssi* y ne figure pas dans t *et* t est substituable à x dans ψ. Dans ce cas: $\varphi^x_t :\equiv \forall y \psi^x_t$ (resp. $\exists y \psi^x_t$).

5.1.2 Exemples

Soit L un langage du premier ordre, avec $c \in \mathrm{Cst}(L)$, $f_2 \in \mathrm{Fct}(L)$, $R_1 \in \mathrm{Rel}(L)$ et $x, y, z \in \mathrm{Var}$.

- Si $\varphi \equiv R_1(x) \vee (\forall y(y=x))$, $t \equiv f_2(x, y)$ et $x \not\equiv y$, alors t n'est pas substituable à x dans φ.
- Si $\varphi \equiv R_1(x) \vee (\forall x(y=x))$ et $t \equiv f_2(x, y)$, alors t est substituable à x dans φ et $\varphi_t^x \equiv R_1(f_2(x, y)) \vee (\forall x(y=x))$.
- Si $\varphi \equiv R_1(x) \vee (\forall z(z=x))$, $t \equiv f_2(x, c)$ et $x \not\equiv z$, alors t est substituable à x dans φ et $\varphi_t^x \equiv R_1(f_2(x, c)) \vee (\forall z(z=f_2(x, c)))$.

5.1.3 Remarque

Le seul obstacle à la substitution d'un terme à une variable réside dans le dernier cas évoqué par la définition 5.1.1. Si la variable y figure dans t, le fait de substituer t à x dans $\forall y\psi$ (ou $\exists y\psi$) risque de modifier le "sens" de la formule φ alors qu'on désire montrer ce qu'elle devient dans le cas particulier où x est remplacé par t. Par exemple, si $\varphi \equiv \exists y(\neg(y=x))$, il serait peu raisonnable d'y remplacer x par y, ce qui conduirait à $\exists y(\neg(y=y))$.

5.1.4 Remarque

Si $\varphi \equiv \forall x\psi$ (ou $\exists x\psi$), x n'est pas une variable libre de φ. La définition 2.2.11 montre que x pourrait être typographiquement remplacée par n'importe quel symbole de variable n'apparaissant pas dans ψ; la formule obtenue est satisfaite ou non en même temps que φ dans toute spécialisation d'une L-structure. On peut dire que x est une "variable muette" et il est naturel de poser $\varphi_t^x \equiv \varphi$. Par analogie, la substitution de 2 à x dans l'expression analytique $x^2 + \int_0^1 f(x)dx$ conduit à $4 + \int_0^1 f(x)dx$ car x apparaît comme une variable muette dans l'intégrale.

5.1.5 Remarque

Nous constatons que lorsqu'un terme $t \in \mathrm{Ter}(L)$ ne comporte aucune variable, il est substituable dans n'importe quelle formule de L.

Nous sommes conduits à adopter quelques conventions.

5.1.6 Convention

Soit L un langage du premier ordre. Un terme t de L est dit *clos* lorsqu'il ne comporte aucun symbole de variable.

Un terme clos de L est substituable à toute variable libre dans n'importe quelle formule de L.

5.1.7 Convention

Soit s une spécialisation d'une L-structure (E, J) et soit t un terme clos de L. Il résulte de la définition 2.2.4, que l'élément $s(t)$ de E dépend de J mais non de s. Nous le noterons donc $J(t)$ ou $\tilde{t}$.

5.1.8 Convention

Nous noterons $\mathrm{For}_1(L)$ l'ensemble des formules de L comportant au plus une variable libre. Si $\varphi \in \mathrm{For}_1(L)$ et si $VL(\varphi) \subset \{x\}$, nous le préciserons parfois en notant $\varphi(x)$ au lieu de φ. Dans ce cas, si t est un terme clos de L, $\varphi(x)_t^x$ sera noté généralement $\varphi(t)$. Remarquons que $\varphi(t)$ est alors un énoncé.

5.1.9 Convention

Soit (E, J) une L-structure et soit $\varphi(x) \in \mathrm{For}_1(L)$. Si s_1 et s_2 sont deux spécialisations de (E, J) telles que $s_1(x) = s_2(x)$, alors $(E, J) \vDash \varphi(x)[s_1]$ *ssi* $(E, J) \vDash \varphi(x)[s_2]$ (cf. prop. 2.2.19). Cela justifie la notation suivante: si $a \in E$ et s'il existe une spécialisation s de (E, J) telle que $s(x) = a$ et que $(E, J) \vDash \varphi(x)[s]$, on écrit: $(E, J) \vDash \varphi(x)[\frac{x}{a}]$.

5.1.10 Remarque importante

Cette convention d'écriture permet d'exprimer simplement l'importante remarque que voici. Reprenons les notations de la convention 5.1.9 et soit t un terme clos de L. On a alors:

$$(E, J) \vDash \varphi(x)\left[\frac{x}{J(t)}\right] \Leftrightarrow (E, J) \vDash \varphi(t) \tag{5.0}$$

Autrement dit, on peut indifféremment:

- vérifier que l'énoncé $\varphi(t)$ est satisfait dans (E, J)
- vérifier que la formule $\varphi(x)$ est satisfaite dans une (toute) spécialisation de (E, J) qui envoie x sur $J(t)$.

Ce fait est intuitivement évident. Il mérite toutefois une démonstration formelle, à laquelle nous reviendrons en fin de paragraphe, sous forme d'appendice.

5.2 L'EXTENSION DE HENKIN D'UN LANGAGE DU PREMIER ORDRE

5.2.0 Notation générale

Si M est un langage du premier ordre et si D est un ensemble quelconque de symboles ne comportant aucun symbole de M sauf éventuellement des constantes de M, nous noterons $M(D)$ le langage du premier ordre obtenu en réunissant D aux constantes de M. En d'autres termes:

$$\mathrm{Cst}(M(D)):=\mathrm{Cst}(M)\cup D;\ \mathrm{Fct}(M(D)):=\mathrm{Fct}(M);\ \mathrm{Rel}(M(D)):=\mathrm{Rel}(M).$$

5.2.1 Préparation

Dans la suite du paragraphe, L désigne un langage du premier ordre fixé une fois pour toutes.

Pour préparer la définition suivante, construisons à partir de L une suite $(L_n)_{n=0,1,2,\ldots}$ de langages du premier ordre:

- Posons $L_0:=L$.
- A chaque $\varphi\in\mathrm{For}_1(L_0)$ associons un nouveau symbole de constante c_φ.
- Si C_1 est l'ensemble de ces nouveaux symboles, posons $L_1:=L(C_1)$.
- Soit $n\geqq 1$ tel que L_n et C_n sont construits. A chaque φ pris dans $\mathrm{For}_1(L_n)-\mathrm{For}_1(L_{n-1})$, associons un nouveau symbole de constante c_φ. Si C_{n+1} désigne la réunion de C_n et de ces nouveaux symboles, posons $L_{n+1}:=L(C_{n+1})$.

5.2.2 Définition

Avec les notations précédentes:

- On appelle *constantes de Henkin* de L les éléments de l'ensemble $C:=\bigcup_{n=1}^{\infty} C_n$.
- La *hauteur d'une constante de Henkin* $c\in C$ est le plus petit entier n tel que $c\in C_n$. Pour $n>1$, C_n-C_{n-1} est l'ensemble des constantes de Henkin de L de hauteur n.
- Le langage du premier ordre $L(C)$ s'appelle l'*extension de Henkin* de L.

5.2.3 Remarque

En anglais, les constantes de Henkin sont appelées "witnessing constants", c'est-à-dire "constantes-témoins". On peut considérer que chaque élément de C témoigne de l'existence d'une formule dans $\mathrm{For}_1(L(C))$, (cf. remarque 5.2.4).

5.2.4 Remarque

Soit $\varphi\in\mathrm{For}_1(L(C))$. Si dans φ n'apparaît aucun élément de C, $\varphi\in\mathrm{For}_1(L)=\mathrm{For}_1(L_0)$. Sinon, soit n le plus petit entier $\geqq 1$ tel que toutes les constantes apparaissant dans φ appartiennent à C_n. Comme les ensembles C_j sont emboîtés, $\varphi \in \mathrm{For}_1(L_n) - \mathrm{For}_1(L_{n-1})$. Ainsi

$$\mathrm{For}_1(L(C)) = \mathrm{For}_1(L) \cup \{\bigcup_{n=1}^{\infty} (\mathrm{For}_1(L_n) - \mathrm{For}_1(L_{n-1})\}.$$

D'où il résulte que:

$$C = \{c_\varphi | \varphi \in \mathrm{For}_1(L(C))\}.$$

C'est en partie pour obtenir cette égalité qu'on a construit l'extension de Henkin de L.

5.2.5 Remarque

Si $\varphi \in \mathrm{For}_1(L(C))$, $\neg\varphi \in \mathrm{For}_1(L(C))$, puisque $VL(\neg\varphi) = VL(\varphi)$.

5.3 LES AXIOMES DE HENKIN ET LES AXIOMES DES QUANTIFICATEURS

5.3.0 Définition

- Les énoncés suivants:
  $H_1(\varphi) :\equiv \exists x\varphi(x) \rightarrow \varphi(c_\varphi)$
  $H_2(\varphi) :\equiv \varphi(c_{\neg\varphi}) \rightarrow \forall x\varphi(x)$
  où $\varphi \equiv \varphi(x)$ parcourt $\mathrm{For}_1(L(C))$, s'appellent *axiomes de Henkin* pour le langage L.
- Les énoncés suivants:
  $Q_1(\varphi, t) :\equiv \forall x\varphi(x) \rightarrow \varphi(t)$
  $Q_2(\varphi, t) :\equiv \varphi(t) \rightarrow \exists x\varphi(x)$
  où $\varphi \equiv \varphi(x)$ parcourt $\mathrm{For}_1(L(C))$ et t parcourt l'ensemble des termes clos de $L(C)$, s'appellent *axiomes des quantificateurs* pour le langage L.
- L'ensemble des axiomes de Henkin et des axiomes des quantificateurs pour L sera désigné par $\mathrm{Hen}(L)$.

5.3.1 Remarque

Le contenu intuitif des axiomes des quantificateurs est clair. Plus précisément, il résulte de l'assertion (5.0) du numéro 5.1.10 qu'ils sont satisfaits dans toute $L(C)$-structure.

5.3.2 Remarque

Les axiomes de Henkin peuvent être compris intuitivement de la manière suivante.

Considérons d'abord le cas de $H_1(\varphi)$. Soit (E, J) une L-structure. Si $(E, J) \models \exists x \varphi(x)$, alors il existe $a \in E$ tel que $(E, J) \models \varphi(x) \left[\frac{x}{a}\right]$. Etendons alors J en posant $J(c_\varphi) := a$. En vertu de (5.0), on a $(E, J) \models \varphi(c_\varphi)$. Si, au contraire, $(E, J) \models \neg(\exists x \varphi(x))$, prenons arbitrairement $b \in E$ et étendons J en posant $J(c_\varphi) := b$. Dans les deux cas, $(E, J) \models (\exists x \varphi(x) \rightarrow \varphi(c_\varphi))$.

Considérons maintenant le cas de $H_2(\varphi)$. Si $(E, J) \models \neg(\forall x \varphi(x))$; il existe $a \in E$ tel que $(E, J) \models \neg \varphi(x) \left[\frac{x}{a}\right]$. Etendons J en posant $J(c_{\neg\varphi}) := a$. En vertu de (5.0), on a $(E, J) \models \neg \varphi(c_{\neg\varphi})$; autrement dit, il est faux que $(E, J) \models \varphi(c_{\neg\varphi})$. Si, au contraire, $(E, J) \models \forall x \varphi(x)$, prenons arbitrairement $b \in E$ et étendons J en posant $J(c_{\neg\varphi}) := b$. Donc, dans les deux cas, $(E, J) \models (\varphi(c_{\neg\varphi}) \rightarrow \forall x \varphi(x))$.

5.3.3 Convention

Convenons de dire qu'une $L(C)$-structure (E, J') est une *extension* d'une L-structure (E, J) lorsque J et J' coïncident sur $\mathrm{Cst}(L) \cup \mathrm{Fct}(L) \cup \mathrm{Rel}(L)$.

Les deux remarques ci-dessus montrent qu'on peut étendre toute L-structure en une $L(C)$-structure de manière à satisfaire tous les axiomes des quantificateurs ainsi que les axiomes de Henkin $H_1(\varphi)$ et $H_2(\varphi)$ pour autant que $\varphi \in \mathrm{For}_1(L)$. La proposition suivante montre qu'on peut étendre cette possibilité au cas où $\varphi \in \mathrm{For}_1(L(C))$.

5.3.4 Proposition

Toute L-structure (E, J) peut être étendue en une $L(C)$-structure (E, J') qui soit un modèle de $\mathrm{Hen}(L)$.

5.3.5 Démonstration

Nous devons construire une interprétation J' en étendant J à l'ensemble C des constantes de Henkin de L. Pour tout entier $n \geqq 1$, nous allons construire une application $J'_n : C_n \rightarrow E$ qui sera la restriction de J' à C_n. Nous procédons par récurrence sur n.

Remarquons au préalable que, si $\varphi(x) \in \mathrm{For}_1(L(C))$, la satisfaction de $H_2(\varphi)$ équivaut à celle de:

	$\varphi(c_{\neg\varphi}) \rightarrow \forall x \varphi(x)$
ou	$\neg(\forall x \varphi(x)) \rightarrow \neg \varphi(c_{\neg\varphi})$
ou encore	$\neg(\forall x \neg(\neg \varphi(x))) \rightarrow \neg \varphi(c_{\neg\varphi})$
ou enfin	$\exists x(\neg \varphi(x)) \rightarrow \neg \varphi(c_{\neg\varphi})$.

Mais ce dernier énoncé n'est autre que $H_1(\neg \varphi)$.

Nous nous proposons de construire J'_n de manière que tous les axiomes $H_1(\varphi)$ et $H_2(\varphi)$ soient satisfaits dans (E, J'_n), pour $\varphi \in \mathrm{For}_1(L_{n-1})$. Nous constatons qu'il suffit de le faire pour les seuls axiomes $H_1(\varphi)$.

Si $n=1$, nous devons construire J'_1 de manière à satisfaire tous les axiomes $H_1(\varphi)$ où φ parcourt $\mathrm{For}_1(L)$. Comme $C_1 = \{c_\varphi | \varphi \in \mathrm{For}_1(L)\}$, la remarque 5.3.2 et son commentaire nous indiquent la façon de construire J'_1.

Si $n \geqq 1$, supposons par induction qu'on a construit J'_n de manière que soient satisfaits tous les axiomes $H_1(\psi)$ où $\psi \in \mathrm{For}_1(L_{n-1})$. Prenons alors $\varphi \equiv \varphi(x) \in \mathrm{For}_1(L_n - \mathrm{For}_1(L_{n-1})$. $\exists x \varphi(x)$ est alors un énoncé de L_n.

Lorsque $(E, J'_n) \vDash \exists x \varphi(x)$, il existe $a \in E$ tel que $(E, J'_n) \vDash \varphi(x) \left[\frac{x}{a}\right]$. Posons alors $J'_{n+1}(c_\varphi) := a$; moyennant cette définition, $\varphi(c_\varphi)$ est satisfaite en vertu de (5.0). $H_1(\varphi) \equiv \exists x \varphi(x) \to \varphi(c_\varphi)$ est donc satisfait dans ce premier cas. Lorsqu'au contraire (E, J'_n) ne satisfait pas $\exists x \varphi(x)$, on prend arbitrairement b dans E et on pose $J'_{n+1}(c_\varphi) := b$. $H_1(\varphi)$ est à nouveau satisfait.

Comme $C_{n+1} = \{c_\varphi | \varphi \in \mathrm{For}_1(L_n)\}$, on définit ainsi J'_{n+1} et $(E, J'_{n+1}) \vDash H_1(\varphi)$ pour toute $\varphi \in \mathrm{For}_1(L_n)$.

Définissons J' par $J'|_{C_n} := J'_n$ pour tout $n \geqq 1$. (E, J') est une $L(C)$-structure satisfaisant les conditions de l'énoncé. □

Remarquons en passant que J' est bien loin d'être univoquement déterminée.

5.4 LE LEMME DE RÉDUCTION À LA LOGIQUE DES PROPOSITIONS

5.4.0 Préambule

Nous voici parvenus au point culminant de ce chapitre.

5.4.1 Convention

Convenons de dire qu'une $L(C)$-structure (E, J') est *canonique* lorsque $J'(C) = E$.

5.4.2 Proposition: lemme de réduction à la logique des propositions (Henkin 1949)

Soit S un ensemble d'énoncés de L - donc *a fortiori* de $L(C)$. Les trois assertions suivantes sont équivalentes:

a) Il existe une $L(C)$-structure canonique (E, J') qui est un modèle pour S.

b) Il existe une L-structure (E, J) qui est un modèle pour S.
c) La partie $S \cup \text{Leib}(L(C)) \cup \text{Hen}(L)$ de $\text{For}(L(C))$ est consistante pour la logique des propositions.

5.4.3 Démonstration

- a)$\Rightarrow$b) est évident.
- b)$\Rightarrow$c) Soit (E, J) un modèle pour S. On peut étendre (E, J) en une $L(C)$-structure (E, J') qui est un modèle pour $S \cup \text{Hen}(L)$ d'après la proposition 5.3.4. Soit s une spécialisation de (E, J'); en vertu de la proposition 4.1.1, pour toute formule $\varphi \in \text{Leib}(L(C))$, $(E, J') \models \varphi[s]$. Si V_s est la fonction de vérité associée à s, $V_s(\alpha)=1$ pour toute formule $\alpha \in S \cup \text{Hen}(L) \cup \text{Leib}(L(C))$; par suite c) est vérifié.
- c)$\Rightarrow$a) C'est la partie non banale de la démonstration. Nous la parcourrons en plusieurs étapes.
  L'hypothèse c) nous permet d'affirmer qu'il existe une fonction de vérité V sur $\text{For}(L(C))$ valant 1 sur $S \cup \text{Leib}(L(C)) \cup \text{Hen}(L)$.

i) Posons $C^* = \text{Cst}(L(C))$.
Introduisons dans C^* la relation $\sim$ définie par:
$$c_1 \sim c_2 \Leftrightarrow V(c_1 = c_2) = 1, \text{ pour tous } c_1, c_2 \in C^*.$$
Montrons que $\sim$ est une relation d'équivalence, c'est-à-dire qu'elle est réflexive, symétrique et transitive. Soit $c_1, c_2, c_3 \in C^*$.
- Réflexivité: comme $(c_1 = c_1) \in \text{Leib}(L(C))$, $V(c_1 = c_1) = 1$. Donc $c_1 \sim c_1$.
- Symétrie: si $c_1 \sim c_2$, $V(c_1 = c_2) = 1$. D'autre part,
  $((c_1 = c_2) \leftrightarrow (c_2 = c_1)) \in \text{Leib}(L(C))$; donc $V((c_1 = c_2) \leftrightarrow (c_2 = c_1)) = 1$.
  En vertu de la définition 3.1.8, $V(c_2 = c_1) = 1$; donc $c_2 \sim c_1$.
- Transitivité: si $c_1 \sim c_2$ et $c_2 \sim c_3$, alors $V(c_1 = c_2) = V(c_2 = c_3) = 1$.
  Comme $(((c_1 = c_2) \wedge (c_2 = c_3)) \rightarrow (c_1 = c_3)) \in \text{Leib}(L(C))$,
  V vaut 1 sur cette formule. En vertu de la définition 3.1.8, $V(c_1 = c_3) = 1$ et, par suite, $c_1 \sim c_3$.

Les éléments de C^* se répartissent en sous-ensembles disjoints non vides appelés "classes d'équivalence pour $\sim$". Chacune de ces classes est le sous-ensemble des éléments de C^* équivalents à l'un quelconque des éléments de cette classe. Nous définissons E comme l'ensemble de ces classes d'équivalence. La classe de $c \in C^*$ sera notée $\tilde{c}$.

ii) Si t est un terme clos de $L(C)$ et x un symbole de variable, nous noterons $\varphi_t(x)$ la formule $(t = x)$ de $\text{For}_1(L(C))$.

5.4.4 Lemme

Avec les notations ci-dessus, on a $V(t = c_{\varphi_t(x)}) = 1$.

5.4.5 Démonstration du lemme 5.4.4

$V(\exists x\varphi_t(x)\to\varphi_t(c_{\varphi_t(x)}))=1$, puisque l'argument de V appartient à Hen(L). Si $V(\varphi_t(c_{\varphi_t(x)})$ était 0, on aurait $V(\exists x\varphi_t(x))=0$; or, $V(\varphi_t(t)\to\exists x\varphi_t(x))=1$, puisque l'argument de V appartient à Hen(L); par suite, on aurait $V(\varphi_t(t))=V(t=t)=0$: ce serait absurde puisque V prend la valeur 1 sur Leib($L(C)$). Par suite, $V(\varphi_t(c_{\varphi_t(x)}))=1$, c'est-à-dire $V(t=c_{\varphi_t(x)})=1$. □

iii) Définition de $J'|_{C^*}$.
Pour tout $d\in\mathrm{Cst}(L(C))=C^*$; posons:

$$J'(d):=\tilde{c}_{\varphi_d(x)} \tag{5.1}$$

Comme $V(d=c_{\varphi_d(x)})=1$, $\tilde{d}=\tilde{c}_{\varphi_d(x)}$, en vertu du lemme 5.4.4. Il en résulte que $J'|_{C^*}$ n'est rien d'autre que l'application "canonique"

$$\begin{aligned}&C^*\to E\\ &d\ \mapsto\tilde{d}.\end{aligned}$$

En particulier, $J'|_{C^*}$ est surjective.

iv) *Définition de* $J'|_{\mathrm{Fct}(L(C))}$ $(=J'|_{\mathrm{Fct}(L)})$.

Soit $f_n\in\mathrm{Fct}(L)$. Prenons $c_1, c_2, \dots, c_n, c'_1, c'_2, c'_n\in C^*$ tels que $V(c_i=c'_i)=1$ pour $i=1, 2, \dots$, n. Posons:

$$t:\equiv f_n(c_1, c_2, \dots, c_n),\ t':\equiv f_n(c'_1, c'_2, \dots, c'_n)$$

les termes t et t' sont clos. Comme

$$V(((c_1=c'_1)\wedge(c_2=c'_2)\wedge\dots\wedge(c_n=c'_n))\to(t=t'))=1.$$

(l'argument de V étant une formule de Leibniz), on a $V(t=t')=1$. Mais, par une généralisation facile de la 3[e] formule de Leibniz, déf. 4.1.0,

$$V(((c_{\varphi_t(x)}=t)\wedge(t=t')\wedge(t'=c_{\varphi_{t'}(x)}))\mapsto(c_{\varphi_t(x)}=c_{\varphi_{t'}(x)}))=1.$$

En vertu du lemme 5.4.4, $V(c_{\varphi_t(x)}=c_{\varphi_{t'}(x)})=1$.

Cette discussion montre que la définition suivante a un sens: si $c_1, c_2, \dots, c_n\in C^*$, on pose:

$$J'(f_n)(\tilde{c}_1, \tilde{c}_2, \dots, \tilde{c}_n):=\tilde{c}_{\varphi_{t(x)}} \text{ où } t\equiv f_n(c_1, c_2, \dots, c_n) \tag{5.2}$$

5.4.6 Lemme

Pour tout terme clos t de $L(C)$, on a:

$(E, J')\vDash(t=c_{\varphi_t(x)})$ i.e. d'après iii): $J'(t)=\tilde{c}_{\varphi_t(x)}$.

5.4.7 Démonstration du lemme 5.4.6

On procède par récurrence sur la longueur de t. Lorsque $t\in C^*$, la conclusion est vraie en vertu de la définition de J' (cf. formule (5.1)). Supposons que

$t \equiv f_n(t_1, t_2, \dots, t_n)$ où $t_1, t_2, \dots, t_n$ sont des termes clos pour lesquels la conclusion est vraie. Alors:

$$J'(t) = J'(f_n)(J'(t_1), \dots, J'(t_n)) = J'(f_n)(\tilde{c}_{\varphi_{t_1}(x)}, \dots, \tilde{c}_{\varphi_{t_n}(x)}) = \tilde{c}_{\varphi_{t'}(x)}$$

en vertu de la formule (5.2), et en posant $t' :\equiv f_n(c_{\varphi_{t_1}(x)}, \dots, c_{\varphi_{t_n}(x)})$. Or en vertu du lemme 5.4.4:

$$V(c_{\varphi_t(x)} = f_n(t_1, \dots, t_n)) = 1$$
$$V(t_i = c_{\varphi_{t_i}(x)}) = 1,\ i = 1, \dots, n$$
$$V(f_n(c_{\varphi_{t_1}(x)}, \dots, c_{\varphi_{t_n}(x)}) = c_{\varphi_{t'}(x)}) = 1.$$

D'où par les troisième et quatrième formules de Leibniz:

$$V(c_{\varphi_t(x)} = c_{\varphi_{t'}(x)}) = 1, \text{ c'est-à-dire } \tilde{c}_{\varphi_{t'}(x)} = \tilde{c}_{\varphi_t(x)}. \qquad \square$$

v) *Définition de* $J'|_{\mathrm{Rel}(L(C))} (= J'|_{\mathrm{Rel}(L)})$.

Prenons $R_m \in \mathrm{Rel}(L)$. Soit $c_1, c_2, \dots, c_m, d_1, d_2, \dots, d_m \in C^*$, tels que $V(c_i = d_i) = 1$, pour $i = 1, 2, \dots, m$. Comme

$$V(((c_1 = d_1) \wedge \dots \wedge (c_m = d_m) \wedge R_m(c_1, \dots, c_m)) \rightarrow R_m(d_1, \dots, d_m)) = 1$$

(l'argument de V étant une formule de Leibniz), si $V(R_m(c_1, \dots, c_m)) = 1$, alors $V(R_m(d_1, \dots, d_m)) = 1$. Cela montre que la définition suivante a un sens:

$$J'(R_m) := \{(\tilde{c}_1, \dots, \tilde{c}_m) \in E^m \mid V(R_m(c_1, \dots, c_m)) = 1\}. \tag{5.3}$$

vi) *Démonstration de l'existence d'un modèle canonique de S.*

L'interprétation J' est maintenant complètement définie. Nous nous proposerons de montrer que (E, J') est un modèle pour S; le fait qu'il est canonique résulte de iii). Nous allons même établir un fait plus général, à savoir que, pour tout énoncé $\varphi \in \mathrm{For}(L(C))$:

$$(E, J') \vDash \varphi \Leftrightarrow V(\varphi) = 1. \tag{5.4}$$

Nous procédons par récurrence sur la formation de φ.

vi a) *Cas où* $\varphi \equiv (t_1 = t_2)$, où t_1, t_2 sont des termes clos de $L(C)$.

On a successivement:

$$(E,J') \vDash \varphi \Leftrightarrow J'(t_1) = J'(t_2) \overset{\text{lemme 5.4.6}}{\Leftrightarrow} \tilde{c}_{\varphi_{t_1}(x)} = \tilde{c}_{\varphi_{t_2}(x)} \Leftrightarrow$$
$$\Leftrightarrow V(c_{\varphi_{t_1}(x)} = c_{\varphi_{t_2}(x)}) = 1 \underset{\substack{\text{lemme 5.4.4.} \\ \text{3e form. de Leibniz}}}{\Leftrightarrow} V(t_1 = t_2) = 1$$

vi b) *Cas où* $\varphi \equiv R_m(t_1, \dots, t_m)$ où $t_1, \dots, t_m$ sont des termes clos de $L(C)$.

On a successivement:

$$(E,J) \vDash \varphi \Leftrightarrow (J'(t_1), \dots, J'(t_m)) \in J'(R_m) \overset{\text{form. (5.1)}}{\Leftrightarrow} (\tilde{c}_{\varphi_{t_1}(x)}, \dots, \tilde{c}_{\varphi_{t_m}(x)}) \in J'(R_m) \Leftrightarrow$$
$$\Leftrightarrow V(R_m(c_{\varphi_{t_1}(x)}, \dots, c_{\varphi_{t_m}(x)})) = 1 \underset{\substack{\text{lemme 5.4.6} \\ \text{5e form. de Leibniz}}}{\Leftrightarrow} V(R_m(t_1, \dots, t_m)) = 1$$

vi a) et vi b) établissent (5.4) pour les énoncés atomiques de $L(C)$.

vi c) *Intervention des connecteurs*

Soit φ, ψ des énoncés de $L(C)$ pour lesquels (5.4) est vrai. Montrons que (5.4) est vrai pour $\neg\varphi$ et pour $\varphi\wedge\psi$.

$$(E,J')\models(\neg\varphi)\Leftrightarrow \text{il est faux que } (E,J')\models\varphi\Leftrightarrow$$
$$\Leftrightarrow V(\varphi)=0\Leftrightarrow V(\neg\varphi)=1.$$

$$(E,J')\models(\varphi\wedge\psi)\Leftrightarrow\{(E,J')\models\varphi \textit{ et } (E,J')\models\psi)\}\Leftrightarrow$$
$$\Leftrightarrow\{V(\varphi)=1 \textit{ et } V(\psi)=1\}\Leftrightarrow V(\varphi\wedge\psi)=1.$$

vi d) *Intervention des quantificateurs*

Pour achever la démonstration, il reste à établir le résultat suivant: Si $\psi(x)\in\mathrm{For}_1(L(C))$ est telle que, pour tout terme clos t de $L(C)$, (5.4) est vrai pour $\psi(t)$, alors (5.4) est vrai pour $\varphi:\equiv\exists x\psi(x)$.

Supposons que $V(\varphi)=1$. Comme $V(\varphi\rightarrow\psi(c_\psi))=1$ (car l'argument de V est l'axiome de Henkin $H_1(\psi)$), on a $V(\psi(c_\varphi))=1$. D'où, par hypothèse: $(E, J')\models\psi(c_\psi)$. Par suite, en vertu de la propriété (5.0), $(E, J')\models\exists x\psi(x)$, i.e. $(E, J')\models\varphi$.

Supposons que $V(\varphi)=0$. $V(\psi(t)\rightarrow\varphi)=1$, pour tout terme clos t de $L(C)$, (car l'argument de V est l'axiome des quantificateurs $Q_2(\psi, t)$), on a, pour tout $c\in C^*$, $V(\psi(c))=0$. Donc, en vertu de l'hypothèse de récurrence, pour tout $c\in C^*$, il est faux que $(E, J')\models\psi(c)$; cela revient à dire, moyennant (5.0), qu'il est faux que $(E, J')\models\psi(x)[\frac{x}{c}]$. Mais, lorsque c parcourt C^*, $\tilde{c}$ parcourt E puisque $J'|_{C^*}:C^*\rightarrow E$ est surjective. Donc, il est faux que $(E, J')\models\exists x\psi(x)$. Ainsi s'achève la démonstration de la proposition 5.4.2. □

5.5 LES THÉORÈMES DE COMPACITÉ ET DE LÖWENHEIM-SKOLEM

5.5.0 Préambule

Pour atténuer l'impression désagréable laissée par la démonstration un peu laborieuse du lemme de réduction, montrons que cette proposition entraîne immédiatement des résultats intéressants et importants.

5.5.1 Proposition: théorème de compacité de la logique du premier ordre (Gödel 1930, Malčev 1936–1941)

Soit S un ensemble d'énoncés dans un langage du premier ordre L. La condition nécessaire et suffisante pour que S admette un modèle est que toute partie finie de S admette un modèle.

Démonstration. La nécessité est évidente.

Pour établir la suffisance, supposons que toute partie finie T de S admet un modèle. En vertu de la proposition 5.4.2 (partie b)$\Rightarrow$c)), $T\cup$Leib($L(C)$)$\cup$Hen(L) est LP-consistant. On en déduit que toute partie finie de $S\cup$Leib($L(C)$)$\cup$Hen(L) est LP-consistante. D'après le théorème de compacité pour la LP-consistance (prop. 3.1.29), $S\cup$Leib($L(C)$)$\cup$Hen(L) est LP-consistant. En vertu de la proposition 5.4.2 (partie c)$\Rightarrow$b)), S admet un modèle. □

Avant de passer à la proposition suivante, rappelons que nous ne considérons pour l'instant que les langages du premier ordre dits "élémentaires", c'est-à-dire ceux dont chaque formule peut être effectivement écrite. Nous avons vu (prop. 2.3.2) que, dans un tel langage, l'ensemble des formules est dénombrable.

5.5.2 Proposition: théorème de Löwenheim-Skolem

(Löwenheim 1917, Skolem 1920)
Soit L un langage du premier ordre "élémentaire".
Soit S un ensemble d'énoncés de L admettant un modèle.
Alors S admet un modèle au plus dénombrable.

5.5.3 Démonstration

Si S admet un modèle, il existe une $L(C)$-structure canonique (E, J') qui est un modèle pour S, d'après la proposition 5.4.2, partie b)$\Rightarrow$a). Quand on se reporte à la construction des constantes de Henkin, on constate que l'ensemble C est la réunion d'une famille dénombrable d'ensembles $C_1, C_2, \ldots, C_n, \ldots$, dénombrables en vertu de la proposition 2.3.2. Il en résulte que C^* est lui-même dénombrable (cf. n° 2.3.0). Comme l'application $J'_{C^*}: C^* \to E$ est surjective, E est au plus dénombrable. □

Nous reviendrons ultérieurement sur certaines conséquences surprenantes du théorème de Löwenheim-Skolem (cf. 8.2.14). Pour l'instant, nous nous contenterons de montrer deux phénomènes intéressants qui découlent d'une utilisation très simple du théorème de compacité de la logique du premier ordre.

5.5.4 Exemple

Reprenons le langage L_3 de l'exemple 2.2.24. Nous avons vu qu'il convient à la formalisation des groupes. Il ne comporte que deux symboles propres: une constante et une fonction binaire. Pour simplifier, nous désignerons par e la constante et, au lieu de noter $f_2(t_1, t_2)$, où t_1 et t_2 sont des termes de L_3, nous utiliserons la notation multiplicative: $t_1 \cdot t_2$. Les *axiomes des groupes* s'écrivent alors:

$$\varphi_1: \equiv \forall z \forall y \forall x\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

φ_2: $\equiv \forall x(x \cdot e = x) \wedge (e \cdot x = x)$
φ_3: $\equiv \forall x \exists y(x \cdot y = e) \wedge (y \cdot x = e)$

L'exemple 2.2.24 nous a montré que $\{\varphi_1, \varphi_2, \varphi_3\}$ admet un modèle. Nous savons aussi qu'on appelle *groupe* tout modèle de $\{\varphi_1, \varphi_2, \varphi_3\}$.

Considérons maintenant un groupe (G, J). Notons 1 l'élément $J(e)$ de G; si $t_1, t_2 \in \mathrm{Ter}(L_3)$, écrivons $s(t_1) \cdot s(t_2)$ l'élément de G donné par $s(t_1 \cdot t_2)$, s étant une spécialisation de J. On dit que le groupe (G, J) *a de la torsion* s'il existe $a \in G$-$\{1\}$ et un nombre naturel $n > 0$ tels que: $\underbrace{\mathrm{a} \cdot \mathrm{a} \cdot \mathrm{a} \cdot \ldots \cdot \mathrm{a}}_{\text{n éléments}} = 1$. Relevons en passant que l'expression «a · a · a · ... · a» désigne sans ambiguïté $a \cdot (a \cdot (a \cdot (.. \cdot a) \ldots))$ en vertu de l'axiome d'associativité φ_1.

Par suite, on dit que le groupe (E, J) est *sans torsion* si outre les axiomes φ_1, φ_2 et φ_3, il satisfait les énoncés suivants:

α: $\equiv \exists x \neg(x = e)$
β_2: $\equiv \forall x(\neg(x = e) \rightarrow \neg(x \cdot x = e))$
β_3: $\equiv \forall x(\neg(x = e) \rightarrow \neg[x \cdot x \cdot x = e))$
$\vdots$
β_n: $\equiv \forall x(\neg(x = e) \rightarrow \neg(\underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{n}) = e))$
$\vdots$

Nous devons évidemment nous poser la question suivante: existe-t-il un groupe sans torsion? En d'autres termes, existe-t-il un modèle de l'ensemble d'énoncés:

$$S := \{\varphi_1, \varphi_2, \varphi_3, \alpha, \beta_2, \beta_3, \ldots, \beta_n, \ldots\} \subset \mathrm{For}(L_3)\ ?$$

En vertu de la proposition 5.5.1, on peut répondre positivement pour autant que toute partie finie de S admette un modèle. Considérons donc une partie finie quelconque T de S. Soit $\beta_{n_1}, \beta_{n_2}, \ldots, \beta_{n_q}$ les axiomes de type β_n figurant dans T. Posons $p := (n_1 \cdot n_2 \cdot \ldots\ldots \cdot n_q) + 1$.

Soit C_p le groupe cyclique des rotations d'angles $k \cdot \dfrac{2\pi}{p}$, où $k = 0, 1, 2, \ldots, p\text{-}1$, autour d'un point du plan. L'élément neutre 1 de C_p correspond à $k = 0$. On sait que l'ordre de tout élément $a \neq 1$ dans C_p divise p. (L'ordre de a est le plus petit nombre naturel $\mathrm{m} > 0$ tel que $a^m = 1$.) Il en résulte que $a^{n_1} \neq 1$, $a^{n_2} \neq 1$, ..., $a^{n_q} \neq 1$. Donc C_p est un modèle de T. Nous pouvons en conclure qu'il existe un groupe sans torsion.

Il est piquant de remarquer qu'on parvient à ce résultat à partir de la connaissance des groupes cycliques finis. Or, ceux-ci se situent d'une certaine manière aux antipodes des groupes sans torsion. Relevons aussi que nous avons prouvé l'existence d'un groupe sans torsion sans en montrer ni en nommer un seul. Il est clair que l'ensemble $\mathbb{Z} = \{0, +1, -1, +2, -2, \ldots\}$ des nombres entiers rationnels muni de l'addition ordinaire en est un exemple. Mais la connaissance de

$\mathbb{Z}$ n'est pas nécessaire pour parler des groupes finis de rotations autour d'un point du plan.

5.5.5 Remarque

Faisons un pas de plus. Soit Q l'ensemble des énoncés de L_3 satisfaits par les groupes finis. Posons:

$$R := Q \cup \{\alpha, \beta_1, \beta_2, \dots, \beta_n, \dots\}.$$

Le raisonnement précédent montre que R admet un modèle. Comme ce modèle est sans torsion, il est infini. Nous constatons qu'il est impossible de caractériser les groupes finis dans le langage L_3; autrement dit qu'il est impossible de donner un ensemble d'énoncés de L_3 qui soient satisfaits par les groupes finis et par eux seulement. Nous verrons plus tard que cette bizarrerie n'est pas propre au langage L_3.

5.6 APPENDICE

■ 5.6.0 Préambule

Revenons à l'affirmation 5.0 énoncée au numéro 5.1.10. Nous en avons fait usage dans la démonstration du lemme de réduction 5.4.2. Intuitivement, elle est assez évidente. Néanmoins, elle exige une preuve et celle-ci, malheureusement, est un peu laborieuse. Nous allons en présenter les grandes lignes. Comme à l'habitude, nous procéderons par récurrence sur la formation des formules. Cela va nous obliger à établir un résultat plus général que 5.0:

5.6.1 Proposition

Soit L un langage du premier ordre et M un langage du premier ordre obtenu en adjoignant éventuellement à L de nouvelles constantes. Soit φ une formule de L avec $VL(\varphi)=\{x_1, x_2, \dots, x_k\}$; soit $t_1, t_2, \dots, t_k$ des termes clos de M et soit l un nombre naturel tel que $0 \leqq l \leqq k\text{-}1$.

Posons $\varphi_l(x_{l+1}, \dots, x_k) :\equiv \varphi(t_1, t_2, \dots, t_l, x_{l+1}, \dots, x_k)$. Convenons de poser $\varphi_0 :\equiv \varphi$. Soit enfin (E, J) une M-structure.

Alors:

$$(E,J) \vDash \varphi(t_1,t_2,\dots,t_k) \Leftrightarrow (E,J) \vDash \varphi_l(x_{l+1}\dots,x_k)\left[\frac{x_{l+1}}{\tilde{t}_{l+1}}\dots,\frac{x_k}{\tilde{t}_k}\right] \tag{5.5}$$

5.6.2 Remarques préliminaires

- $\tilde{t}_j$ désigne $J(t_j)$ conformément à la convention 5.1.7.
- Le langage initial L étant fixé, l'affirmation (5.5) fait intervenir le choix de M, de φ, de l et de (E, J). Pour le mettre en évidence, nous noterons cette assertion ((5.5); M, φ, l, (E, J))).
- L'affirmation (5.0) n'est autre que ((5.5), L, φ, 0, (E, J)) avec $\varphi \in \mathrm{For}_1(L)$.

5.6.3 Démonstration

1^er^ cas: M, l et (E, J) sont quelconques et φ est *atomique*.

Dans ce cas, $\varphi_l \in \mathrm{For}(M)$ est aussi atomique et $\varphi_l(t_{l+1}, \ldots, t_k) \equiv \varphi(t_1, \ldots, t_k)$; il suffit dès lors de considérer le cas où M coïncide avec L et où $l=0$. Considérons l'éventualité où $\varphi \equiv R_m(u_1, \ldots, u_m)$, avec $u_1, \ldots, u_m \in \mathrm{Ter}(L)$. Alors $\varphi(t_1, \ldots, t_k) \equiv R_m(u'_1, \ldots, u'_m)$, où les u'_i sont des termes clos. On a $(E, J) \models \varphi(t_1, \ldots, t_k)$ si et seulement si l'affirmation ensembliste

$$\text{(AE)}\left\{\begin{array}{l} \tilde{R}_m(\tilde{u}, \ldots, \tilde{u}_m) \\ \qquad \text{obtenue en remplaçant dans } \varphi(t_1, \ldots, t_k) \\ \\ \quad \left\{\begin{array}{l} \text{1) } R_m \text{ par } \tilde{R}_m\ (= J(R_m)) \\ \text{2) chaque symbole de fonction } f_n \text{ par } \tilde{f}_n\ (=J(f_n)) \\ \text{3) chaque symbole de constante } c \text{ par } \tilde{c} \end{array}\right. \end{array}\right. \tag{5.6}$$

est satisfaite.

Reportons-nous maintenant à la définition de l'image par J des termes clos de M (cf. convention 5.1.7). Les opérations 2) et 3) ci-dessus reviennent à remplacer chaque terme w apparaissant dans $\varphi(t_1, \ldots, t_k)$ par $\tilde{w}$ (ce point constitue le pivot de la démonstration).

Parmi ces termes w figurent $t_1, \ldots, t_k$. Donc l'assertion (5.6) de (AE) est aussi celle qu'on obtient en exécutant sur $\varphi(t_1, \ldots, t_k)$ les opérations suivantes:

$$\left\{\begin{array}{ll} \text{1)} & \text{remplacer } R_m \text{ par } \tilde{R}_m; \\ \text{2')} & \text{remplacer } t_1 \text{ par } \tilde{t}_1, \ldots, t_k \text{ par } \tilde{t}_k; \\ \text{3')} & \text{mettre un signe}\,\tilde{}\ \text{sur tous les symboles de fonctions et de constantes} \\ & \text{qui n'apparaissent dans aucun des termes } t_1, \ldots, t_k. \end{array}\right.$$

On en déduit immédiatement que (5.6) s'obtient aussi en exécutant sur $\varphi(x_1, \ldots, x_k)$ les opérations purement typographiques suivantes:

1) remplacer R_m par $\tilde{R}_m$;
2″) remplacer x_1 par $\tilde{t}_1, \ldots, x_k$ par $\tilde{t}_k$;
3″) mettre un signe ˜ sur tous les symboles de fonctions et de constantes laissés intacts par 2″).

Or, cela revient exactement à s'assurer que:

$$(E, J) \models \varphi(x_1, \ldots, x_k)\left[\frac{x_1}{\tilde{t}_1}, \ldots, \frac{x_k}{\tilde{t}_k}\right].$$

L'assertion (5.5) est donc établie lorsque $\varphi \equiv R_m(u_1, \dots, u_m)$.

Dans l'éventualité où $\varphi \equiv (u_1 = u_2)$, on reprend textuellement la discussion précédente, m étant remplacé par 2, R_m par $=$ et $\tilde{R}_m$ par $=$. Le premier cas est ainsi réglé.

5.6.4 Exemple intermédiaire

Pour éclairer l'argumentation que nous venons de présenter, donnons un exemple. Admettons que le langage L comporte une constante c, deux fonctions f_1 et f_2 respectivement unaire et binaire, ainsi qu'une relation binaire R_2. Soit x et y des variables. Considérons alors:

$$\varphi(x, y) :\equiv R_2(f_1(x), f_2(y, c)),\ t_1 := f_2(c, c),\ t_2 := f_1(c).$$

Dans ce cas:

$$\varphi(t_1, t_2) \equiv R_2(f_1(f_2(c, c)), f_2(f_1(c), c)).$$

L'assertion (5.6) devient ici:

$$\tilde{R}_2(\tilde{f}_1(\tilde{f}_2(\tilde{c}, \tilde{c})), \tilde{f}_2(\tilde{f}_1(\tilde{c}), \tilde{c})) \tag{5.7}$$

en vertu des règles 1), 2) et 3). Or $\tilde{t}_1$ peut s'écrire indifféremment $\widetilde{f_2(c, c)}$ ou $\tilde{f}_2(\tilde{c}, \tilde{c})$; de même, $\tilde{t}_2$ est à la fois $\widetilde{f_1(c)}$ ou $\tilde{f}_1(\tilde{c})$. (5.7) peut donc aussi s'écrire:

$$\tilde{R}_2(\tilde{f}_1(\tilde{t}_1), \tilde{f}_2(\tilde{t}_2, \tilde{c})),$$

ce qui revient à appliquer les règles 1), 2′) et 3′). Mais cette dernière assertion ensembliste est vraie si

$$(E, J) \vDash \varphi(x, y)\left[\frac{x}{\tilde{t}_1}, \frac{y}{\tilde{t}_2}\right]$$

et, dans ce cas seulement.

2ᵉ cas: $\varphi \equiv \neg\psi$, $VL(\psi) = \{x_1, x_2, \dots, x_k\}$, M, l et (E, J) sont quelconques et $((5.5);\ M, \psi, l, (E, J))$ est vraie.

En utilisant les règles concernant la substitution et celles qui définissent la satisfaction d'une formule:

$$\begin{aligned}
&(E,J) \vDash (\neg\psi)\ (t_1, \dots, t_k) \Leftrightarrow (E,J) \vDash \neg(\psi(t_1, \dots, t_k)) \Leftrightarrow \\
&\Leftrightarrow \text{il est faux que } (E,J) \vDash \psi(t_1, \dots, t_k) \quad \underset{\text{(hypothèse sur } \psi)}{\Leftrightarrow} \\
&\Leftrightarrow \text{il est faux que } (E,J) \vDash \psi_l\left[\frac{x_{l+1}}{\tilde{t}_{l+1}}, \dots, \frac{x_k}{\tilde{t}_k}\right] \Leftrightarrow \\
&\Leftrightarrow (E,J) \vDash \neg(\psi_l)\left[\frac{x_{l+1}}{\tilde{t}_{l+1}}, \dots, \frac{x_k}{\tilde{t}_k}\right] \Leftrightarrow \\
&\Leftrightarrow (E,J) \vDash (\neg\psi)_l\left[\frac{x_{l+1}}{\tilde{t}_{l+1}}, \dots, \frac{x_k}{\tilde{t}_k}\right]
\end{aligned}$$

3ᵉ cas: $\varphi \equiv \alpha * \beta$ où α, $\beta \in \mathrm{For}(L)$, où $*$ est l'un des symboles $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$; M, l et (E, J) sont quelconques et ((5.5); M, α, l, (E, J)) et ((5.5); M, β, l, (E, J)) sont vraies.

On procède exactement comme dans le 2ᵉ cas.

Il n'est peut-être pas inutile de relever, à l'occasion de ces deux derniers cas, que si $VL(\varphi)=\{x_1, \dots, x_k\}$ et si $l \geqq k$, φ_l désigne l'énoncé $\varphi(t_1, t_2, \dots, t_k)$. L'assertion ((5.5); M, φ, l, (E, J)) est alors banalement vraie.

4ᵉ cas: M, l et (E, J) sont quelconques;

$\varphi \equiv \exists y \psi$ où $\psi \in \mathrm{For}(L)$ telle que:

- le nombre des variables libres de ψ est k_1.
- ((5.5); M_1, ψ, l_1, (E_1, J_1)) est vraie pour tout langage du premier ordre M_1 obtenu en adjoignant des constantes à L, pour tout l_1 tel que $0 \leqq l_1 \leqq k_1 - 1$ et pour toute M_1-structure.

(Remarquons que nous avons besoin pour la première fois de la forme complète de l'hypothèse de récurrence; dans les cas 2 et 3, nous n'avons utilisé cette hypothèse que pour $M_1 = M$, $l_1 = l$ et $(E_1, J_1) = (E, J)$.)

Suivant que la variable y est libre ou non dans ψ, on a $VL(\psi)=\{x_1, \dots, x_k, y\}$ ou $VL(\psi)=\{x_1, \dots, x_k\}$. Dans les deux éventualités notons $\psi \equiv \psi(x_1, \dots, x_k, y)$. Nous pouvons donc écrire:

$$\varphi(t_1, \dots, t_k) \equiv \exists y \psi(t_1, \dots, t_k, y); \; \varphi_l(x_{l+1}, \dots, x_k) \equiv \exists y \psi_l(x_{l+1}, \dots, x_k, y).$$

L'assertion $(E, J) \models \varphi(t_1, \dots, t_k)$ équivaut à

$$\text{il existe } a \in E \text{ tel que } (E, J) \models \psi(t_1, \dots, t_k, y)\left[\frac{y}{a}\right] \tag{5.8}$$

L'assertion $(E, J) \models \varphi_l\left[\frac{x_{l+1}}{\tilde{t}_{l+1}}, \dots, \frac{x_k}{\tilde{t}_k}\right]$ équivaut à

$$\text{il existe } a \in E \text{ tel que } (E, J) \models \psi_l(x_{l+1}, \dots, x_k, y)\left[\frac{x_{l+1}}{\tilde{t}_{l+1}}, \dots, \frac{x_k}{\tilde{t}_k}, \frac{y}{a}\right] \tag{5.9}$$

Lorsque $y \notin VL(\psi)$, l'hypothèse de récurrence sur ψ implique immédiatement (5.8)$\Leftrightarrow$(5.9).

Considérons alors le cas où $y \in VL(\psi)$. Supposons que (5.8) est vérifiée. Introduisons un nouveau symbole de constante e (i.e. $e \notin \mathrm{Cst}(M)$. Désignons par M_1 le langage obtenu en adjoignant e aux constantes de M et soit J_1 l'interprétation de M_1 prolongeant J sur M, et telle que $J_1(e) := a (= \tilde{e})$. On a, en vertu de (5.8):

$$(E, J_1) \models \psi(t_1, \dots, t_k, y)\left[\frac{y}{\tilde{e}}\right]$$

En vertu de l'hypothèse ((5.5); M_1, ψ, k, (E_1, J_1)):

$$(E_1, J_1) \models \psi(t_1, \dots, t_k, e).$$

Puis, en vertu de l'hypothèse ((5.5); M, ψ, l, (E_1, J_1)):

$$(E_1, J_1) \models \psi_l(x_{l+1}, \ldots, x_k, y) \left[\frac{x_{l+1}}{\tilde{t}_{l+1}}, \ldots, \frac{x_k}{\tilde{t}_k}, \frac{y}{\tilde{e}} \right]$$

qui est évidemment équivalent à:

$$(E, J) \models \psi_l(x_{l+1}, \ldots, x_k, y) \left[\frac{x_{l+1}}{\tilde{t}_{l+1}}, \ldots, \frac{x_k}{\tilde{t}_k}, \frac{y}{\tilde{e}} \right]$$

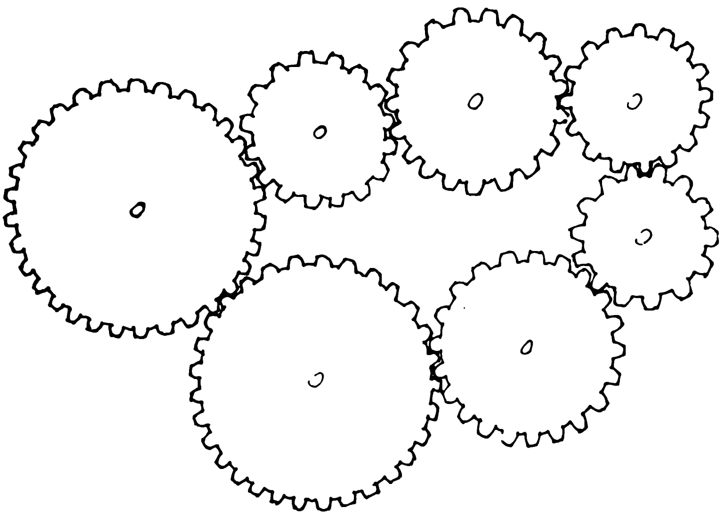
Cela implique (5.9).

La preuve que (5.9)$\Rightarrow$(5.8) se fait exactement de la même façon.

5^e^ cas: $\varphi \equiv \forall y \psi$ avec les même hypothèses qu'au 4^e^ cas sur ψ, M, l et (E, J).

Comme $(E, J) \models \varphi \Leftrightarrow$ (il est faux que $(E, J) \models \exists y(\neg \psi)$), le 5^e^ cas se ramène aux cas 2 et 4.

Cela achève la preuve de (5.5) □ ■



CHAPITRE 6

L'idée de preuve. Le théorème de complétude de la logique du premier ordre

6.0 INTRODUCTION

Nous parvenons maintenant à l'essentiel. Jusqu'ici nous avons fait ce qu'on pourrait appeler la "linguistique" des langages du premier ordre. Nous avons étudié la syntaxe et la sémantique ainsi que leurs rapports mutuels. Mais la logique est avant tout l'art d'élaborer, d'analyser ou de critiquer des raisonnements. C'est à quoi nous devons en venir.

Pour mieux sentir ce qui nous manque, partons d'un raisonnement formulé dans la langue ordinaire, soit le syllogisme typique:

	a est un *b*
tout	*b* est un *c*
donc	*a* est un *c*.

La conclusion présente deux caractères. D'une part, elle paraît construite mécaniquement à partir des deux prémisses. Le mécanisme est peut-être difficile à décrire (il ressemble un peu à la règle de simplification des fractions: $\frac{a}{b}\cdot\frac{b}{c}=\frac{a}{c}$) mais son existence ne fait pas de doute. On dit que la conclusion est *déduite* des deux prémisses. D'autre part, si on suppose "vraies" les deux prémisses, on est contraint d'admettre que la conclusion est "vraie" également.

Revenons à un langage du premier ordre L. Au lieu des phrases de la langue ordinaire, nous allons considérer des formules de L. Pour l'instant, nous ne disposons d'aucune règle permettant, à partir de deux formules données α et β, de "déduire" une nouvelle formule en combinant un morceau de α et un de β. En revanche, nous sommes moins démunis pour parler de "vérité". Considérons une L-structure (E, J) et une spécialisation s de (E, J). Il existe une fonction de vérité V_s sur For(L) telle que, pour toute $\alpha\in$For(L):

$$(E, J)\vDash\alpha[s]\Leftrightarrow V_s(\alpha)=1$$

(cf. prop. 3.1.10). Soit α et $\alpha\to\beta$ deux formules de L. Si $V_s(\alpha)=V_s(\alpha\to\beta)=1$, alors $V_s(\beta)==1$, en vertu des règles de la définition 3.1.8. Donc, de $(E, J)\vDash\alpha[s]$ et

$(E, J) \vDash (\alpha \to \beta)[s]$, on peut "déduire" que $(E, J) \vDash \beta[s]$. On est tenté d'adopter la règle d'inférence suivante: de α et $\alpha \to \beta$, on infère β.

On pourrait imaginer encore d'autres règles. Par exemple, si $V_s(\alpha \wedge \beta) = 1$, alors $V_s(\beta) = 1$. D'où: de $\alpha \wedge \beta$, on infère β. A l'aide de règles de ce genre et à partir de formules de L satisfaites dans la spécialisation s, on peut en trouver de nouvelles, également satisfaites dans s. Reste à trouver des formules de L satisfaites dans s. Heureusement nous en connaissons. Les tautologies, par exemple: si γ est une tautologie de L, $V_s(\gamma) = 1$; donc $(E, J) \vDash \gamma[s]$. La formule $(x = x)$, qui n'est pas une tautologie, est aussi satisfaite dans toute spécialisation s de (E, J).

Nous voyons apparaître deux notions nécessaires pour décrire l'idée d'inférence:

- une *base axiomatique logique* ou un *système d'axiomes logiques,* formés d'un ensemble de formules "universellement vraies" (comme $(x = x)$, par exemple);
- un ensemble de *règles d'inférence* (ou de *dérivation*) (telles que: de α et $\alpha \to \beta$, on infère β, par exemple).

La donnée de ces deux notions fixe le *système d'inférence* dans lequel on se place. C'est au sein d'un tel système qu'on peut définir l'idée de *preuve.*

Même si on se borne à la logique du premier ordre, il existe beaucoup de systèmes d'inférence distincts, bien qu'équivalents dans un sens que nous pourrons préciser plus loin. Nous allons décrire le système d'inférence de Hilbert pour un langage du premier ordre L. Il comporte une base axiomatique logique relativement vaste et peu de règles d'inférence, ce qui le rend d'un accès facile.

6.1 LE SYSTÈME D'INFÉRENCE DE HILBERT

6.1.0 Définition: le système d'inférence de Hilbert

Soit L un langage du premier ordre. On appelle:

1) *Axiomes logiques de L:*

- les tautologies
- les axiomes de l'égalité (voir chapitre 4)
- les *axiomes de spécification,* c'est-à-dire les formules du type:

  $\forall x\varphi \to \varphi^x_t$ et $\varphi^x_t \to \exists x\varphi$

  où $\varphi \in \mathrm{For}(L)$, $x \in \mathrm{Var}$ et $t \in \mathrm{Ter}(L)$ est un terme substituable à x dans φ.

2) *Règles d'inférence*

- *"modus ponens"*: si α et β sont des formules de L, de α et $\alpha \to \beta$ on dérive (ou infère) β;

- *règles de généralisation*: si φ et ψ sont des formules de L et x une variable,
  I) si $x \notin VL(\varphi)$, de $\varphi \to \psi$ on dérive (ou infère) $\varphi \to \forall x \psi$

  II) si $x \notin VL(\psi)$, de $\varphi \to \psi$ on dérive (ou infère) $\exists x \varphi \to \psi$

6.1.1 Remarques

- Les axiomes logiques ne sont pas nécessairement des énoncés de L.
- Il ne faut pas confondre "inférence" et "implication".
- Les axiomes des quantificateurs (définition 5.3.0) figurent parmi les axiomes de spécification. Mais ils ne les épuisent pas grâce à une plus grande liberté dans le choix des formules, des variables et des termes.

6.1.2 Définition

Soit L un langage du premier ordre et S un ensemble d'énoncés de L. Soit φ une formule de L. Une *preuve de φ à partir de S* dans le système d'inférence de Hilbert est une suite finie de formules $\psi_1, \psi_2, \ldots, \psi_n$ où:

i) $\psi_n \equiv \varphi$
ii) pour tout indice k, ψ_k est
  - soit un axiome logique de L
  - soit un énoncé de S
  - soit une formule dérivée selon les règles d'inférence de Hilbert de certaines ψ_j où $j<k$.

On dit alors que φ est *dérivable à partir de S* et on note $S \vdash \varphi$.

6.1.3 Notation

Nous utiliserons la notation $\dfrac{\alpha \ \beta}{\gamma}$ qui se lit "de α et β on dérive γ".

Par exemple, "*modus ponens*" se note $\dfrac{\alpha \quad \alpha \to \beta}{\beta}$ et les règles de généralisation deviennent

I) si $x \notin VL(\varphi)$ $\dfrac{\varphi \to \psi}{\varphi \to \forall x \psi}$

II) si $x \notin VL(\psi)$ $\dfrac{\varphi \to \psi}{\exists x \varphi \to \psi}$

6.1.4 Remarque

Il est facile d'obtenir d'autres règles d'inférence. Par exemple, comme $(\alpha \to \beta) \to (\neg \beta \to \neg \alpha)$ est une tautologie, donc un axiome logique, on peut écrire, par *modus ponens*

$$\frac{\alpha\to\beta \quad (\alpha\to\beta)\to(\neg\beta\to\neg\alpha)}{\neg\beta\to\neg\alpha}$$

Ainsi, à partir de $\alpha\to\beta$ on peut prouver $\neg\beta\to\neg\alpha$. On peut abréger cela en:

$$\frac{\alpha\to\beta}{\neg\beta\to\neg\alpha}.$$

Cette dérivation est appelée *règle de contraposition.*

6.1.5 Remarque

Soit $\varphi\in\mathrm{For}(L)$. Le premier axiome de spécification pour $\neg\varphi$ s'écrit $(\forall x\neg\varphi)\to(\neg\varphi_t^x)$, où t est un terme substituable à x dans φ. D'autre part, $(\neg\neg\alpha\to\neg\beta)\to(\alpha\to\neg\beta)$ est une tautologie.

On peut donc écrire successivement:

(contraposition) $$\frac{(\forall x\neg\varphi)\to(\neg\varphi_t)}{}$$

(*modus ponens*) $$\frac{(\neg\neg\varphi_t^x)\to(\neg\forall x\neg\varphi) \quad ((\neg\neg\varphi_t^x)\to(\neg\forall x\neg\varphi))\to(\varphi_t^x\to(\neg\forall x\neg\varphi))}{\varphi_t^x\to(\neg\forall x\neg\varphi)}$$

Si on considère que "$\exists x$" est une abréviation pour "$\neg\forall x\neg$", on constate que les deuxièmes axiomes de spécification sont dérivables à partir des seuls premiers axiomes de spécification.

6.1.6 Remarque

Soit φ, ψ, α, $\beta\in\mathrm{For}(L)$ et soit $x\in\mathrm{Var}$ telle que $x\notin VL(\psi)$. Comme $(\neg\alpha\to\neg\neg\beta)\to(\neg\alpha\to\beta)$ est une tautologie, on peut écrire successivement:

$$\begin{array}{ll}
\text{(contr.)} & \varphi\to\psi \\ \hline
\text{(1}^{\text{e}}\text{ de génér.)} & \neg\psi\to\neg\varphi \\ \hline
\text{(contr.)} & \neg\psi\to\forall x\neg\varphi \\ \hline
(m.p.) & \neg\forall x\neg\varphi\to\neg\neg\psi \quad (\neg\forall x\neg\varphi\to\neg\neg\psi)\to(\neg\forall x\neg\varphi\to\psi) \\ \hline
 & \neg\forall x\neg\varphi\to\psi
\end{array}$$

Donc, lorsque $x\notin VL(\psi)$, de $\varphi\to\psi$ on dérive $\neg\forall x\neg\varphi\to\psi$. Si on admet que "$\exists x$" est une abréviation pour "$\neg\forall x\neg$", on retrouve la deuxième règle de généralisation.

En conclusion, il résulte des remarques 6.1.5 et 6.1.6 que:

- on n'introduit aucune contradiction dans le système d'inférence de Hilbert lorsqu'on considère "$\exists x$" comme une abréviation de "$\neg\forall x\neg$";
- on peut se passer sans risque des deuxièmes axiomes de spécification et de la deuxième règle de généralisation. Nous en tiendrons compte par la suite en nous dispensant d'examiner systématiquement ces éventualités au cours de nos démonstrations.

6.2 QUELQUES LEMMES

6.2.0 Préambule

La démonstration du théorème de complétude requiert quelques faits que nous allons introduire sous forme de lemmes. Auparavant, nous allons convenir de quelques notations qui allègeront les écritures.

Si ψ est une formule de L et que $VL(\psi)\subset\{x\}$, nous avons décidé de noter $\psi\equiv\psi(x)$ pour attirer l'attention sur la variable x, même si $x\notin VL(\psi)$. Convenons de faire de même pour n'importe quelle formule $\psi\in\mathrm{For}(L)$. De plus, si z est une variable substituable à x dans ψ et si $z\notin VL(\psi)-\{x\}$, nous noterons $\psi(z)$ pour ψ^x_z.

6.2.1 Lemmes 1: (extension des règles de généralisation)

Soit x une variable et soit φ et $\psi(x)$ deux formules de L. Soit z une variable substituable à x dans $\psi(x)$ et n'appartenant pas à $VL(\psi(x))-\{x\}$. Si $x\notin VL(\varphi)$, alors:

6.2.1.0 $\dfrac{\varphi\to\psi(x)}{\varphi\to\forall z\psi(z)}$

6.2.1.1 $\dfrac{\psi(x)\to\varphi}{\exists z\psi(z)\to\varphi}$

6.2.2 Démonstration

La formule $\forall x\psi(x)\to\psi(z)$ est un axiome de spécification. Comme $z\notin VL(\psi(x))-\{x\}$, la première règle de généralisation s'applique à cette formule et on obtient:

$$\frac{\forall x\psi(x)\to\psi(z)}{\forall x\psi(x)\to\forall z\psi(z)}$$

D'autre part, comme $x\notin VL(\varphi)$, la première règle de généralisation s'applique à $\varphi\to\psi(x)$:

$$\frac{\varphi\to\psi(x)}{\varphi\to\forall x\psi(x)}.$$

En utilisant la tautologie $(\alpha\to\beta)\to((\beta\to\gamma)\to(\alpha\to\gamma))$ avec $\alpha, \beta, \gamma\in\mathrm{For}(L)$ et par *modus ponens:*

$$\frac{\varphi\to\forall x\psi(x)\quad(\varphi\to\forall x\psi(x))\to((\forall x\psi(x)\to\forall z\psi(z))\to(\varphi\to\forall z\psi(z)))}{(\forall x\psi(x)\to\forall z\psi(z))\to(\varphi\to\forall z\psi(z))}$$

Puis, à nouveau par *modus ponens:*

$$\frac{\forall x\psi(x)\to\forall z\psi(z) \quad (\forall x\psi(x)\to\forall z\psi(z))\to(\varphi\to\forall z\psi(z))}{\varphi\to\forall z\psi(z)}$$

Cela établit le lemme 6.2.1.0.

Le lemme 6.2.1.1 se démontre d'une manière analogue. □

Ainsi, dans l'application des règles de généralisation, on peut choisir presque arbitrairement le nom de la variable sur laquelle on quantifie.

6.2.3 Lemmes

Soit L un langage du premier ordre. Soit S un ensemble d'énoncés de L. Soit encore α, β, γ, φ et ψ des formules de L.

6.2.3.0 Si $S\vdash(\alpha\to\beta)$ *et* $S\vdash(\neg\alpha\to\beta)$, alors $S\vdash\beta$.

6.2.3.1 Si $S\vdash(\alpha\to\beta)\to\gamma$, alors $S\vdash(\beta\to\gamma)$ *et* $S\vdash(\neg\alpha\to\gamma)$.

Supposons en outre que x et y sont des variables telles que:

- $x\in VL(\varphi)$, $x\notin VL(\psi)$;
- y est substituable à x dans $\varphi(x)$;
- $y\notin VL(\varphi(x))-\{x\}$.

6.2.3.2 Si $S\vdash(\exists y\varphi(y)\to\varphi(x))\to\psi$, alors $S\vdash\psi$.

6.2.3.3 Si $S\vdash(\varphi(x)\to\forall y\varphi(y))\to\psi$, alors $S\vdash\psi$.

6.2.3.4 Si $S\vdash(\varphi(x)\to\forall y\varphi(y))\to((\exists y(\neg\varphi(y))\to(\neg\varphi(x)))\to\psi)$, alors $S\vdash\psi$.

6.2.4 Démonstration du lemme 6.2.3.0

Partons de la tautologie:

$(\alpha\to\beta)\to((\neg\alpha\to\beta)\to\beta)$.

En utilisant deux fois *modus ponens*, on obtient:

$$\frac{\dfrac{(\alpha\to\beta)\quad(\alpha\to\beta)\to((\neg\alpha\to\beta)\to\beta)}{(\neg\alpha\to\beta)\to\beta}\quad(\neg\alpha\to\beta)}{\beta}$$

Donc $S\vdash\beta$. □

6.2.5 Démonstration du lemme 6.2.3.1

Partons de la tautologie:

$((\alpha\to\beta)\to\gamma)\to(\beta\to\gamma)$.

Comme, par hypothèse, $S\vdash(\alpha\to\beta)\to\gamma$, on obtient immédiatement $S\vdash(\beta\to\gamma)$ à l'aide de *modus ponens*.

A partir de la tautologie $((\alpha\to\beta)\to\gamma)\to(\neg\alpha\to\gamma)$ et en appliquant à nouveau *modus ponens,* on obtient $S\vdash(\neg\alpha\to\gamma)$. □

6.2.6 Démonstration du lemme 6.2.3.2

De l'hypothèse de 6.2.3.2, le lemme 6.2.3.1 permet de tirer:

$$S\vdash\varphi(x)\to\psi \tag{6.0}$$

et

$$S\vdash(\neg\exists y\varphi(y))\to\psi. \tag{6.1}$$

De (6.0), le lemme 6.2.1.1 permet de tirer:

$$S\vdash\exists y\varphi(y)\to\psi. \tag{6.2}$$

A partir de (6.1) et (6.2), le lemme 6.2.3.0 permet de conclure que $S\vdash\psi$. □

6.2.7 Démonstration du lemme 6.2.3.3

De l'hypothèse de 6.2.3.3, le lemme 6.2.3.1 permet de tirer:

$$S\vdash\forall y\varphi(y)\to\psi \tag{6.3}$$

et

$$S\vdash(\neg\varphi(x))\to\psi. \tag{6.4}$$

En utilisant deux fois la tautologie $(\alpha\to\neg\neg\beta)\to(\alpha\to\beta)$, $\alpha,\beta\in\mathrm{For}(L)$, on a successivement:

$$\begin{array}{ll}
\text{(contr.)} & \underline{(\neg\varphi(x))\to\psi} \\
\text{(m.p.)} & \underline{\neg\psi\to\neg\neg\varphi(x) \qquad (\neg\psi\to\neg\neg\varphi(x))\to(\neg\psi\to\varphi(x))} \\
\text{(lemme 6.2.1.0)} & \underline{\neg\psi\to\varphi(x)} \\
\text{(contr.)} & \underline{\neg\psi\to\forall y\varphi(y)} \\
\text{(m.p.)} & \underline{\neg\forall y\varphi(y)\to\neg\neg\psi \qquad (\neg\forall y\varphi(y)\to\neg\neg\psi)\to(\neg\forall y\varphi(y)\to\psi)} \\
 & \qquad\qquad\qquad \neg\forall y\varphi(y)\to\psi.
\end{array} \tag{6.5}$$

A partir de (6.3) et (6.5), le lemme 6.2.3.0 permet de conclure que $S\vdash\psi$. □

6.2.8 Démonstration du lemme 6.2.3.4

De l'hypothèse de 6.2.3.4, le lemme 6.2.3.1 permet de tirer:

$$S\vdash\forall y\varphi(y)\to((\exists y(\neg\varphi(y))\to(\neg\varphi(x)))\to\psi) \tag{6.6}$$

et

$$S\vdash\neg\varphi(x)\to((\exists y(\neg\varphi(y))\to(\neg\varphi(x)))\to\psi). \tag{6.7}$$

A partir de (6.7), en utilisant les tautologies suivantes:

$$(\alpha\to((\beta\to\alpha)\to\gamma))\to(\alpha\to\gamma)$$

$$(\alpha\to\neg\neg\beta)\to(\alpha\to\beta) \qquad \text{(deux fois)}$$
$$(\alpha\to\beta)\to(\alpha\to((\gamma\to\delta)\to\beta))$$

où α, β, γ, $\delta\in\mathrm{For}(L)$, on peut écrire successivement:

$$\begin{array}{ll}
 & (\neg\varphi(x)\to((\exists y(\neg\varphi(y))\to(\neg\varphi(x)))\to\psi)) \quad ((\neg\varphi(x)\to((\exists y(\neg\varphi(y))\to \\
 & \to(\neg\varphi(x)))\to\psi))\to(\neg\varphi(x)\to\psi)) \\
\text{(m.p.)} & \overline{\neg\varphi(x)\to\psi} \\
\text{(contr.)} & \overline{\neg\psi\to\neg\neg\varphi(x)} \quad (\neg\psi\to\neg\neg\varphi(x))\to(\neg\psi\to\varphi(x)) \\
\text{(m.p.)} & \overline{\neg\psi\to\varphi(x)} \\
\text{(lemme 6.2.1.0)} & \overline{\neg\psi\to\forall y\varphi(y)} \\
\text{(contr.)} & \overline{\neg\forall y\varphi(y)\to\neg\neg\psi} \quad (\neg\forall y\varphi(y)\to\neg\neg\psi)\to(\neg\forall y\varphi(y)\to\psi) \\
\text{(m.p.)} & \overline{\neg\forall y\varphi(y)\to\psi} \quad (\neg\forall y\varphi(y)\to\psi)\to(\neg\forall y\varphi(y)\to((\exists y(\neg\varphi(y))\to \\
 & \qquad\qquad \to(\neg\varphi(x)))\to\psi)) \\
\text{(m.p.)} & \overline{(\neg\forall y\varphi(y))\to((\exists y(\neg\varphi(y))\to(\neg\varphi(x)))\to\psi).}
\end{array} \tag{6.8}$$

En appliquant le lemme 6.2.3.0 à (6.6) et (6.8), on obtient

$$S\vdash(\exists y(\neg\varphi(y))\to(\neg\varphi(x)))\to\psi$$

puis, grâce au lemme 6.2.3.2: $S\vdash\psi$. □

Le dernier lemme que nous établirons maintenant mérite d'être élevé au rang de proposition.

6.2.9 Proposition: lemme de rectitude (soundness lemma).

Soit L un langage du premier ordre. Soit S un ensemble d'énoncés de L et soit (E, J) un modèle de S. Enfin, soit φ une formule de L telle que $VL(\varphi)\subset\{x_1, x_2, \ldots, x_p\}\subset\mathrm{Var}$.

Si $S\vdash\varphi$, alors $(E, J)\models\forall x_1\forall x_2\ldots\forall x_p\varphi$.

6.2.10 Démonstration

Soit $\psi_1, \psi_2, \ldots, \psi_n\equiv\varphi$ une preuve de φ à partir de S. Nous dirons que cette preuve est de *longueur* n. Nous allons procéder par récurrence sur n.

6.2.10.0 *Cas où* $n=1$. Alors $\psi_1\equiv\varphi$. Il n'y a que deux possibilités:

A) φ est un axiome logique

B) φ est un énoncé de S.

A) Si φ est un axiome logique, trois éventualités peuvent se présenter:
A.0) Si φ est une tautologie: pour toute fonction de vérité V sur $\mathrm{For}(L)$ $V(\varphi)=1$; c'est le cas en particulier lorsque V est une fonction de vérité V_s, où s est une spécialisation quelconque de (E, J). Partons d'une spécialisation arbitraire s' de (E, J) et soit $a_1, a_2, \ldots, a_p$ des éléments de E. Considérons la spécialisation

$$s'_a := s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\ldots\left(\frac{x_p}{a_p}\right)$$

Remarquons que l'effet de s'_a sur φ ne dépend pas du choix de s'. Nous pouvons écrire successivement:

$V_{s'_a}(\varphi)=1$, quels que soient $a_1, a_2, \dots, a_p \in E \Leftrightarrow$
$\Leftrightarrow (E, J) \models \varphi[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\dots,\left(\frac{x_p}{a_p}\right)]$ quels que soient $a_1, a_2, \dots, a_p \in E \Leftrightarrow$
$\Leftrightarrow (E, J) \models \forall x_1 \forall x_2 \dots \forall x_p \varphi$.

A.1) φ est un axiome de l'égalité. Alors $(E, J) \models \varphi[s]$ pour toute spécialisation s de (E, J) (cf. prop. 4.1.1). C'est le cas en particulier pour la spécialisation s'_a ci-dessus. Par suite, $(E, J) \models \varphi[s'_a]$ quels que soient $a_1, \dots, a_p \in E$, donc $(E, J) \models \forall x_1 \forall x_2 \dots \forall x_p \varphi$.
A.2 φ est un axiome de spécification. Il est alors de l'une des formes:

A.2.0) $\varphi \equiv \forall y \theta \rightarrow \theta^y_t$
A.2.1) $\varphi \equiv \theta^y_t \rightarrow \exists x \theta$

où θ est une formule de L et t un terme de L substituable à la variable y dans θ. Soit s' une spécialisation de (E, J).

A.2.0) Si $\varphi \equiv \forall y \theta \rightarrow \theta^y_t$, de deux choses l'une:

ou bien $(E, J) \models \theta^y_t[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_1}{a_2}\right)\dots\left(\frac{x_p}{a_p}\right)]$ quels que soient $a_1, a_2, \dots, a_p \in E$ et,

dans ce cas, $(E, J) \models \varphi[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\dots\left(\frac{x_p}{a_p}\right)]$; quels que soient $a_1\ a_2 \dots, a_p \in E$;

ou bien il existe $a_1, a_2, \dots, a_p \in E$ tels que: $(E, J) \models (\neg \theta^y_t)\ [s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\dots\left(\frac{x_p}{a_p}\right)]$;

posons alors $b := s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\dots\left(\frac{x_p}{a_p}\right)(t)$;

il est clair que $(E, J) \models (\neg \theta[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\dots\left(\frac{y_p}{a_p}\right)\left(\frac{y}{b}\right)]$;

autrement dit, il est faux que:

$(E, J) \models (\forall y \theta)[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\dots\left(\frac{x_p}{a_p}\right)]$.

Par suite, quels que soient $a_1, a_2, \dots, a_p \in$E,

$(E, J) \models\ (\forall y \theta) \rightarrow \theta^y_t)[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\dots\left(\frac{x_p}{a_p}\right)]$,

ce qui équivaut à: $(E, J) \models \forall x_1\ \forall x_2 \dots\ \forall x_p\ (\forall y \theta \rightarrow \theta^y_t)$.

A.2.1) Les remarques formulées au numéro 6.1.5 nous dispensent d'examiner le cas des axiomes de spécification de la seconde espèce. Nous allons le faire néanmoins à titre d'exercice. Nous constaterons que le raisonnement est le même que pour A.2.0). Par la suite, nous renoncerons au plaisir d'effectuer ces démonstrations en partie double.

Partons donc de A.2.1) $\varphi \equiv \theta^y_t \rightarrow \exists y \theta^y_t$ où $\theta \in \mathrm{For}(L)$, t est un terme de L substituable à la variable y dans θ. Soit s' une spécialisation de (E, J). Soit

$a_1, a_2, \ldots, a_p \in E$. Alors:

ou bien $(E, J) \models (\neg \theta_t^y)[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\ldots\left(\frac{x_p}{a_p}\right)]$

ou bien $(E, J) \models (\theta_t^y)[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\ldots\left(\frac{x_p}{a_p}\right)]$;

dans ce dernier cas, posons $b := s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\ldots\left(\frac{x_p}{a_p}\right)(t)$;

il est clair que:

$(E, J) \models \theta[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\ldots\left(\frac{x_p}{a_p}\right)\left(\frac{y}{b}\right)]$

et par suite que:

$(E, J) \models (\exists y\theta)[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\ldots\left(\frac{x_p}{a_p}\right)]$.

Donc, quels que soient $a_1, a_2, \ldots, a_p \in$E:

$(E, J) \models (\theta_t^y \to \exists y\theta)[s'\left(\frac{x_1}{a_1}\right)\left(\frac{x_2}{a_2}\right)\ldots\left(\frac{x_p}{a_p}\right)]$,

ce qui équivaut à:

$(E, J) \models \forall x_1 \forall x_2 \ldots \forall x_p \varphi$.

B) Si φ est un énoncé pris dans S, $(E, J) \models \varphi$, par hypothèse. Il résulte immédiatement de la déf. 2.2.11 et du corollaire 2.2.21 que, pour toute variable x_p, $(E, J) \models \forall x_p \varphi$. En répétant le raisonnement successivement pour les variables $x_{p-1}, \ldots, x_2$ et x_1, on obtient: $(E, J) \models \forall x_1 \forall x_2 \ldots \forall x_p \varphi$.

6.2.10.1 *Cas où* $n > 1$. Supposons le lemme vrai pour toutes les preuves de longueur strictement inférieure à n. Soit $\psi_1, \psi_2, \ldots, \psi_n \equiv \varphi$ une preuve de φ à partir de S.

Si ψ_n est un axiome logique ou un énoncé de S, c'est le cas $n = 1$, qui se présente à nouveau. Mais si ψ_n est une formule dérivée de certains ψ_j où $j < n$, examinons ce qui se passe quand on effectue l'inférence qui produit ψ_n. Donnons-nous arbitrairement une spécialisation s' de (E, J) et examinons les deux cas possibles.

1) *Cas de modus ponens*. Admettons qu'il existe deux indices k et j inférieurs à n tels que:

$$\frac{\psi_k \ \psi_j}{\psi_n} \text{ où } \psi_j \equiv \psi_k \to \psi_n$$

L'hypothèse de récurrence nous permet d'écrire:

$(E, J) \models (\forall x_1 \forall x_2 \ldots \forall x_p \psi_k)[s']$ *et*
$(E, J) \models (\forall x_1 \forall x_2 \ldots \forall x_p (\psi_k \to \psi_n))[s']$.

Donc, quels que soient $a_1, a_2, \ldots, a_p \in E$

$$(E, J) \models \psi_k[s'\binom{x_1}{a_1}\binom{x_2}{a_2}\ldots\binom{x_p}{a_p}] \text{ et}$$

$$(E, J) \models (\psi_k \to \psi_n)[s'\binom{x_1}{a_1}\binom{x_2}{a_2}\ldots\binom{x_p}{a_p}],$$

d'où il découle: $(E, J) \models \psi_n[s'\binom{x_1}{a_1}\binom{x_2}{a_2}\ldots\binom{x_n}{a_n}]$

quels que soient $a_1, a_2, \ldots, a_p \in E$. Donc $(E, J) \models \forall x_1 \forall x_2 \ldots \forall x_p \psi_n$.

2) *Cas des règles de généralisation.* Nous savons qu'elles se ramènent toutes aux règles de généralisation de la première espèce. Bornons-nous donc à celles-ci.

Supposons qu'il existe un indice $k < n$ tel que $\psi_k \equiv \alpha \to \beta$, où $\alpha, \beta \in \mathrm{For}(L)$. Soit y une variable ne figurant pas dans les variables libres de α et admettons enfin que la formule ψ_n est obtenue à partir de ψ_k par généralisation: $\psi_n \equiv \alpha \to \forall y \beta$.

Commençons par montrer que, sous la condition que $y \notin VL(\alpha)$, pour toute spécialisation s de (E, J):

$$(E, J) \models (\forall y(\alpha \to \beta))[s] \Leftrightarrow (E, J) \models (\alpha \to \forall y \beta)[s]. \tag{6.9}$$

En effet, $(E, J) \models (\forall y(\alpha \to \beta))[s]$ équivaut à dire:

pour tout $b \in E : (E, J) \models (\alpha \to \beta)[s\binom{y}{b}]$,

ce qui, à son tour, équivaut à:

$$\left\{\begin{array}{l} (E, J) \models (\neg\alpha)[s] \\ \textit{ou}, \text{ pour tout } b,\ (E, J) \models \beta[s\binom{y}{b}]. \end{array}\right. \tag{6.10}$$

C'est à cet endroit qu'on fait usage de l'hypothèse $y \notin VL(\alpha)$. (6.10) équivaut à:

$$(E, J) \models (\neg\alpha)[s] \textit{ ou } (E, J) \models (\forall y \beta)[s],$$

ce qui se note encore: $(E, J) \models (\alpha \to \forall y \beta)[s]$.

Revenons à ψ_k. Il faut distinguer deux éventualités:

1er cas. $y \notin (x_1, x_2, \ldots, x_p)$. Alors $VL(\psi_k) \subset \{x_1, x_2, \ldots, x_p, y\}$. En vertu de l'hypothèse de récurrence:

$$(E, J) \models \forall x_1 \forall x_2 \ldots \forall x_p \forall y(\alpha \to \beta).$$

Or, à cause de (6.9): $(E, J) \models \forall x_1 \forall x_2 \ldots \forall x_p(\alpha \to \forall y \beta)$

Autrement dit $(E, J) \models \forall x_1 \forall x_2 \ldots \forall x_p \psi_n$.

2e cas. $y \in \{x_1, x_2, \ldots, x_p\}$. Supposons que $y \equiv x_1$. Alors $VL(\psi_k) \subset \{y, x_2, \ldots, x_p\}$. En vertu de l'hypothèse de récurrence:

$$(E, J) \models \forall x_2 \ldots \forall x_p \forall y(\alpha \to \beta)$$

Appliquons à nouveau la propriété (6.9):

$$(E, J) \models \forall x_2 \ldots \forall x_p(\alpha \to \forall y \beta)$$

Comme la formule de droite est un énoncé de L, elle est satisfaite dans toute spécialisation de (E, J). En particulier:

$$(E, J) \models \forall x_1 \forall x_2 \ldots \forall x_p (\alpha \rightarrow \forall y \beta)$$

ce qui achève la démonstration. □

6.2.11 Corollaire

Soit S un ensemble d'énoncés dans un langage du premier ordre L. Soit φ un énoncé de L.

Si $S \vdash \varphi$ alors, pour tout modèle (E, J) de S, $(E, J) \models \varphi$.

Ce corollaire signifie que si S admet un modèle, alors le système d'inférence de Hilbert permet de trouver des énoncés qui sont satisfaits dans tous les modèles de S. Il admet une réciproque qui n'est autre que la partie forte du théorème de complétude.

6.3 LE THÉORÈME DE COMPLÉTUDE

6.3.0 Préambule

Nous sommes maintenant en mesure d'établir le théorème central de la logique élémentaire du premier ordre.

6.3.1 Proposition: théorème de complétude de la logique du premier ordre (Gödel 1930)

Soit S un ensemble d'énoncés dans un langage du premier ordre L. Soit φ un énoncé de L.

La condition nécessaire et suffisante pour que φ admette une preuve à partir de S est que φ soit satisfait dans tout modèle de S.

6.3.2 Démonstration

La nécessité de cette condition est établie par le corollaire 6.2.11.

Démontrons-en la suffisance. Partons de l'hypothèse que, pour tout modèle (E, J) de S, $(E, J) \models \varphi$. Dans l'extension de Henkin $L(C)$ de L, considérons l'ensemble:

$$S \cup \{\neg \varphi\} \cup \mathrm{Leib}(L(C)) \cup \mathrm{Hen}(L) \tag{6.11}$$

S'il était LP-consistant, $S \cup \{\neg \varphi\}$ admettrait un modèle (E', J') en vertu de la proposition 5.4.2. Mais (E', J') serait aussi un modèle de S, où φ serait satisfait par hypothèse. On aurait donc $(E', J') \models \varphi$ et $(E', J') \models \neg\varphi$, ce qui est impossible. Donc l'ensemble (6.11) n'est pas LP-consistant (nous dirons qu'il est "LP-inconsistant").

Selon le théorème de compacité de la logique des propositions (prop. 5.5.1), il existe dans (6.11) une partie finie LP-inconsistante T. Or $T \cup \{\neg\varphi\}$ est aussi LP-inconsistant. Enumérons sans répétitions l'ensemble $T \cup \{\neg\varphi\}$ en posant:

$$T \cup \{\neg\varphi\} = \{\alpha_1, \alpha_2, \dots, \alpha_p, \beta_1, \beta_2, \dots, \beta_p, \neg\varphi\} \tag{6.12}$$

Dans le membre de droite, les éléments sont rangés selon les règles suivantes:

- pour $i = 1, 2, \dots, p$, α_i est ou dans S, ou dans Leib($L(C)$), ou encore dans les axiomes des quantificateurs (cf. déf. 5.3.0);
- pour $k = 1, 2, \dots, q$, β_k est un axiome de Henkin, c'est-à-dire un énoncé de l'une des formes
  $\exists x \psi(x) \to \psi(c_\psi)$ ou $\psi(c_{\neg\psi}) \to \forall x \psi(x)$
  avec $\psi \in \mathrm{For}(L(C))$, et $VL(\psi(x)) \subset \{x\}$;
- les axiomes β_k sont en outre ordonnés comme suit: chaque β_k introduit une constante de Henkin c_k de la forme c_ψ de hauteur maximum qui lui est propre; une même constante de Henkin n'est propre à plusieurs axiomes de Henkin que si elle est de la forme $c_{\neg\psi}$; elle est alors introduite par les axiomes de Henkin: $\exists x \neg\psi(x) \to \neg\psi(c_{\neg\psi})$ et $\psi(c_{\neg\psi}) \to \forall x \psi(x)$, et par eux seuls; notons $h(\beta_k)$ la hauteur de c_k (cf. déf. 5.2.2); on range alors les β_k de sorte que
  $$j < k \Rightarrow h(\beta_j) \geq h(\beta_k).$$
  De plus, quitte à renuméroter les β_k de même "hauteur", on exige que, si β_i et β_j, $(i<j)$, sont tels que $c_i = c_j$, $j = i+1$, $\beta_i \equiv \psi(c_{\neg\psi}) \to \forall x \psi(x)$ et $\beta_{i+1} \equiv \exists x \neg\psi(x) \to \psi(c_{\neg\psi})$. De la sorte, si c_j est la constante de Henkin propre à β_j, elle n'apparaît plus dans β_k quand $k > j$, sauf éventuellemment dans β_{j+1}.

Comme $\{\alpha_1, \alpha_2, \dots, \alpha_p, \beta_1, \beta_2, \dots, \beta_q, \neg\varphi\}$ est LP-inconsistant, la formule

$$\Omega \equiv (\alpha_1 \to (\alpha_2 \to \dots \to (\alpha_p \to (\beta_1 \to (\beta_2 \to \dots (\beta_q \to \varphi)) \dots) \tag{6.13}$$

est une tautologie: en effet, soit V une fonction de vérité sur For($L(C)$); si $V(\varphi) = 1$, alors $V(\Omega) = 1$; si $V(\varphi) = 0$, alors $V(\neg\varphi) = 1$; donc V s'annule sur l'un au moins des α_i ou des β_k et, par suite, $V(\Omega) = 1$.

Soit $D = \{d_1, d_2, \dots, d_m\}$ l'ensemble des constantes de Henkin de L apparaissant dans Ω. On a évidemment $\Omega \in \mathrm{For}(L(C))$. Choisissons alors m symboles de variables distincts: $x_1, x_2, \dots, x_m$, dont aucun ne figure dans Ω. A toute formule $\xi \in \mathrm{For}(L(D))$, attachons la formule ξ' de L obtenue en remplaçant, dans ξ, d_i par x_i, avec $i = 1, 2, \dots, m$. Formulons quelques remarques simples:

1) tout x_i apparaissant dans ξ' y est libre, car, dans ξ, aucun quantificateur ne porte sur une constante de Henkin;
2) si ξ est une formule première, ξ' l'est aussi, et réciproquement;
3) si $\xi \equiv \neg\alpha$ (avec $\alpha \in \mathrm{For}(L(D))$), alors $\xi' = \neg\alpha'$;
4) si $\xi \equiv \alpha * \beta$ (avec $\alpha, \beta \in \mathrm{For}(L(D))$ où $*$ désigne l'un des connecteurs $\wedge, \vee, \to, \leftrightarrow$), $\xi' \equiv \alpha' * \beta'$;
5) si $\xi \equiv (t_1 = t_2)$, avec $t_1, t_2 \in \mathrm{Ter}(L(D))$, alors $\xi' \equiv (t'_1 = t'_2)$, où t'_i désigne le terme de L obtenu en remplaçant, dans t_i, chaque d_k par x_k, $k = 1, 2, \dots, m$, $i = 1, 2$.

6) si $\xi \in \mathrm{For}(L)$, alors $\xi' \equiv \xi$. En particulier, $\varphi' \equiv \varphi$.

Il est facile de voir que

$$\Omega' \equiv (\alpha'_1 \to (\alpha'_2 \to \ldots \to (\alpha'_p \to (\beta'_1 \to (\beta'_2 \to \ldots \beta'_q \to \varphi))\ldots)$$

est une tautologie dans For(L). En effet, soit V une fonction de vérité quelconque sur For(L). Pour toute formule première θ de $L(D)$, posons $\bar{V}(\theta) := V(\theta')$. On détermine ainsi une fonction de vérité $\bar{V}$ sur For($L(D)$). En vertu de 1), 2), 3), 4), 5), on a, pour tout $\psi \in \mathrm{For}(L(D))$, $\bar{V}(\psi) = V(\psi')$. Donc, en particulier, $V(\Omega') = \bar{V}(\Omega) = 1$.

Remarquons maintenant que:

7) si $\alpha_i \in S$, alors $\alpha'_i \equiv \alpha_i$ (cf. remarque 6));
8) si $\alpha_i \in \mathrm{Leib}(L(D))$, alors $\alpha'_i \in \mathrm{Leib}(L)$;
9) si α_i est un axiome des quantificateurs de $L(D)$, alors α'_i est un axiome de spécification dans L.

Considérons en effet le cas où α_i est l'axiome des quantificateurs $Q_2(\psi, t)$, dans lequel ψ est une formule de $L(D)$ et t un terme clos de $L(D)$: $\alpha_i \equiv \forall x \psi \to \psi^x_t$. Désignons comme jusqu'ici par t' le terme de L obtenu en remplaçant, dans t, d_k par x_k, $k = 1, 2, \ldots, m$. Etant clos, t est évidemment substituable à x dans ψ. Il en résulte que t' est substituable à x dans ψ'. Cela tient à la remarque 1): les obstacles à la substitution de t' ne pourraient naître que de la présence dans ψ' de quantificateurs portant sur des variables figurant dans t'; or, comme t est clos, les seules variables de t' proviennent des constantes de Henkin apparaissant dans t et, répétons-le, on ne quantifie pas sur les constantes.

Donc, $S \vdash \alpha'_i$, pour $i = 1, 2, \ldots, p$. A l'aide de *modus ponens* appliquée p fois de suite à la tautologie Ω', on dérive la formule

$$(\beta'_1 \to (\beta'_2 \to \ldots \to (\beta'_q \to \varphi))\ldots). \tag{6.14}$$

La dernière étape de la démonstration consiste à montrer que si

$$S \vdash (\beta'_i \to (\beta'_{i+1} \to \ldots \to (\beta'_q \to \varphi))\ldots) \text{ avec } i \in \{1, 2, \ldots q\} \tag{6.15}$$

alors

$$\begin{aligned} &\text{ou bien } S \vdash (\beta'_{i+1} \to \ldots \to (\beta'_q \to \varphi))\ldots) \\ &\text{ou bien } S \vdash (\beta'_{i+2} \to \ldots \to (\beta'_q \to \varphi))\ldots), \end{aligned} \tag{6.16}$$

où on admet que $\beta'_{q+1} \equiv \beta'_{q+2} \equiv \varphi$.

Il convient de distinguer deux cas.

1^er^ cas: si β'_i est formé à partir d'un axiome de Henkin du type $H_1(\xi) \equiv \exists y \xi(y) \to \xi(c_\xi)$, alors

$$\beta'_i \equiv \exists y \xi'(y) \to \xi'(z_i)$$

où z_i désigne la variable de $\{x_1, x_2, \ldots, x_m\}$ qui a remplacé c_ξ. L'hypothèse (6.15) s'écrit

$$S \vdash ((\exists y \xi'(y) \to \xi'(z_i)) \to (\beta'_{i+1} \to \ldots \to (\beta'_q \to \varphi))\ldots).$$

La variable z_i ne figure pas dans $(\beta'_{i+1}\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots)$ à cause de la convention de numérotation des β_k et y est substituable à z_i dans $\xi'(z_i)$, car on a substitué c_ξ à y, puis remplacé typographiquement c_ξ par z_i qui est distinct de y. De plus, $y\notin VL(\xi'(z_i))-\{z_i\}$. Donc, en vertu du lemme 6.2.3.2, on a $S\vdash(\beta'_{i+1}\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots)$.

2^e *cas*: si β'_i est formé à partir d'un axiome de Henkin du type $H_2(\xi)\equiv\xi(c_{\neg\xi})\rightarrow\forall y\xi(y)$, alors

$$\beta'_i\equiv\xi'(z_i)\rightarrow\forall y\xi'(y),$$

où z_i désigne la variable de $\{x_1, x_2, \ldots, x_m\}$ qui a remplacé $c_{\neg\xi}$. L'hypothèse (6.15) s'écrit alors:

$$S\vdash((\xi'(z_i)\rightarrow\forall y\xi'(y))\rightarrow(\beta'_{i+1}\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots).$$

Deux éventualités peuvent se présenter:

- si la variable z_i ne figure pas dans $(\beta'_{i+1}\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots)$, on utilise le lemme 6.2.3.3, et on conclut, comme précédemment, que $S\vdash(\beta'_{i+1}\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots)$;
- si la variable z_i figure dans $(\beta'_{i+1}\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots)$, elle ne peut apparaître que dans β'_{i+1} à cause de la manière de numéroter les β_k, et $\beta'_{i+1}\equiv\exists y\neg\xi'(y)\rightarrow\neg\xi'(z_i)$, z_i désignant toujours la variable de $\{x_1, x_2, \ldots, x_m\}$ qui a remplacé $c_{\neg\xi}$. L'hypothèse (6.15) s'écrit alors:
  $S\vdash((\xi'(z_i)\rightarrow\forall y\xi'(y))\rightarrow((\exists y\neg\xi'(y)\rightarrow\neg\xi'(z_i))\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots)$
  z_i n'apparaît pas dans $(\beta'_{i+2}\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots)$. Comme y est substituable à z_i dans $\xi'(z_i)$ et que, de plus, $y\notin VL(\xi'(z_i))-\{z_i\}$, en vertu du lemme 6.2.3.4, on a: $S\vdash(\beta'_{i+2}\rightarrow\ldots\rightarrow(\beta'_q\rightarrow\varphi))\ldots)$.

Nous avons montré précédemment que l'hypothèse (6.15) est satisfaite pour $i=1$. Par application itérée de (6.16), nous déduisons que $S\vdash\varphi$. □

6.3.3 Corollaire

Reprenons les notations de la proposition 6.3.1. Si ψ est une formule de L telle que $VL(\psi)\subset\{x_1, x_2,\ldots, x_p\}$, alors: $S\vdash\psi\Leftrightarrow S\vdash\forall x_1\forall x_2\ldots\forall x_p\psi$.

6.3.4 Démonstration

6.3.4.0 Suffisance de la condition $S\vdash\psi$

Si $S\vdash\psi$, la proposition 6.2.9 permet d'affirmer que, pour tout modèle (E, J) de S, $(E, J)\models\forall x_1\forall x_2\ldots\forall x_p\psi$. En vertu du théorème de complétude, $S\vdash\forall x_1\forall x_2\ldots\forall x_p\psi$.

6.3.4.1 Nécessité de la condition $S\vdash\psi$

Nous allons montrer que si $S\vdash\forall x_i\forall x_{i+1}...\forall x_p\psi$, alors $S\vdash\forall x_{i+1}...\forall x_p\varphi$ pour tout $i\in\{1, 2, \ldots, p\}$, et où $\forall x_{i+1}...\forall x_p\psi$ désigne ψ quand $i=p$. Comme, par hypothèse, $S\vdash\forall x_1\forall x_2...\forall x_p\psi$, on déduit de proche en proche que $S\vdash\psi$.

Supposons que $S\vdash\forall x_i\forall x_{i+1}...\forall x_p\psi$. Posons $\xi:\equiv\forall x_{i+1}...\forall x_p\psi$. Comme x_i est un terme substituable à x_i dans ξ, $\forall x_i\xi\rightarrow\xi^{x_i}_{x_i}$ est un axiome de spécification. Donc, en appliquant *modus ponens*, on infère $S\vdash\xi^{x_i}_{x_i}$, c'est-à-dire $S\vdash\xi$ ou encore $S\vdash\forall x_{i+1}...\forall x_p\psi$. □

6.3.5 Définition

Un *système formel du premier ordre* est un couple (L, S) où L est un langage du premier ordre et S un ensemble d'énoncés de L. On dit que S est l'ensemble des axiomes non logiques du système formel (L, S).

Un système formel du premier ordre (L, S) est dit *consistant* (pour la logique du premier ordre) s'il existe un énoncé dans $\mathrm{For}(L)$ qui n'admet pas de preuve à partir de S. On dit aussi dans ce cas que (L, S) est une *théorie* du premier ordre. Tout énoncé $\alpha\in\mathrm{For}(L)$ qui admet une preuve à partir de S est alors appelé un *théorème* de la théorie (L, S).

6.3.6 Remarque

Si le système formel (du premier ordre) (L, S) n'est pas une théorie, alors $S\vdash\alpha$ pour tout énoncé $\alpha\in\mathrm{For}(L)$. En particulier, si α est un énoncé quelconque de L, $S\vdash\alpha\wedge(\neg\alpha)$. C'est pourquoi on dit aussi d'un système formel inconsistant qu'il *implique contradiction.*

6.3.7 Remarque

Réciproquement, si $S\vdash\alpha\wedge(\neg\alpha)$ pour un certain énoncé α de L, (L, S) est inconsistant. En effet, si β est un énoncé de L, $(\alpha\wedge(\neg\alpha))\rightarrow\beta$ est une tautologie; par *modus ponens* on conclut que $S\vdash\beta$ pour tout énoncé de L.

6.3.8 Remarque

$(L, \varnothing)$ est une théorie. En effet, toutes les L-structures sont des modèles de $\varnothing$. L'énoncé $\forall x(\neg(x=x))$ n'est satisfait dans aucune d'elles. Donc il n'existe pas de preuve de $\forall x(\neg(x=x))$ à partir de $\varnothing$. Si α est un théorème dans $(L, \varnothing)$, on note souvent: $\vdash\alpha$.

6.3.9 Remarque

Le corollaire 6.3.3 montre que, dans toute théorie du premier ordre (L, S), la preuve d'une formule φ peut être prolongée en une preuve d'un énoncé de la forme $\forall x_1 \forall x_2 ... \forall x_p \varphi$ où $VL(\varphi)=\{x_1, x_2, ..., x_p\}$. (On dit parfois que cet énoncé est obtenu en *saturant* φ.) Réciproquement, une preuve de l'énoncé obtenu en saturant φ peut se prolonger en une preuve de φ.

Ce phénomène apparaît constamment en mathématiques. Par exemple, "soit ABC un triangle; les médiatrices de ABC sont concourantes" peut être considéré comme une formule non saturée dans une théorie de la géométrie euclidienne plane. L'énoncé obtenu en saturant cette formule est: "quel que soit le triangle ABC, les médiatrices de ABC sont concourantes". On passe de l'une à l'autre et inversement sans y penser.

6.3.10 Proposition

Soit (L, S) un système formel du premier ordre. La condition nécessaire est suffisante pour que (L, S) soit consistant pour la logique du premier ordre est que S admette un modèle.

6.3.11 Démonstration

6.3.11.0 Suffisance

Supposons que S admette un modèle (E, J). Soit α un énoncé de L. Il est faux que $(E, J) \models \alpha \wedge (\neg \alpha)$. Donc, en vertu du théorème de complétude, il n'existe pas de preuve de $\alpha \wedge (\neg \alpha)$ à partir de S. Par suite, (L, S) est consistant.

6.3.11.1 Nécessité

Supposons (L, S) consistant pour la logique du premier ordre. Supposons par absurde que S n'admette pas de modèle. En vertu du théorème de compacité de la logique du premier ordre (prop. 5.5.1), il existe une partie finie T de S qui n'admet pas de modèle. On peut supposer, sans restriction, que T est minimal en ce sens que toute partie propre de T admet un modèle. Notons $T=\{\alpha_1, \alpha_2, ..., \alpha_r\}$. $r>0$ d'après la remarque 6.3.8.

α_r n'est satisfait dans aucun modèle de $T-\{\alpha_r\}$. Donc $(\neg \alpha_r)$ est satisfait dans tous les modèles de $T-\{\alpha_r\}$. En vertu du théorème de complétude: $T-\{\alpha_r\} \vdash (\neg \alpha_r)$. Et par suite: $T \vdash (\neg \alpha_r)$. Mais il est clair que $T \vdash \alpha_r$. D'où il découle que:

$$T \vdash (\alpha_r \wedge (\neg \alpha_r)). \tag{6.17}$$

(En effet, quelle que soient les formules φ et ψ de L, $(\varphi \rightarrow (\psi \rightarrow (\varphi \wedge \psi)))$ est une tautologie. D'où les inférences:

$$(\text{m.p}) \; \dfrac{\dfrac{\varphi \quad (\varphi \rightarrow (\psi \rightarrow (\varphi \wedge \psi)))}{\psi \rightarrow (\varphi \wedge \psi)} \quad \psi}{\varphi \wedge \psi}.)$$

Or, (6.17) contredit l'hypothèse selon laquelle (L, S) est consistant. Donc S admet un modèle. □

6.3.12 Proposition

Soit (L, S) une théorie du premier ordre.

Soit φ un énoncé de L non dérivable à partir de S. Alors, il existe un modèle (E, J) de S tel que $(E, J) \models (\neg \varphi)$.

6.3.13 Démonstration

Par hypothèse, il est faux que $S \vdash \varphi$. En vertu du théorème de complétude, il est faux que φ soit satisfait dans tout modèle de S. Autrement dit, il existe au moins un modèle de S dans lequel $(\neg \varphi)$ est satisfait. □

6.3.14 Remarque

Historiquement, la proposition 6.3.12 a reçu au moins une illustration éclatante. Ce fut à l'occasion de la découverte des géométries non euclidiennes planes. La géométrie plane d'Euclide avait toutes les apparences d'une théorie du premier ordre avant la lettre. Parmi ses axiomes non logiques figurait le "cinquième axiome" dit "d'Euclide" ou "des parallèles": par tout point pris hors d'une droite, il existe une parallèle à cette droite et une seule. Longtemps, cette propriété a paru si évidente qu'on s'est demandé s'il n'en existait pas une preuve à partir des autres axiomes de la géométrie euclidienne plane. Cependant, tous les efforts pour trouver cette preuve restèrent vains. La plupart des géomètres étaient disposés à admettre que l'axiome d'Euclide n'était pas un théorème dérivable à partir des autres axiomes de la géométrie euclidienne plane. La proposition 6.3.12 nous permet aujourd'hui de penser qu'il était alors raisonnable de rechercher un modèle des autres axiomes de la géométrie euclidienne plane, modèle ne vérifiant pas l'axiome des parallèles.

En fait, le problème fut attaqué des deux côtés à la fois. D'une manière logique d'abord: Lobatchevsky, Bolyai et Gauss développèrent, sans contradiction apparente, une "théorie" où l'axiome d'Euclide était remplacé par celui-ci: "par tout point pris hors d'une droite, il existe une infinité de parallèles à cette droite"; pour sa part, Riemann développa de même une "théorie" géométrique où l'axiome d'Euclide était remplacé par: "il n'existe pas de droites distinctes parallèles". Une seconde voie d'approche consiste à tenter de construire des modèles de ces géométries non euclidiennes, comme on vient de le dire. Riemann y parvint en remplaçant le plan ordinaire par le plan projectif réel muni d'une métrique qui convenait à la "géométrie riemannienne plane". Beltrami obtint un résultat analogue, donnant un modèle de la géométrie plane de Lobatchevsky en substituant au plan euclidien une surface appelée pseudo-sphère. Par la suite, Poincaré et Klein donnèrent des modèles encore plus simples des géométries non euclidiennes. Cette seconde voie a l'avantage de prouver que, sous cette réserve de la consistance de la géométrie euclidienne, les géométries planes de Lobatchevsky et de Riemann sont consistantes.

6.3.15 Remarque

Le théorème de complétude permet de démontrer facilement des propositions qu'on peut établir d'une façon purement formelle, mais avec plus de peine. Ainsi, par exemple:

6.3.16 Proposition: théorème de déduction

Soit (L, S) un système formel du premier ordre. Soit α et β deux énoncés de L. Alors:

$S \vdash \alpha \rightarrow \beta \Leftrightarrow S \cup \{\alpha\} \vdash \beta$.

6.3.17 Démonstration

La conclusion est banale si (L, S) n'est pas une théorie. Considérons donc le cas où (L, S) est une théorie.

Si $S \vdash (\alpha \rightarrow \beta)$, alors $S \cup \{\alpha\} \vdash (\alpha \rightarrow \beta)$, évidemment. Comme $S \cup \{\alpha\} \vdash \alpha$, il résulte, moyennant *modus ponens*, que $S \cup \{\alpha\} \vdash \beta$.

Réciproquement, admettons que $S \cup \{\alpha\} \vdash \beta$. Soit (E, J) un modèle de S. Alors:

- ou bien $(E, J) \models \beta$
- ou bien $(E, J) \models (\neg \beta)$; dans ce cas, $(E, J) \models (\neg \alpha)$. En effet, si $(E, J) \models \alpha$, (E, J) serait un modèle de $S \cup \{\alpha\}$. En vertu du théorème de complétude et de l'hypothèse $S \cup \{\alpha\} \vdash \beta$, $(E, J) \models \beta$.

Par suite, $(E, J) \models \alpha \rightarrow \beta$. Ce raisonnement étant valable pour tout modèle de S, le théorème de complétude permet de conclure que $S \vdash \alpha \rightarrow \beta$. □

6.3.18 Corollaire: théorème de la preuve par l'absurde

Soit (L, S) une théorie du premier ordre. Soit α un énoncé de L. Si $(L, S \cup \{\neg \alpha\})$ est un système formel inconsistant, alors $S \vdash \alpha$, et réciproquement.

6.3.19 Démonstration

Si $(L, S \cup \{\neg \alpha\})$ est inconsistant, $S \cup \{\neg \alpha\} \vdash \alpha \wedge (\neg \alpha)$. D'après la proposition 6.3.16, $S \vdash (\neg \alpha) \rightarrow (\alpha \wedge \neg \alpha))$. Mais $((\neg \alpha) \rightarrow (\alpha \wedge (\neg \alpha))) \rightarrow \alpha$ est une tautologie. En vertu de la règle *modus ponens*, $S \vdash \alpha$.

Si $S \vdash \alpha$, $S \cup \{\neg \alpha\} \vdash \alpha \wedge (\neg \alpha)$: il suffit de partir de la tautologie $\alpha \rightarrow ((\neg \alpha) \rightarrow (\alpha \wedge (\neg \alpha)))$ et d'appliquer deux fois la règle *modus ponens*. Donc $(L, S \cup \{\neg \alpha\})$ est inconsistant. □

6.3.20 Commentaire

Commentons un peu la proposition 6.3.16. Elle nous enseigne qu'il revient au même de prouver l'énoncé $\alpha \to \beta$ dans le système formel (L, S) ou l'énoncé β dans $(L, S \cup \}\alpha\})$.

A titre d'exemple, considérons le système formel $(L_3, \{\varphi_1, \varphi_2, \varphi_3\})$ présenté à l'exemple 5.5.4. Nous savons qu'il admet des modèles. C'est donc une théorie: la théorie des groupes. On peut prouver (ce que nous ne ferons pas ici, mais qui constitue un excellent exercice) que:

$$(L_3, \{\varphi_1, \varphi_2, \varphi_3\}) \vdash (\forall x \forall y (x \cdot y = y \cdot x)) \to (\forall x \forall y \forall x' \forall y' ((x \cdot x' = e \wedge y \cdot y' = e) \to ((x \cdot y) \cdot (x' \cdot y') = e)))$$

Intuitivement, $x \cdot x' = e$ se traduit par "x' est le *symétrique* de x"; $x \cdot y = y \cdot x$ s'exprime en disant que "x et y *commutent*". L'expression ci-dessus s'interprète alors ainsi: dans un groupe, si tous les éléments commutent deux à deux, alors le symétrique du produit de deux éléments quelconques égale le produit des symétriques de ces éléments.

D'après la proposition 6.3.16, il revient au même d'établir:

$$(L_3, \{\varphi_1, \varphi_2, \varphi_3\} \cup \{\forall x \forall y (x \cdot y = y \cdot x\}) \vdash (\forall x \forall y \forall x' \forall y' ((x \cdot x' = e \wedge y \cdot y' = e) \to ((x \cdot y) \cdot (x' \cdot y') = e))). \tag{6.18}$$

Le système formel $(L_3, \{\varphi_1, \varphi_2, \varphi_3, \forall x \forall y (x \cdot y = y \cdot x)\})$ admet un modèle: celui de l'exemple 2.2.24, fig. (2.2). C'est la *théorie des groupes commutatifs* (ou *abéliens*), groupes dont les éléments commutent deux à deux. On peut interpréter (6.18) ainsi: dans un groupe abélien, le symétrique du produit de deux éléments quelconques égale le produit des symétriques de ces éléments.

Dans la pratique, les choses se présentent encore un peu autrement. Pour reprendre l'exemple ci-dessus, adjoignons au langage L_3 un nouveau symbole de relation binaire que nous noterons $C(,)$. On peut alors montrer que:

$$\begin{aligned}(L_3 \cup \{C\}, \{\varphi_1, \varphi_2, \varphi_3\}) \vdash (\forall x \forall y C(x, y) \leftrightarrow (x \cdot y = y \cdot x)) \to \\ (\forall x \forall y \forall x' \forall y' ((C(x, y) \wedge (x \cdot x') = e \wedge (y \cdot y') = e) \\ \to (x \cdot y) \cdot (x' \cdot y') = e)).\end{aligned}$$

Ce qui signifie intuitivement que, dans un groupe, lorsque deux éléments commutent, le symétrique de leur produit égale le produit des symétriques de ces éléments. En vertu de la proposition 6.3.16, on peut aussi écrire:

$$\begin{aligned}&(L_3 \cup \{C\}, \{\varphi_1, \varphi_2, \varphi_3\} \cup \{(\forall x \forall y C(x, y) \leftrightarrow (x \cdot y = y \cdot x))\}) \vdash \\ &\forall x \forall y \forall x' \forall y' ((C(x, y) \wedge (x \cdot x') = e \wedge (y \cdot y') = e) \to (x \cdot y) \cdot (x' \cdot y') = e).\end{aligned}$$

Ainsi on ajoute au langage formel un nouveau symbole et on pose un nouvel axiome qui donne les propriétés de ce symbole. Cela revient à introduire une *définition*. Dans un ouvrage sur la théorie des groupes, on verra apparaître:

"*Définition*: quels que soient les éléments x et y d'un groupe G, on dira que x et y commutent et on notera $C(x, y)$ lorsque $x \cdot y = y \cdot x$."

Nous reviendrons ultérieurement sur le thème de complétude de la logique du premier ordre. Bornons-nous ici à deux remarques très simples.

6.3.21 Remarque

Soit (L, S) une théorie du premier ordre quelconque. Le système d'inférence de Hilbert permet de prouver tous les énoncés satisfaits dans tous les modèles de (L, S). Aucun autre système d'inférence ne saurait aller au-delà, sans introduire de discrimination entre les modèles de (L, S). Les systèmes d'inférence les plus intéressants en logique du premier ordre sont ceux qui ont exactement la même force que le système de Hilbert. Il en existe beaucoup. Celui de Hilbert convient bien à la démonstration du théorème de complétude. D'autres systèmes se prêtent mieux à la description des raisonnements pratiques ou à d'autres recherches théoriques.

6.3.22 Remarque

Reprenons une théorie quelconque du premier ordre (L, S). Le système d'inférence de Hilbert permet de prouver tous les théorèmes de (L, S) même si on ignore la notion de modèle ensembliste de (L, S). On pourrait alors oublier tout des interprétations sémantiques que l'on a données aux formules du premier ordre. La logique du premier ordre redeviendrait ainsi purement formelle.

CHAPITRE 7

Extension de la logique élémentaire du premier ordre

7.0 COMPLÉMENTS SUR LES ENSEMBLES

7.0.0 Quelques questions

La logique du premier ordre que nous avons considérée jusqu'ici était *élémentaire* en ceci que les langages considérés comportaient des ensembles de symboles propres finis ou dénombrables. Cette hypothèse s'impose, nous l'avons vu, lorsqu'on exige que toute formule puisse être effectivement écrite, à la rigueur par une machine. On peut toutefois soulever quelques questions. L'hypothèse mentionnée constitue-t-elle une véritable restriction? Peut-on imaginer des langages du premier ordre qui ne soient pas élémentaires au sens que nous avons dit? Le cas échéant, les théorèmes établis aux paragraphes précédents restent-ils valides? Nous allons essayer d'y répondre.

7.0.1 Ensembles infinis non dénombrables

Considérons l'ensemble $\mathbb{N}$. Nous avons admis que toute partie P de $\mathbb{N}$ est soit finie, soit dénombrable. Dans cette seconde éventualité, il existe une bijection (i.e. une application bijective) de P vers $\mathbb{N}$.

On convient de dire que deux ensembles E et F ont le *même cardinal* lorsqu'il existe une bijection de E vers F (ou de F vers E, ce qui revient au même). On note cela:

$$\#(E) = \#(F).$$

On écrit $\#(E) \leqq \#(F)$ lorsqu'il existe une injection (i.e. une application injective) de E vers F. On est amené à écrire $\#(E) < \#(F)$ s'il existe une injection de E vers F mais pas de bijection de E vers F.

Nous n'avons pas défini ce qu'est en soi un cardinal. La chose est possible mais elle dépasserait le cadre de cet exposé. Contentons-nous d'admettre que tous les ensembles qui peuvent être envoyés les uns vers les autres par des bijections ont en commun quelque chose que nous appellerons leur cardinal. Cette notion généralise celle de nombre des éléments d'un ensemble fini. On peut donc considérer une suite de cardinaux:

$$\underbrace{0 \quad 1 \quad 2 \quad 3 \ldots}_{\text{cardinaux finis}} \; \omega$$

0 étant le cardinal de l'ensemble vide et ω désignant le cardinal de $\mathbb{N}$, soit $\#(\mathbb{N})$. Peut-on imaginer des ensembles dont le cardinal soit strictement supérieur à ω?

Soit P une partie d'un ensemble donné E. Considérons la fonction:

$$f_P : E \to \{0, 1\}$$

telle que $f_P(x) = 1$ quand $x \in P$ et dans ce cas seulement. f_P est appelée *fonction caractéristique de P dans E* et elle détermine entièrement la partie P de E. On admet que les parties d'un ensemble quelconque E constituent un ensemble noté $\mathscr{P}(E)$. On constate que $\mathscr{P}(E)$ peut être mis en bijection avec l'ensemble des fonctions sur E à valeurs dans $\{0, 1\}$.

Considérons alors $\mathscr{P}(\mathbb{N})$. Il existe une injection i de $\mathbb{N}$ dans $\mathscr{P}(\mathbb{N})$:

$$\begin{aligned} i : \mathbb{N} &\to \mathscr{P}(\mathbb{N}) \\ n &\mapsto \{n\}. \end{aligned}$$

Donc $\omega \leqq (\mathscr{P}(\mathbb{N}))$. Montrons maintenant qu'il n'existe pas de bijection de $\mathbb{N}$ vers $\mathscr{P}(\mathbb{N})$. Considérons une application g de $\mathbb{N}$ vers $\mathscr{P}(\mathbb{N})$:

$$\begin{aligned} g : \mathbb{N} &\to \mathscr{P}(\mathbb{N}) \\ n &\mapsto g_n. \end{aligned}$$

Construisons l'application h: $\mathbb{N} \to \{0, 1\}$

$$n \to \begin{cases} 1 \text{ si } n \notin g_n \\ 0 \text{ si } n \in g_n \end{cases}$$

h est la fonction caractéristique d'une partie H de N. Comme $n \in H$ *ssi* $n \notin g_n$ et cela pour tout n dans $\mathbb{N}$, H ne coïncide avec aucun élément de l'image de g. Donc g n'est pas surjective. Par suite, $\omega < \#(\mathscr{P}(\mathbb{N}))$.

Il existe donc au moins un ensemble dont le cardinal est strictement supérieur à celui de $\mathbb{N}$. Lorsqu'on exige d'un langage du premier ordre L que l'ensemble de ses symboles soit dénombrable, on lui impose une véritable restriction.

7.0.2 Deux théorèmes sur les ensembles

Le raisonnement que nous venons de faire pour $\mathbb{N}$ peut être repris sans changement pour tout ensemble E. Cela s'exprime par le *théorème de Cantor*: pour tout ensemble E, $\#(E) < \#(P(E))$. On en déduit immédiatement que la suite des cardinaux infinis qui commence par ω est illimitée vers la droite.

Mentionnons en passant un autre théorème relativement élémentaire qui justifie la notation adoptée pour comparer les cardinaux. Le théorème de Cantor-Bernstein s'énonce ainsi: soit E et F deux ensembles tels qu'il existe une injection de E dans F et une injection de F dans E, alors il existe une bijection de E vers F (ou, ce qui revient au même, de F vers E). Autrement dit:

si $\#(E) \leqq \#(F)$ *et* $\#(F) \leqq \#(E)$, alors $\#(E) = \#(F)$.

7.0.3 Axiome du bon ordre et axiome du choix

Au cours de certaines démonstrations de logique élémentaire du premier ordre, nous avons utilisé le fait qu'un ensemble fini ou dénombrable peut être muni d'un bon ordre (par exemple, lemme 3.1.33). Existe-t-il une propriété analogue pour tous les ensembles?

Par des procédés qui dépassent beaucoup la portée de ce paragraphe, on peut montrer qu'on n'introduit pas de contradiction lorsqu'on ajoute aux opérations et aux hypothèses faites jusqu'ici sur les ensembles la condition suivante:

(BO) *tout ensemble non vide peut être muni d'un bon ordre*

Il est d'ailleurs aussi possible de montrer qu'on ne fait apparaître aucune contradiction non plus quand on adopte la négation de cette assertion, à savoir: il existe un ensemble non vide qui ne peut pas être muni d'un bon ordre. Ainsi (BO) peut être posé comme hypothèse de la "théorie des ensembles" on l'appelle *axiome* ou *principe du bon ordre*. Il est en relation étroite avec l'*axiome du choix* (ou *de Zermelo*) qui peut s'énoncer ainsi:

(AC) Soit $(A_i)_{i \in J}$ une famille non vide d'ensembles non vides.
Il existe une fonction dite "de choix":

$$f : J \to \bigcup_{i \in J} A_i$$

telle que, pour tout $i \in J$, $f(i) \in A_i$.
f "choisit" un élément $f(i)$ dans chaque A_i.

Lorsque (BO) est satisfait, on peut supposer que tous les ensembles A_i sont bien ordonnés; on définit alors $f(i)$ comme le plus petit élément de A_i. On obtient ainsi une fonction de choix f pour $(A_i)_{i \in J}$. Réciproquement, si (AC) est satisfait, tout ensemble non vide E peut être muni d'un bon ordre. Notre "théorie des ensembles" est trop sommaire pour que nous puissions le prouver ici. Essayons cependant de suggérer le principe de la démonstration. Considérons l'ensemble $\mathscr{P}^*(E)$ des parties non vides de E. Elle constitue une famille non vide d'ensembles non vides indexée par elle-même. En vertu de l'axiome du choix, il existe une fonction de choix:

$$f : \mathscr{P}^*(E) \to E \left(= \bigcup_{X \in \mathscr{P}^*(E)} X\right)$$

telle que pour toute partie non vide X de E, $f(X) \in X$. Posons

$$x_0 = f(E),\ x_1 = f(E - \{x_0\}),\ x_2 = f(E - \{x_0, x\}),\ \ldots$$

$x_0 < x_1 < x_2 < \ldots$ fait apparaître le début d'un bon ordre sur E.

Le nœud de la démonstration consiste à prouver qu'on peut ainsi épuiser tous les éléments de E.

Ce procédé ressemble beaucoup à une construction par récurrence à cela près qu'elle ne porte pas nécessairement sur un ensemble fini ou dénombrable. On parle à ce sujet d'*induction transfinie.* L'existence de constructions par induction transfinie sur tout ensemble bien ordonné fait l'objet de théorèmes sur lesquels nous n'insisterons pas ici. Bornons-nous à les évoquer de la manière suivante. Soit E et F deux ensembles non vides. Soit u un élément de F. Supposons E muni d'un bon ordre noté $\leqq$. Désignons par a_0 le plus petit élément de E et, pour tout a dans E, par $S(a)$ l'ensemble des $b \in E$ tels que $b \leqq a$.

Supposons que:

1) $f_{a_0}: \{a_0\} \to F$
   $a_0 \mapsto u$
2) Quel que soit a dans E:
   2.1. pour tout $b \in E$ tel que $b < a$, il existe une application
   $f_b : S(b) \to F$
   ($b < a$ est mis pour $b \leqq a$ *et* $b \neq a$)
   2.2. pour tous b, $c \in E$ tels que $b < c < a$, $f_b = f_c|_{S(b)}$
   2.3. il existe une procédure "raisonnable" déterminant une application
   $f_a : S(a) \to F$
   telle que, pour tout $b \in E$ tel que $b < a$, $f_b = f_a|_{S(b)}$

Alors il existe une unique application $f: E \to F$ telle que pour tout $a \in E$, $f(a) = f_a(a)$.

Nous ne sommes pas en mesure de préciser ici ce que nous entendons par une procédure "raisonnable". Contentons-nous d'admettre qu'elle doit pouvoir être décrite complètement dans la terminologie des ensembles et qu'elle ne relève pas du tirage au sort, par exemple.

L'induction transfinie permet d'étendre aux ensembles bien ordonnés quelconques les constructions que nous avons décrites précédemment pour les ensembles dénombrables. En particulier, moyennant l'axiome du bon ordre, on peut établir les faits suivants.

7.0.4 Trois propriétés des cardinaux infinis

7.0.4.0 Soit E un ensemble infini et $(E_i)_{i \in J}$ une famille d'ensembles telle que:

$\#(E_i) \leqq \#(E)$ pour tout $i \in J$
et $\#(J) \leqq \#(E)$.
Alors: $\#(\bigcup_{i \in J} E_i) \leqq \#(E)$.

7.0.4.1 Si en outre, pour l'un des indices k, $\#(E_k) = \#(E)$, alors

$$\#(\bigcup_{i \in J} E_i) = \#(E).$$

7.0.4.2 Si F est un ensemble non vide et si $\#(F) \leqq \#(E)$, E étant toujours un ensemble infini:

$$\#(E \times F) = \#(E).$$

7.1 CARDINAL D'UN LANGAGE DU PREMIER ORDRE

7.1.0 Préambule

Revenons à la logique et considérons le cas général où l'ensemble des symboles d'un langage du premier ordre L n'est pas nécessairement dénombrable.

7.1.1 Définition du cardinal d'un langage du premier ordre

Observons d'abord que les symboles logiques et les symboles de ponctuation sont toujours au nombre de 11. En ce qui concerne l'ensemble Var des symboles de variables, nous admettrons comme jusqu'ici qu'il est dénombrable. De sorte que seuls les ensembles Cst(L), Fct(L) et Rel(L) peuvent éventuellement être de cardinal supérieur à ω. Posons:

$$\alpha = \#(\mathrm{Cst}(L) \cup \mathrm{Fct}(L) \cup \mathrm{Rel}(L) \cup \mathrm{Var}).$$

Nous appellerons α le *cardinal* du langage L. Notons que $\#(\mathbb{N}) \leqq \alpha$ et que α est aussi le cardinal de tous les symboles de L.

7.1.2 Proposition

Si L est un langage du premier ordre de cardinal α, $\#(\mathrm{For}(L) = \alpha$.

7.1.3 Démonstration

Fixons un symbole de variable x. c désignant un symbole de constante, f_n un symbole de fonction n-aire, R_m un symbole de relation m-aire et y un symbole de variable, considérons les formules:

$$\begin{aligned} & c = x \\ & f_n(x, x, \dots, x) = x \\ & R_m(x, x, \dots, x) \\ & y = y. \end{aligned} \tag{7.0}$$

Quand c, f_n, R_m et y parcourent respectivement Cst(L), Fct(L), Rel(L) et Var, on fait apparaître une injection de (Cst(L)$\cup$Fct(L)$\cup$Rel(L)$\cup$Var) dans For(L). Donc $\#(\mathrm{For}(L)) \geqq \alpha$.

Désignons par For(L, n) l'ensemble des formules de L comportant exactement n symboles. For(L, n) constitue une partie de l'ensemble des suites de n symboles de L: $s_1 s_2 s_3 \ldots s_n$. Cet ensemble est le produit cartésien de n ensembles de cardinal α. D'après la propriété 7.0.4.2, ce produit cartésien est de cardinal α. Donc $\#(\text{For}(L, n)) \leqq \alpha$. Comme

$$\text{For}(L) = \bigcup_{n \in \mathbb{N}} \text{For}(L, n)$$

il résulte de la propriété 7.0.4.0 que $\#(\text{For}(L)) \leqq \alpha$. Par suite, $\#(\text{For}(L)) = \alpha$. □

Remarquons en passant que toutes les formules mises sous (7.0) comportent exactement un symbole de variable libre. Il en résulte que le cardinal de l'ensemble $\text{For}_1(L)$ des formules de L comportant au plus un symbole de variable libre égale aussi α.

7.2 THÉORÈME DE LÖWENHEIM-SKOLEM-TARSKI

7.2.0 Passage aux langages du premier ordre de cardinal infini quelconque

Tout au long des chapitres 1 à 6, nous nous sommes placés dans l'hypothèse où les langages du premier ordre considérés n'avaient qu'un ensemble fini ou dénombrable de symboles propres. Nous allons passer brièvement en revue ces chapitres pour examiner comment on peut étendre les résultats obtenus aux langages dont le cardinal est supérieur ou égal à ω.

Relevons d'abord que dans tout langage du premier ordre L, chaque formule est de longueur finie. Les démonstrations procédant par récurrence sur la longueur des formules sont donc valides dans le cas général. Le chapitre 1 peut donc être repris intégralement. Il en est de même du chapitre 2, à l'exception de la proposition 2.3.2 qui, moyennant l'axiome du bon ordre, peut être remplacée par:

si le cardinal de L est α, $\#(\text{For}(L)) = \alpha$

selon la proposition 7.1.2. Le corollaire 2.3.4 peut alors être repris sans changement.

Passons au chapitre 3. Dans tout langage du premier ordre L chaque formule admet un arbre de composition fini. C'est sur ce fait que reposent toutes les propriétés élémentaires des fonctions de vérité sur For(L). On peut donc les reprendre sans changement dans le cas général. Le premier obstacle lié au cardinal de L apparaît au cours de la démonstration du théorème de compacité de la logique des propositions (prop. 3.1.29), et plus précisément au lemme 3.1.33. Tout d'abord on demande de munir For(L) d'un bon ordre: heureusement nous nous sommes placés dans l'hypothèse où l'axiome du bon ordre est satisfait. La suite de la preuve repose essentiellement sur la construction d'une certaine application:

$$\begin{aligned} T:\mathrm{For}(L) &\to \mathscr{P}(\mathrm{For}(L)) \\ \alpha &\mapsto T_\alpha. \end{aligned}$$

En suivant cette construction de près, on constate que nous avons procédé par une induction transfinie. Au numéro 7.0.3, nous avons montré qu'il est plausible – et on peut établir en toute rigueur – que cette procédure est admissible, dans le cas général, moyennant l'axiome du bon ordre. La remarque clôturant le chapitre 3 mentionne une autre démonstration, fondée sur le théorème de Tychonoff. Mais celui-ci découle à son tour de l'axiome du bon ordre. En fait, les deux démonstrations sont équivalentes.

En bref, le théorème de compacité de la logique des propositions est valable sans restriction sur le cardinal de L lorsqu'on adopte l'axiome du bon ordre. Le chapitre 3 peut alors être repris sans changement dans le cas général.

Il est intéressant de noter en passant qu'au chapitre 3 nous avons considéré toutes les fonctions de vérité sur For(L) (cf. définition 3.1.8). Pour déterminer une fonction de vérité sur For(L), il suffit de se donner arbitrairement une fonction à valeurs dans $\{0; 1\}$ sur l'ensemble des formules premières de For(L). Dans le cas élémentaire, ces dernières constituent un ensemble dénombrable. Donc l'ensemble des fonctions de vérité sur For(L) est en correspondance biunivoque avec l'ensemble des parties d'un ensemble dénombrable; nous avons vu que le cardinal de cet ensemble de parties est supérieur à ω (cf. numéro 7.0.1). Ainsi dans le cas élémentaire et sans nous en douter, nous avons déjà travaillé avec des ensembles infinis non dénombrables.

Le chapitre 4 concernant les “axiomes de l'égalité” ne soulève aucune difficulté dans le cas général.

Il en va de même du chapitre 5, au moins jusqu'à la fin de la démonstration du lemme de réduction à la logique des propositions. Les démonstrations des propositions 5.3.4 et 5.4.2 font intervenir des récurrences sur la longueur des formules ou sur la hauteur des constantes de Henkin. Celles-ci étant toujours finies, aucune difficulté n'apparaît de ce fait. Le lemme de réduction de la logique du premier ordre à la logique des propositions est donc valide dans le cas général. Le théorème de compacité de la logique des propositions vaut donc dans le cas général lorsqu'on adopte l'axiome du bon ordre. Gödel a établi ce théorème dans le cas élémentaire, c'est-à-dire dénombrable. Malčev l'a étendu au cas général.

Avant de passer à la suite du chapitre 5, examinons d'un peu plus près la construction de l'extension de Henkin d'un langage du premier ordre L. Désignons à nouveau par α le cardinal de L. Ainsi que nous l'avons constaté à la proposition 7.1.2, $\#(\mathrm{For}_1(L))=\alpha$. Donc l'ensemble C_1 des constantes de Henkin de hauteur 1 est de cardinal α. Si $L_1=L(C_1)$, $\#(\mathrm{For}_1(L_1))=\alpha$ et le cardinal de l'ensemble C_2 des constantes de Henkin de hauteur 2 égale aussi α. Il en est de même de l'ensemble $\mathrm{For}_1(L_1(C_2))$, et ainsi de suite. D'une manière générale $\#(C_n)=\alpha$, $n=1, 2, 3,\ldots$. D'après la propriété 7.0.4.1, $\#(C)=\alpha$, où C est l'ensemble des constantes de Henkin de L. Il en résulte que le cardinal de l'extension de Henkin $L(C)$ de L est aussi α.

Venons-en au théorème de Löwenheim-Skolem. Il a été énoncé et démontré dans l'hypothèse où l'ensemble des symboles propres à L est fini ou dénombrable. Peut-on l'étendre au cas général où le cardinal α du langage L est supérieur ou égal à ω? Remarquons que sa démonstration repose entièrement sur le lemme de réduction à la logique des propositions: si S est un ensemble d'énoncés de L admettant un modèle, alors il existe une $L(C)$-structure canonique (E, J') qui est un modèle de S. Dire que (E, J') est canonique, c'est, rappelons-le, affirmer que $J'|_{C^*}C^* \to E$ est surjective. Munissons C^* d'un bon ordre. Soit e un élément quelconque de E. L'ensemble des éléments $k \in C^*$ tels que $J'(k) = e$ n'est pas vide. Désignons par e^* son plus petit élément. L'application

$$\begin{aligned} * : E &\to C^* \\ e &\mapsto e^* \end{aligned}$$

est injective. Donc $\#(E) \leqq \#(C^*) = \alpha$. Ayant adopté l'axiome du bon ordre, nous sommes donc en mesure d'énoncer une généralisation de la proposition 5.5.2.

7.2.1 Proposition: théorème de Löwenheim-Skolem, cas général

Soit L un langage du premier ordre de cardinal α. Soit S un ensemble d'énoncés de L admettant un modèle. Alors S admet un modèle (E, J) où $\#(E) \leqq \alpha$.

7.2.2 Extension du théorème de complétude

Passons enfin au chapitre 6. Les raisonnements qui conduisent au théorème de complétude de la logique du premier ordre s'appuient sur les propositions des chapitres précédents. Nous venons de constater que, moyennant l'axiome du bon ordre, ces propositions sont valides dans le cas général. Les démonstrations du théorème de complétude de Gödel et de ses divers corollaires ne font apparaître aucune restriction sur le cardinal α du langage L.

En conclusion, il est possible d'imaginer des langages du premier ordre de cardinal arbitrairement grand, supérieur ou égal à ω. Pour ces langages et à condition d'adopter l'axiome du bon ordre, tous les théorèmes vus jusqu'ici s'étendent naturellement.

7.2.3 Proposition: théorème de Löwenheim-Skolem-Tarski

Soit L un langage du premier ordre de cardinal α. Soit (L, S) une théorie du premier ordre telle que l'une des deux hypothèses suivantes soit satisfaite:
(H_1): S admet un modèle infini;
(H_2): S admet des modèles finis de cardinal aussi grand qu'on veut. Alors:
quel que soit le cardinal β supérieur ou égal à α, il existe un modèle de S de cardinal β.

7.2.4 Démonstration

Prenons un ensemble D tel que:

$$\#(D)=\beta \text{ et } D\cap\mathrm{Cst}(L)=\emptyset.$$

Introduisons un nouveau langage du premier ordre $L'=L(D)$. On a donc: $\mathrm{Cst}(L')=\mathrm{Cst}(L)\cup D$, $\mathrm{Fct}(L')=\mathrm{Fct}(L)$ et $\mathrm{Rel}(L')=\mathrm{Rel}(L)$. A tout modèle (E, J) de (L, S) on peut associer un modèle (E, J') de (L', S) en posant:

$$\begin{aligned} J'|_{\mathrm{Cst}(L')}:\mathrm{Cst}(L') &\to E \\ c &\mapsto J(C) \text{ si } c\in\mathrm{Cst}(L) \\ d &\mapsto a_d \text{ si } d\in D, \end{aligned}$$

les a_d étant des éléments arbitrairement choisis dans E.

Formons maintenant l'ensemble Γ des énoncés de L' de la forme:

$$\gamma_{d,\,d'}\equiv(\neg(d=d'))$$

quels que soient d, $d'\in D$ tels que $d\not\equiv d'$. Montrons que $S\cup\Gamma$ admet un modèle. En vertu du théorème de compacité de la logique du premier ordre, il suffit de montrer que toute partie finie F de $S\cup\Gamma$ admet un modèle. Or, en vertu de (H_1) comme de (H_2), il existe un modèle de S tel que les constantes (en nombre fini) apparaissant dans les axiomes $\gamma_{d,\,d'}$ appartenant à F soient envoyées sur des éléments distincts du modèle. F admet donc un modèle et $(L', S\cup\Gamma)$ est une théorie.

Comme $\#(L')=\beta$ (cf. propriété 7.0.4.1), il résulte du théorème de Löwenheim-Skolem que $(L', S\cup\Gamma)$ admet un modèle de cardinal inférieur ou égal à β. Mais tous les axiomes de Γ y étant satisfaits, ce modèle a un cardinal au moins égal à β. Il s'ensuit qu'il est exactement de cardinal β. □

7.2.5 Remarque

Il résulte de ce théorème que l'hypothèse (H_2) implique l'hypothèse (H_1).

7.2.6 Corollaire

Il n'existe pas de théorie du premier ordre admettant pour seuls modèles les ensembles finis ou les groupes finis.

7.2.7 Démonstration

En effet, si elle existait, une telle théorie satisferait l'hypothèse (H_2) (cf. 5.5.4). Elle admettrait donc des modèles de cardinal infini arbitrairement grand. □

Ce corollaire étend considérablement la portée de la remarque 5.5.5. La notion même de finitude semble échapper à la logique du premier ordre.

7.2.8 Autre conséquence du théorème de Löwenheim-Skolem-Tarski

Le théorème de Löwenheim-Skolem-Tarski montre que lorsqu'une théorie du premier ordre (L, S) admet un modèle infini, elle admet des modèles essentiellement distincts puisque de cardinaux différents. (Rappelons à ce propos que la liste des cardinaux n'est pas limitée supérieurement.) Pour énoncer ce fait, nous allons préciser un peu notre vocabulaire.

Si $\beta: E \to E'$ est une bijection, l'application β'' définie par:

$$\begin{array}{ll} \beta^n: E^n \to E'^n & n=1, 2, 3, \ldots \\ (a_1, \ldots, a_n) \mapsto (\beta(a_1), \ldots, \beta(a_2)) & \end{array}$$

est aussi une bijection. Donc les réciproques respectives β^{-1} et $(\beta^n)^{-1}$ de β et β^n existent; elles sont évidemment aussi des bijections.

7.2.9 Définition

Soit (L, S) une théorie du premier ordre. Deux modèles (E, J) et (E', J') de (L, S) sont dits *isomorphes* lorsqu'il existe une bijection $\beta: E \to E'$ telle que:

i) $J'|_{\mathrm{Cst}(L)} = \beta \circ J|_{\mathrm{Cst}(L)}$

ii) pour tout symbole de fonction f_n dans Fct(L):
$J'(f_n) = \beta \circ J(f_n) \circ (\beta^n)^{-1}$

iii) pour tout symbole de relation R_m dans Rel(L),
$J'(R_m) = \beta^m(J(R_m))$.

Deux modèles isomorphes de (L, S) ont évidemment même cardinal. Cette définition apparemment compliquée exprime simplement que la L-structure (E', J') s'obtient en "transportant" la L-structure (E, J) par la bijection β. (E', J') apparaît comme le modèle (E, J) noté autrement. Tout modèle (E, J) de (L, S) donne naissance à une collection de modèles isomorphes moyennant des bijections de E vers les ensembles de même cardinal que E.

7.2.10 Autre corollaire du théorème de Löwenheim-Skolem-Tarski

Aucune théorie du premier ordre ne permet de déterminer un modèle infini à isomorphisme près.

7.2.11 Remarque

Les corollaires 7.2.6 et 7.2.10 du théorème de Tarski montrent que le fini et l'infini mathématiques, chacun de son côté et de manières différentes, soulèvent des difficultés en logique du premier ordre. Et pourtant, d'après le théorème de complétude de Gödel, il semble que cette logique convienne aux mathématiques. Nous reviendrons ultérieurement sur ce point.

CHAPITRE 8

Quelques remarques sur la logique du premier ordre

8.0 INTRODUCTION

Au cours des chapitres précédents, nous avons établi quelques propositions concernant les systèmes formels du premier ordre: le théorème de compacité, le théorème de Löwenheim-Skolem-Tarski et surtout le théorème de complétude de Gödel, entre autres. Ces résultats sont importants en eux-mêmes parce qu'ils ne se bornent pas à énoncer des banalités évidentes – contrairement à ce qu'on reproche trop souvent à la logique. Ils sont aussi intéressants parce qu'ils permettent de voir fonctionner la machinerie nécessaire pour les démontrer. Nous pouvons maintenant jeter un regard en arrière et examiner d'un œil critique ce que nous avons fait.

Revenons à la logique élémentaire du premier ordre, c'est-à-dire aux langages du premier ordre dont l'ensemble des symboles propres (constantes, fonctions, relations) est au plus dénombrable. Comme nous l'avons fait remarquer, dans un tel langage, on peut écrire effectivement toute formule à l'aide d'un petit nombre de signes typographiques. De plus, les règles de formation des formules sont suffisamment simples pour qu'on puisse confier à une machine le soin de vérifier si un agrégat de signes est une formule ou non. Ce sont les propriétés de ce jeu de combinaisons assez élémentaires que nous avons montrées.

Pour y parvenir, nous avons employé les nombres naturels et les ensembles. Or les uns et les autres relèvent de théories mathématiques dont on peut présumer qu'elles sont traduisibles par des systèmes formels du premier ordre. Nous avons en outre effectué des raisonnements, des déductions apparemment logiques. On peut se demander si tout cela ne constitue pas, après tout, un cercle vicieux.

Notre propos est de montrer qu'en réalité nous avons parcouru une sorte d'hélice. Au point où nous sommes arrivés, nous pouvons jeter un regard au-dessous de nous. Nous constaterons que nous sommes désormais en mesure de décrire les notions de nombre naturel, d'ensemble et de preuve d'une manière relativement élaborée. Par comparaison, les notions dont nous nous sommes servis jusqu'ici peuvent être considérées comme "naïves". Et nous allons essayer de faire apparaître ce qu'il faut entendre par-là.

8.1 UN SYSTÈME FORMEL DU PREMIER ORDRE POUR L'ARITHMÉTIQUE

8.1.0 Préambule

Nous aimerions décrire un système formel (L_n, S_n) du premier ordre admettant pour modèle l'ensemble (naïf) des nombres naturels $\mathbb{N}=\{0, 1, 2, 3, ...\}$ au sein duquel opèrent l'addition et la multiplication bien connues. Celui que nous allons présenter n'est pas le plus élégant, mais il est relativement proche de l'intuition. D'autre part, nous allons nous permettre deux sortes d'abus.

8.1.1 Le langage L_n

Premièrement, comme nous traiterons d'un système formel particulier et non plus de la totalité des systèmes formels du premier ordre, nous adopterons des notations proches de l'algèbre élémentaire. Le langage L_n est caractérisé par:

- deux symboles de constantes: 0 1 (et non c et c')
- deux symboles de fonctions binaires: $+$ $\cdot$ (et non f_2 et f_2')
- aucun symbole de relation.

Nous noterons les symboles de variables $x, y, z, \ldots, u, v_1, v_2, \ldots$. Au lieu de $+(x, y)$, nous noterons $x+y$ et, au lieu de $\cdot(x, y)$, $x \cdot y$. En outre, nous ferons un usage parcimonieux des parenthèses.

Deuxièmement, lorsque nous considérerons $(\mathbb{N}, J)$ comme une L_n-structure, nous noterons: $J(0)$ sous la forme 0 et $J(1)$ sous la forme 1, au lieu de $\tilde{0}$ et $\tilde{1}$ respectivement. Ainsi, 0 et 1 désigneront indifféremment les symboles de constantes de L_n et les deux premiers éléments du modèle $(\mathbb{N}, J)$. De même, $J(+)$ et $J(\cdot)$ seront notés $+$ et $\cdot$ respectivement.

Venons-en aux axiomes non logiques S_n:

8.1.2 Premiers axiomes

$A_1 \equiv \forall x(x+0=x) \wedge (0+x=x) \wedge (x \cdot 0=0) \wedge (0 \cdot x=0) \wedge (x \cdot 1=x) \wedge (1 \cdot x=x)$
$A_2 \equiv \forall x \forall y \forall z(x+(y+z)=(x+y)+z) \wedge (x \cdot (y \cdot z)=(x \cdot y) \cdot z)$
$A_3 \equiv \forall x \forall y \forall z(x \cdot (y+z)=x \cdot y+x \cdot z) \wedge ((y+z) \cdot x=y \cdot x+z \cdot x)$
$A_4 \equiv \forall x \neg(x+1=0)$
$A_5 \equiv \forall x \forall y(x+1=y+1) \rightarrow (x=y)$.

Ces cinq énoncés ne permettent pas de déduire toutes les propriétés des membres naturels. Par exemple:

il est faux que $\{A_1, A_2, A_3, A_4, A_5\} \vdash \forall x \forall y\ x \cdot y=y \cdot x$.

Pourtant, de l'axiome A_1, on tire facilement une preuve
de: $\forall y\ 0 \cdot y=y \cdot 0$
et de: $\forall y\ 1 \cdot y=y \cdot 1$

A l'aide de A_3, on obtient une preuve
de: $\forall y(1+1) \cdot y = y \cdot (1+1)$
puis de: $\forall y((1+1)+1) \cdot y = y \cdot ((1+1)+1)$
et ainsi de suite. Mais ce ne serait pas une preuve de:

$$\forall x \forall y\ x \cdot y = y \cdot x \tag{8.0}$$

8.1.3 L'induction complète

Nous aimerions pouvoir raisonner ainsi: désignons par u l'ensemble des nombres naturels n tels que, pour tout nombre naturel t, $n \cdot t = t \cdot n$. De ce qui précède, il résulte que 0 appartient à u, de même que 1, $1+1$ et $(1+1)+1$. Admettons que le nombre naturel m appartienne à u: nous croyons pouvoir montrer que $m+1$ appartient aussi à u. Nous sommes tentés d'en conclure que tout nombre naturel n appartient à u; ce qui serait une bonne traduction de (8.0). Cette manière de procéder constitue un raisonnement par *récurrence* ou par *induction complète*. Nous l'avons souvent utilisé dans ce qui précède. Ce qu'il nous faudrait, c'est un axiome nous donnant le moyen de construire une preuve formelle de ce genre dans L_n. On aimerait poser:

$$\Omega \equiv \forall u(((0 \in u) \wedge \forall z((z \in u) \rightarrow (z+1) \in u)) \rightarrow \forall x(x \in u)) \tag{8.1}$$

Malheureusement, Ω n'est pas une formule de L_n!

Ne renonçons pas encore. Considérons la formule:

$$\psi(x) \equiv \forall y\ x \cdot y = y \cdot x$$

Par parenthèse, convenons de noter $\psi(t)$ au lieu de ψ_t^x chaque fois que t est un terme de L_n substituable à x dans $\psi(x)$. Nous savons prouver l'énoncé $\psi(0)$; nous sommes probablement en mesure de prouver aussi: $\forall z(\psi(z) \rightarrow \psi(z+1))$. Nous aimerions pouvoir en inférer: $\forall x \psi(x)$. Pour cela, il nous faudrait un axiome tel que

$$(\psi(0) \wedge \forall z(\psi(z) \rightarrow \psi(z+1))) \rightarrow \forall x \psi(x) \tag{8.2}$$

La piste est meilleure. Toutefois, l'axiome (8.2) ne convient guère qu'à la preuve de (8.0). Nous aimerions disposer d'un axiome analogue pour chaque théorème de l'arithmétique.

8.1.3 Définition: le schéma d'axiomes de l'induction complète

Nous sommes ainsi amenés à considérer toutes les formules de L_n comportant au moins un symbole de variable, x par exemple. Nous savons qu'elles constituent un ensemble dénombrable. La p-ième formule de cette liste peut se noter:

$$\varphi_p(x, v_1, v_2, \ldots, v_{m_p}),$$

$v_1, v_2, \ldots, v_{m_p}$ étant des symboles de variables supplémentaires dont le nombre m_p dépend du numéro p de φ_p. Posons alors:

$$B_p \equiv \forall x_1 \dots \forall v_{m_p}((\varphi_p(0, v_1, \dots, v_{m_p}) \wedge \forall z(\varphi_p(z, v_1, \dots, v_{m_p}) \rightarrow \varphi_p(z+1, v_1, \dots, v_{m_p})) \rightarrow \forall x \varphi_p(x, v_1, \dots, v_{m_p})) \quad p=0, 1, 2, 3, \dots \tag{8.3}$$

La collection $\{B_p | p=0, 1, 2, 3, \dots\}$ comporte les axiomes semblables à (8.2) à raison d'un par formule de L_n comportant au moins la variable libre x. (Notons qu'il est inutile d'envisager les formules de L_n sans variable libre, c'est-à-dire les énoncés de L_n: ils donnent naissance à des tautologies qui figurent déjà dans les axiomes logiques.) Il n'est pas possible d'écrire effectivement la totalité des énoncés B_p. Mais (8.3) nous montre comment écrire effectivement chacun d'eux pris isolément. $\{B_p | p=0, 1, 2, 3, \dots\}$ est le *schéma d'axiomes de l'induction complète.*

8.1.4 Le système formel (L_n, S_n)

Désignons maintenant par S_n l'ensemble $\{A_1, A_2, A_3, A_4, A_5, B_0, B_1, \dots\}$. Bien que ce soit extrêmement fastidieux, on peut montrer que toutes les propriétés des nombres entiers naturels établies par l'arithmétique classique admettent une preuve dans le système formel (L_n, S_n). Toutefois, nous engageons le lecteur à montrer, comme exercice, que $(L_n, S_n) \vdash (\neg 0=1)$ à l'aide de A_1, A_4 et des axiomes de spécification.

(L_n, S_n) apparaît donc comme un système formel du premier ordre susceptible de formaliser l'arithmétique classique. Mais est-il une théorie? Si ce n'était pas le cas, on pourrait y prouver "$0=1$", ce qui aurait des conséquences théoriques (et peut-être pratiques) assez surprenantes. En fait, il est raisonnable de penser que (L_n, S_n) n'implique pas contradiction. L'arithmétique classique s'appuie sur (L_n, S_n) ou un système équivalent et aucune apparence d'incompatibilité ne s'y est encore manifestée.

8.1.5 Discussion sur l'"axiome" (8.1)

La formule Ω appartient à un langage comportant un symbole de relation binaire $\in$. Un tel langage conviendrait à l'étude des ensembles. D'autres difficultés apparaîtraient alors, qui ont peu de choses à voir avec les nombres naturels. Notons cependant que Ω peut être interprété ainsi: quel que soit l'ensemble u de nombres naturels, si 0 appartient à u et si l'appartenance à u de z implique celle de $z+1$, alors u comporte tous les nombres naturels. Pour vérifier cette assertion, il faudrait la tester sur toutes les parties de $\mathbb{N}$. Or celles-ci, nous le savons, constituent un ensemble immense qui n'est ni fini, ni dénombrable. Les nombreux mathématiciens qui ne se préoccupent guère de ce genre de difficultés admettent sans peine un "axiome" tel que Ω (voir, par exemple, van der Waerden, Algebra I, § 3). Le schéma d'axiomes $\{B_p | p=0, 1, 2, 3, \dots\}$ n'envisage l'assertion ci-dessus que pour l'ensemble dénombrable des parties de $\mathbb{N}$ qui admettent une caractérisation arithmétique exprimable dans L_n. Il ne reprend donc qu'une partie relativement très petite du contenu de Ω. Si le système formel (L_n, S_n) était inconsistant, ce serait le cas à plus forte raison de l'arithmétique usuelle. Nous reviendrons sur ce point.

8.1.6 Sur les modèles de (L_n, S_n)

Admettons sans plus de manières que (L_n, S_n) est une théorie. Elle a donc des modèles. Chacun de ces modèles comporte les éléments 0, 1, $1+1$, $(1+1)+1$ $((1+1)+1)+1$, ... On prouve sans trop de peine à partir de S_n que ces éléments sont distincts. Les modèles de (L_n, S_n) sont donc infinis. En vertu du corollaire 7.2.10 du théorème de Löwenheim – Skolem – Tarski, (L_n, S_n) admet une collection illimitée de modèles non isomorphes.

Voilà une affirmation choquante parce que notre imagination ne nous montre qu'un seul modèle des nombres naturels, à isomorphisme près. Mais il est possible d'aller encore un peu plus loin dans l'horreur! Nous allons faire usage d'une proposition assez générale qui s'applique à (L_n, S_n).

8.1.7 Proposition

Soit (L, S) un système formel du premier ordre admettant un modèle infini (E_0, J_0) tel que $J_{0|\mathrm{Cst}(L)}$ soit injective. Il existe un modèle (E_1, J_1) de (L, S) tel que:

$E_0 \subset E_1$ *et* $E_0 \neq E_1$
pour tout $c \in \mathrm{Cst}(L)$, $J_1(c) = J_0(c)$
pour tout $f_n \in \mathrm{Fct}(L)$, $J_1(f_n)|_{E_0^n} = J_0(f_n)$
pour tout $R_m \in \mathrm{Rel}(L)$, $J_1(R_m) \cap E_0^m = J_0(R_m)$

8.1.8 Démonstration

Pour simplifier la présentation, nous allons identifier $\mathrm{Cst}(L)$ avec $J_0|_{\mathrm{Cst}(L)}(\mathrm{Cst}(L))$ dans E_0. C'est un abus d'écriture, mais il est sans conséquence fâcheuse.

Construisons d'abord le langage $L' := L(E_0)$. L et L' ont les mêmes symboles de fonctions et de relations. L' comporte éventuellement des symboles de constantes supplémentaires, à savoir les éléments de E_0 qui ne sont pas dans $\mathrm{Cst}(L)$. Pour obtenir un modèle (E_0, J'_0) de (L', S), il suffit de poser:

$$J'_0|_{\mathrm{Cst}(L')} := id_{E_0} \text{ où } id_{E_0} : \begin{array}{l} E_0 \to E_0 \\ m \mapsto m \end{array}$$

$$J'_0|_{\mathrm{Fct}(L)} := J_0|_{\mathrm{Fct}(L)}$$
$$J'_0|_{\mathrm{Rel}(L)} := J_0|_{\mathrm{Rel}(L)}$$

Nous considérons donc les éléments de E_0 à la fois comme des symboles de constantes dans L' et comme les images de ces symboles dans l'interprétation J'_0.

Introduisons un nouveau langage L^* en adjoignant à L' un nouveau symbole de constante d:

$$L^* := L'(\{d\}) \text{ où } d \notin E_0.$$

On a évidemment: $\mathrm{For}(L) \subset \mathrm{For}(L') \subset \mathrm{For}(L^*)$. Désignons par T l'ensemble des énoncés $\varphi \in \mathrm{For}(L')$ tels que $(E_0, J'_0) \models \varphi$. S est inclus dans T. Considérons ensuite l'ensemble T^* des énoncés de L^* donnés par:

$$\gamma_m \equiv (\neg(m=d)) \text{ où } m \in E_0.$$

Posons: $S^* := T \cup T^*$.

Nous allons montrer que (L^*, S^*) est une théorie à l'aide du théorème de compacité de la logique du premier ordre (prop. 5.5.1). En effet, soit U une partie finie quelconque de S^*:

$$U = T_0 \cup \{\gamma_{i_0}, \gamma_{i_1}, \dots, \gamma_{i_p}\}$$

où T_0 est une partie finie de T. Désignons par

$$\{k_0, k_1, \dots, k_r, i_0, i_1, \dots, i_p\}$$

les éléments de E_0 apparaissant dans les énoncés de U. Etendons J'_0 en une interprétation J^U de L^* en posant:

$$\begin{aligned} &J^U(k_0)=k_0 \quad ; \quad J^U(k_1)=k_1 \quad ; \quad \dots, J^U(k_r)=k_r \\ &J^U(i_0)=i_0 \quad ; \quad J^U(i_1)=i_1 \quad ; \quad \dots, J^U(i_p)=i_p \\ &J^U(d)=v \quad , \quad \text{où } v \in E_0 \quad , \quad v \neq i_j \quad , \quad j=0, 1, \dots, p \\ &\qquad J^U|_{\mathrm{Fct}(L^*)} = J_0|_{\mathrm{Fct}(L)} \\ &\qquad J^U|_{\mathrm{Rel}(L^*)} = J_0|_{\mathrm{Rel}(L)} \end{aligned}$$

Il est clair que (E_0, J^U) est un modèle de (L^*, U), car (E_0, J'_0) est un modèle de (L', T). Il en résulte que (L^*, S^*) admet un modèle (E^*, J^*). $J^*|_{\mathrm{Cst}(L^*)}$ est injective, car si $m, n \in \mathrm{Cst}(L^*)$ sont tels que $m \not\equiv n$, l'énoncé $(\neg(m=n))$ est dans S^*. Par suite, $J^*(m) \neq J^*(n)$.

Montrons que, moyennant une définition convenable de l'interprétation $J^* \circ J_0$, $(J^*(E_0), J^* \circ J_0)$ est un modèle de (L, S) isomorphe à (E_0, J_0).

On a premièrement:

$$J^*|_{\mathrm{Cst}(L)} = J^*|_{\mathrm{Cst}(L^*)} \circ J_0|_{\mathrm{Cst}(L)}. \tag{8.4}$$

Posons en conséquence:

$$(J^* \circ J_0)|_{\mathrm{Cst}(L)} := J^*|_{\mathrm{Cst}(L^*)} \circ J_0|_{\mathrm{Cst}(L)} \tag{8.5}$$

Deuxièmement, pour tout $f_n \in \mathrm{Fct}(L)$:

$$J^*(f_n)|_{(J^*(E_0))^n} = J^*|_{E_0} \circ J_0(f_n) \circ [(J^*|_{E_0})^n]^{-1}. \tag{8.6}$$

En effet, si $a_1, \dots, a_n \in E_0$ et si:

$$b = J_0(f_n)(a_1, \dots, a_n), \tag{8.7}$$

alors:

$$b = f_n(a_1, \dots, a_n) \tag{8.8}$$

est un énoncé appartenant à T. Par suite:

$$J^*(b) = J^*(f_n)(J^*(a_1), \dots, J^*(a_n)). \tag{8.9}$$

Réciproquement, (8.9) signifie que $(E^*, J^*) \models (b=f_n(a_1, \dots, a_n))$. Mais $(b=f_n(a_1, \dots, a_n))$ est un énoncé de L'. Il appartient à T, car sinon, $(\neg(b=f_n(a_1, \dots, a_n))) \in T$ et alors:

$$(E^*, J^*) \models (\neg(b=f_n(a, \dots, a_n))),$$

ce qui contredit (8.9). Ainsi (8.9) entraîne (8.8) qui, à son tour, entraîne (8.7). L'équivalence de (8.7) et (8.9) est exactement traduite par (8.6). Nous poserons alors:

$$\text{quel que soit } f_n \in \mathrm{Fct}(L) : (J^* \circ J_0)(f_n) := J^*|_{E_0} \circ J_0(f_n) \circ [(J^*|_{E_0})^n]^{-1}. \tag{8.10}$$

Troisièmement, pour tout $R_m \in \mathrm{Rel}(L)$:

$$J^*(R_m) \cap (J^*(E_0))^m = (J^*|_{E_0})^m (J_0(R_m)). \tag{8.11}$$

En effet, si $a_1, \dots, a_m \in E_0$ et si

$$(a_1, \dots, a_m) \in J_0(R_m) \tag{8.12}$$

alors

$$R_m(a_1, \dots, a_m) \tag{8.13}$$

est un énoncé appartenant à T, d'où:

$$(J^*(a_1), \dots, J^*(a_m)) \in J^*(R_m). \tag{8.14}$$

Réciproquement (8.14) signifie que $(E^*, J^*) \models R_m(a_1, \dots, a_m)$. Mais $R_m(a_1, \dots, a_m)$ est un énoncé de L'. Il appartient à T, car sinon $(\neg R_m(a_1, \dots, a_m)) \in T$ et alors:

$$(E^*, J^*) \models (\neg R_m(a_1, \dots, a_m)),$$

ce qui contredirait (8.14). Par suite, (8.14) entraîne (8.13) qui, à son tour, entraîne (8.12). L'équivalence de (8.12) et (8.14) est exactement traduite par (8.11). Nous poserons alors:

$$\text{quel que soit } R_m \in \mathrm{Rel}(L) : (J^* \circ J_0)(R_m) := (J^*|_{E_0})^m (J_0(R_m)). \tag{8.15}$$

L'interprétation $J^* \circ J_0$ étant définie par (8.5), (8.10) et (8.15), les égalités (8.4), (8.6) et (8.11) expriment que $(J^*(E_0), J^* \circ J_0)$ est un modèle de (L, S) isomorphe à (E_0, J_0) (voir définition 7.2.9). Pour achever la démonstration, il faut encore transformer (E^*, J^*) par un isomorphisme de manière à obtenir un modèle qui, dans un sens naturel, contienne (E_0, J_0).

Considérons l'ensemble

$$E_1 := (E_0 \cup \{d\}) \cup (E^* - J^*(E_0 \cup \{d\})) \tag{8.16}$$

et posons

$$\begin{aligned} \gamma : E_1 &\to E^* \\ u &\mapsto \begin{cases} J^*(u) & \text{si } u \in E_0 \cup \{d\} \\ u & \text{si } u \notin E_0 \cup \{d\} \end{cases} \end{aligned} \tag{8.17}$$

γ est manifestement une bijection. Transportons la L^*-structure (E^*, J^*) à E_1 à l'aide de la bijection réciproque γ^{-1} en utilisant les formules (i), (ii) et (iii) de la définition 7.2.9. Nous obtenons ainsi un modèle (E_1, J_1) de (L^*, S^*). (E_1, J_1) est *a fortiori* un modèle de (L, S) et, par construction, il possède toutes les propriétés requises. □

8.1.9 Définition

La situation que nous venons de décrire justifie une définition:
Soit (L, S) une théorie du premier ordre.
Soit (E_0, J_0) et (E_1, J_1) deux modèles de (L, S) tels que:
$E_0 \subset E_1$
quel que soit $c \in \mathrm{Cst}(L) : J_1(c) = J_0(c)$
quel que soit $f_n \in \mathrm{Fct}(L) : J_1(f_n)|_{E_0^n} = J_0(f_n)$
quel que soit $R_m \in \mathrm{Rel}(L) : J_1(R_m) \cap E_0^m = J_0(R_m)$.
On dit alors que (E_0, J_0) est un *sous-modèle* de (E_1, J_1). Il est dit *propre* quand $E_0 \neq E_1$.

Par exemple, lorsque (L, S) est une théorie des groupes (cf. exemple 5.5.4), (E_0, J_0) est un *sous-groupe* de (E_1, J_1).

La définition précédente permet de réénoncer et de préciser la proposition 8.1.7:

8.1.10 Corollaire

Soit L un langage du premier ordre de cardinal (infini) α. Soit (L, S) une théorie du premier ordre admettant un modèle (E_0, J_0) de cardinal $\beta \geqq \alpha$, et tel que $J_0|_{\mathrm{Cst}(L)}$ soit injective. Il existe un modèle (E_1, J_1) de (L, S) de cardinal β, admettant (E_0, J_0) comme sous-modèle propre.

8.1.11 Démonstration

Reprenons les notations utilisées dans la démonstration de la proposition 8.1.7. Le cardinal de (E_1, J_1) égale celui de (E^*, J^*). Or d'après le théorème de Löwenheim – Skolem – Tarski (prop. 7.2.3), on peut choisir le modèle (E^*, J^*) de (L^*, S^*) de façon que son cardinal égale celui de L^*. Or celui-ci est exprimé par:

$$\#(E_0 \cup \{d\} \cup \mathrm{Fct}(L) \cup \mathrm{Rel}(L) \cup \mathrm{Var})$$

qui n'est autre que β. □

8.1.12 Remarque

Si L possède un symbole de relation binaire $\leqq$ et si S comporte des axiomes permettant d'inférer que $\leqq$ est une relation d'ordre, on peut remplacer, dans la démonstration de la proposition 8.1.7, les axiomes γ_m par

$$\gamma'_m \equiv (m \leqq d) \wedge (\neg(m = d)) \quad , \quad m \in E_0$$

Dans ce cas, le modèle (E_1, J_1) comporte un élément strictement supérieur à tous les éléments du sous-modèle (E_0, J_0).

8.1.13 Application à (L_n, S_n)

Revenons au système formel (L_n, S_n) construit en vue de formaliser les nombres naturels. Admettons tacitement que c'est une théorie. Le corollaire 8.1.10 permet d'énoncer immédiatement:

8.1.14 Corollaire

Pour tout modèle dénombrable $(\mathbb{N}_1, J_1)$ de (L_n, S_n), il existe un modèle dénombrable $(\mathbb{N}_2, J_2)$ de (L_n, S_n) admettant $(\mathbb{N}_1, J_1)$ comme sous-modèle propre.

8.1.15 Démonstration

Il suffit de remarquer que les symboles propres à L_n sont en nombre fini. La conclusion découle alors du théorème de Löwenheim-Skolem (prop. 5.5.2) et du corollaire 8.1.10. □

8.1.16 Figuration d'un modèle quelconque de (L_n, S_n). L'idée de numéral

Lorsqu'on veut se représenter un modèle quelconque de (L_n, S_n), on est conduit à une image du type suivant:

$$\left.\begin{array}{l}
\left.\begin{array}{l}
\qquad 0 \qquad 1 \quad 1+1 \quad (1+1)+1 \ \ldots\ldots \qquad\qquad \text{numéraux} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots \ \mathrm{p}-1 \quad \mathrm{p} \qquad \mathrm{p}+1 \quad (\mathrm{p}+1)+1 \ \ldots\ldots\ldots\ldots
\end{array}\right\} \mathbb{N}_1 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots \ \mathrm{v}-1 \quad \mathrm{v} \qquad \mathrm{v}+1 \quad (\mathrm{v}+1)+1 \ \ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}\right\} \mathbb{N}_2$$

Fig. 8.0

Sur la première ligne, nous avons écrit 0, son successeur $0+1$, soit 1, le successeur de son successeur, $1+1$ et, d'une façon générale, les éléments successifs qu'on peut ***effectivement*** écrire avec les seuls signes typographiques: 0, 1, +, (,). On convient d'appeler chacun de ces éléments un *numéral*. Un même numéral peut s'écrire de plusieurs manières différentes, par exemple $(1+1)+1 = (1+0)+(1+1)$.

Les axiomes A_1 à A_5 permettent de passer de l'une à l'autre. Pour simplifier, nous les écrirons par la suite sous la forme décimale habituelle.

Considérons maintenant un modèle $(\mathbb{N}_1, J_1)$ de (L_n, S_n). Il comporte chaque numéral. Il est permis de croire qu'il ne contient rien d'autre, mais il est impossible de l'exprimer dans le langage L_n. En effet, s'il existait un ensemble M d'énoncés de L_n capable de traduire le fait que tout modèle de $(L_n\ S_n \cup M)$ ne comporte que les numéraux, la proposition 8.1.7 permettrait d'affirmer l'existence de deux modèles strictement emboîtés de $(L_n, S_n \cup M)$. Nous savons aussi qu'il existe un modèle $(\mathbb{N}_2, J_2)$ de (L_n, S_n), dont $(\mathbb{N}_1, S_1)$ est un sous-modèle propre. Mais, pour la même raison que ci-dessus, on ne peut pas exprimer dans L_n que $(\mathbb{N}_1, J_1)$ est un modèle minimal de (L_n, S_n).

8.1.17 Commentaires

Les numéraux correspondent à ce que nous avons appelé la notion "naïve" de nombre naturel. Nous avons alors utilisé les propriétés suivantes des numéraux:

- 0 et 1 sont des numéraux.
- Il est possible d'écrire effectivement chaque numéral et on peut donner autant d'exemples de numéraux distincts qu'on veut.
- Chaque numéral n admet un successeur bien déterminé qu'on peut noter $n+1$. Convenons d'appeler "chaîne complète" une suite effectivement écrite de numéraux telles que, de deux éléments consécutifs quelconques de la suite, le second est le successeur du premier. Un seul numéral constitue aussi une chaîne complète; il est à la fois le premier et le dernier élément de la chaîne.
- Pour toute collection (non vide) effectivement écrite de numéraux, il existe une unique chaîne complète comportant tous les éléments de la collection et dont le premier et le dernier élément appartiennent à la collection.
- Il est impossible d'écrire effectivement tous les numéraux, mais on peut admettre qu'ils forment une totalité.

On constate que la notion de numéral repose sur deux données apparemment antagonistes. La première est un critère d'écriture effective qui fait de chaque numéral un objet matériel. La deuxième est une décision audacieuse, un acte de foi par lequel on se donne le droit de penser la totalité (non matérielle) des numéraux. On confère alors à cette totalité des propriétés inspirées par certaines constatations faites sur les collections effectivement écrites de numéraux. A partir de là, chacun se forme une image personnelle de la totalité des numéraux.

La conception "naïve" des nombres naturels présente l'avantage considérable de nous faire ***voir*** une totalité des nombres naturels. Chacun de nous est intimement persuadé que le nombre décimal 9,9999 ... où on considère la totalité des chiffres 9 inscriptibles à droite de la virgule égale bien le nombre 10. (Ce fait peut soulever des difficultés chez certains débutants.) Cependant cette image "naïve" repose sur des assertions dont le contenu n'est pas simple et dont on peut craindre qu'elles aient recours à des notions plus complexes que les nombres naturels (voir discussion sur l'"axiome" Ω, 8.1.5).

La notion non naïve de nombre naturel apparaît lorsqu'on adopte par conventions un langage du premier ordre (par exemple L_n), des axiomes dans ce langage (par exemple S_n) et des règles d'inférence (par exemple celle de Hilbert). Dès lors, il n'y a plus d'ambiguïté sur ce qu'on appelle un théorème d'arithmétique. En revanche, on fait surgir la possibilité d'une multitude de modèles différents de l'arithmétique. Et rien dans les conventions passées ne permet de désigner l'un d'eux comme modèle privilégié. C'est l'aspect déconcertant d'un phénomène mathématique intéressant: l'existence de suites illimitées de modèles de l'arithmétique, chacun d'eux étant sous-modèle propre du suivant.

Remarquons encore qu'il existe une analogie étroite entre les propriétés que nous avons prêtées aux numéraux et les conventions que nous avons adoptées pour les formules d'un langage "élémentaire" du premier ordre L. En particulier, nous avons fait usage des faits suivants:

- il est possible d'écrire effectivement n'importe quelle formule de L et on peut donner autant d'exemples de formules de L qu'on veut;
- il est impossible d'écrire effectivement toutes les formules de L; mais on peut admettre qu'elles constituent une totalité: l'ensemble $\mathrm{For}(L)$;
- il est possible d'établir une correspondance biunivoque entre les formules de L et les numéraux.

8.2 UN SYSTÈME FORMEL DU PREMIER ORDRE POUR LES ENSEMBLES

8.2.0 Préambule

Nous nous sommes servis des nombres naturels, au moins sous la forme des numéraux, pour décrire les formules d'un langage du premier ordre L. De leur côté, les ensembles sont intervenus explicitement quand nous avons introduit la notion de L-structure. Nous avons rappelé à ce propos quelques propriétés relevant de ce que nous avons appelé alors la "notion naïve d'ensemble". Un aspect plus élaboré des ensembles apparaît quand on les décrit à l'aide d'un système formel du premier ordre. Nous allons présenter celui de Zermelo – Fraenkel qui a la faveur de beaucoup de mathématiciens.

8.2.1 Le langage L_e

Le langage du premier ordre L_e que nous allons considérer comporte en tout un symbole de constante $\emptyset$ et un symbole de relation binaire $\in$. Au lieu de "$\in(x, y)$", nous noterons "$x \in y$" qui se lit "x appartient à y". Dans toute L_e-structure, la constante et les variables sont interprétés comme des ensembles. Par suite, tout ensemble doit être considéré comme une collection d'ensembles.

Nous allons présenter les axiomes du système formel (L_e, S_e) en décrivant brièvement leur contenu intuitif. Nous nous laisserons guider par l'exposé de Paul J. Cohen.

8.2.2 Axiome de l'ensemble vide:

$$C_1 \equiv \forall x(\forall y(\neg y \in x) \leftrightarrow x = \emptyset).$$

Il existe exactement un ensemble sans élément, noté $\emptyset$.

8.2.3 Axiome d'extensionnalité:

$$C_2 \equiv \forall x(\forall y(\forall z(z \in x) \leftrightarrow (z \in y)) \leftrightarrow (x = y)).$$

Tout ensemble est déterminé par ses éléments.

8.2.4 Axiome des paires:

$$C_3 \equiv \forall x(\forall y(\exists z(t \in z) \leftrightarrow ((t = x) \vee (t = y)))).$$

Etant donnés les ensembles x et y, il existe (exactement) un ensemble admettant exclusivement x et y comme éléments. C'est la *paire* $\{x, y\}$. Lorsque $x = y$, $\{x, y\}$ se note $\{x\}$ au lieu de $\{x, x\}$. La paire ne comporte alors qu'un seul élément. Par exemple, $\emptyset \in \{\emptyset\}$. A l'aide de x et y, on peut former la paire $\{\{x\}, \{x, y\}\}$ appelée *couple* ou *paire ordonnée* (x, y).

8.2.5 Axiome de la réunion:

$$C_4 \equiv \forall x(\exists y(\forall z((z \in y) \leftrightarrow \exists t(t \in x \wedge z \in t)))).$$

Etant donné un ensemble x, il existe un ensemble y comportant exactement tous les éléments des ensembles qui appartiennent à x. y est la *réunion* des ensembles constituant x. Lorsqu'on prend pour x une paire $\{y, z\}$, la réunion considérée se note $y \cup z$.

8.2.6 Axiome de l'infini:

$$C_5 \equiv \exists x((\emptyset \in x) \wedge (\forall y((y \in x) \rightarrow (\exists z(z \in x) \wedge (\forall t(t \in z) \leftrightarrow ((t = y) \vee (t \in y))))))).$$

Lorsqu'on examine attentivement cette formule, on constate qu'elle peut s'abréger en:

$$\exists x((\varnothing \in x) \wedge (\forall y(y \in x) \rightarrow ((y \cup \{y\}) \in x)))$$

qui n'est malheureusement pas une formule de L_e; elle comporte des abréviations $\cup$ et $\{y\}$ liées à l'axiome des paires et à celui de la réunion. L'axiome C_5 peut donc se traduire ainsi: il existe un ensemble x comportant l'élément $\varnothing$ et tel que si y est élément de x, il en est de même de $y \cup \{y\}$. En particulier, x comporte les éléments $\varnothing$, $\{\varnothing\}$, $\{\varnothing\} \cup \{\{\varnothing\}\}$, ... qu'on peut mettre en correspondance avec les numéraux 0, 1, 2 ...

8.2.7 Axiome de l'ensemble des parties:

$$C_6 \equiv \forall x(\exists y(\forall z(z \in y) \leftrightarrow \forall t((t \in z) \rightarrow (t \in x))))$$

La formule $\forall t((t \in z) \rightarrow (t \in x))$ exprime que tout élément de z appartient à x, donc que z est une *partie* de $x : z \subset x$. L'axiome C_6 signifie que, pour tout ensemble x, les parties de x forment un ensemble y. Cet ensemble se note $\mathscr{P}(x)$; c'est l'*ensemble des parties* de x.

8.2.8 Axiome du choix (ou de Zermelo):

$$\begin{aligned} C_7 \equiv \forall x(\exists y(\forall z(((z \in x) \wedge (\neg(z = \varnothing))) \rightarrow \exists t((t \in y) \wedge (t \in z)))) \wedge \\ \forall t((t \in y) \rightarrow \exists s((s \in x) \wedge (t \in s))) \wedge \\ \forall z \forall u \forall v(((z \in x) \wedge (u \in z) \wedge (u \in y) \wedge (v \in z) \wedge (v \in y) \rightarrow (u = v)))). \end{aligned}$$

Pour tout ensemble x il existe un ensemble y ayant les propriétés suivantes:

- si z est un élément non vide de x, y a un élément dans z;
- si t est un élément de y, il existe un élément s de x qui comporte t;
- si z est un élément de x, il comporte au plus un élément de y.

On peut dire que y "choisit" un élément unique dans chaque élément non vide de x.

8.2.9 Axiome de régularité:

$$C_8 \equiv \forall x(\exists y((\neg(x = \varnothing)) \rightarrow ((y \in x) \wedge \forall z((z \in x) \rightarrow (\neg(z \in y))))))$$

Tout ensemble x non vide comporte un élément y qui ne contient aucun élément de x. Cet axiome a pour conséquence particulière qu'un ensemble ne saurait être élément de lui-même. Car si $x \in x$, alors $\{x\}$ qui est réduit au seul élément x ne vérifierait pas l'axiome de régularité.

8.2.10 Schéma d'axiomes de remplacement:

On désigne ainsi une collection d'énoncés qui présente une certaine analogie avec le schéma d'axiomes de l'induction complète. Numérotons cette fois toutes les formules de L_e comportant au moins deux symboles de variables libres x et y. Désignons par $\varphi_p(x, y, v_1, \dots, v_{m_p})$, la p-ième formule de la liste, $v_1, \dots, v_{m_p}$ étant des symboles de variables, posons alors:

$$\begin{aligned} D_p \equiv\ & \forall v_1 \dots \forall v_{m_p} (\forall x(((\exists y \varphi_p(x, y, v_1, \dots, v_{m_p})) \wedge \\ & (\forall y \forall z(((\varphi_p(x, y, v_1, \dots, v_{m_p}) \wedge \varphi_p(x, z, v_1, \dots, v_{m_p})) \rightarrow (y=z)))))) \rightarrow \\ & (\forall u \exists v(\forall r(r \in v) \rightarrow \exists s((s \in u) \wedge \varphi_p(s, r, v_1, \dots, v_{m_p}))))) \\ & p=0, 1, 2, 3, \dots . \end{aligned} \tag{8.18}$$

Pour imaginer le contenu intuitif de D_p, considérons qu'il est de la forme $\forall v_1 \dots v_{m_p}\ \alpha \rightarrow \beta$. La formule α, qui commence par ($\forall x$ et finit à $(y=z))))))$, signifie que, pour tout ensemble x, il existe un ensemble y et un seul tel que $\varphi_p(x, y, v_1, \dots, v_{m_p})$. Autrement dit, lorsqu'on suppose fixées les variables $v_1, \dots, v_{m_p}$, la formule $\varphi_p(x, y, v_1 \dots v_{m_p})$ détermine y "en fonction" de x. La formule β signifie que, pour tout ensemble u, la relation fonctionnelle $\varphi_p(x, y, v_1, \dots, v_{m_p})$ restreinte à u associe aux éléments de u une collection d'images qui constitue un ensemble v.

Prenons un exemple simple: considérons l'axiome de l'ensemble des parties, C_6. Il a la forme $\forall x(\exists y \psi(x, y))$, où $\psi(x, y)$ porte peut-être le numéro 57 dans la liste des formules de L_e comportant au moins les variables libres x et y: $\psi \equiv \varphi_{57}$. L'axiome C_6 exprime que φ_{57} a le caractère fonctionnel: à tout ensemble x correspond exactement un ensemble $y = \mathscr{P}(x)$. L'axiome D_{57} nous dit alors que lorsque x parcourt un ensemble u, $\mathscr{P}(x)$ parcourt aussi un ensemble. Cette assertion n'est pas banale: nous allons voir bientôt qu'il existe des collections d'ensembles qui ne sont pas des ensembles.

$\{D_p | p=0, 1, 2, 3, \dots\}$ est le *schéma d'axiomes de remplacement*. Par lui s'achève la présentation des axiomes. Nous n'en entreprendrons pas l'analyse, renvoyant pour cela le lecteur à l'ouvrage de Paul J. Cohen.

8.2.11 Le système formel (L_e, S_e)

Posons $S_e = \{C_1, C_2, \dots, C_8, D_0, D_1, D_2, D_3, \dots\}$. Le système formel ($L_e$, S_e) permet d'établir toutes les propriétés des ensembles utilisées par les mathématiciens. En particulier, il est possible d'y définir toutes les notions que nous avons introduites pour les ensembles naïfs: celles d'application, d'intersection et de produit cartésien d'ensembles, par exemple. Il y a tout lieu de croire que (L_e, S_e) n'implique pas contradiction. Si c'est bien le cas, (L_e, S_e) est, au sens strict, une *théorie des ensembles*. D'après le théorème de complétude, (L_e, S_e) admet alors au moins un modèle "ensembliste" (E, J).

8.2.12 Remarque

Relevons d'emblée un fait assez surprenant. Les ensembles mathématiques munis de la relation d'appartenance $\in$ constituent une sorte de "modèle" de (L_e, S_e) en ce sens que, selon toute vraisemblance, ils satisfont les axiomes de S_e. Toutefois, ils ne forment pas un ensemble mathématique E, car alors la relation $E \in E$ serait satisfaite dans le "modèle", ce que l'axiome de régularité C_8 exclut. Donc, si, comme il est hautement probable, (L_e, S_e) est une théorie, elle admet des modèles ensemblistes mais aucun d'eux ne coïncide avec le modèle intuitif des mathématiciens.

D'une façon générale, si (E, J) est un modèle de la théorie des ensembles (L_e, S_e), E représente une collection qui, ***dans le modèle*** (E, J), n'est pas un ensemble. La théorie des ensembles (L_e, S_e) nous oblige donc à admettre qu'il existe des collections qui ne sont pas des ensembles.

8.2.13 Remarque

Dans notre présentation de la logique du premier ordre, nous avons fait un ample usage du terme d'"ensemble". Nous avons introduit les interprétations "ensemblistes", nous avons considéré l'"ensemble" des formules d'un langage L, etc. Toutes les opérations que nous avons effectuées sur ces "ensembles" peuvent être décrites dans le langage L_e, avec l'aide des axiomes S_e. Toutefois, nous n'avons pas soumis nos "ensembles" à toute la force des axiomes S_e. Par exemple, nous n'avons jamais eu l'occasion de nous demander si une collection était un "ensemble" ou non; ce qui signifie que nous n'avons pas fait usage de l'axiome de régularité C_8. Nous nous sommes donc servis d'une notion plus vague, moins élaborée que celle d'ensemble mathématique. C'est pourquoi nous l'avons qualifiée, à l'époque, de "naïve".

Sous l'angle où nous les envisageons ici, les nombres naturels et les ensembles présentent une analogie certaine. Au début, nous disposons de notions "naïves" – les numéraux, les ensembles naïfs – auxquelles nous prêtons des propriétés commodes et naturelles. Notre intuition nous en fait voir des exemples nombreux. A partir de ces notions, nous élaborons une logique du premier ordre qui nous conduits à quelques propriétés intéressantes. Nous nous retournons alors vers les nombres naturels et les ensembles que nous nous efforçons de maîtriser à l'aide de notre nouvel outil. Nous constatons alors deux faits remarquables:

- la logique du premier ordre n'est pas en mesure de nous faire *voir* un modèle des nombres naturels ou des ensembles. A cet égard, elle n'a pas le pouvoir persuasif de l'intuition.
- En revanche, pour autant que les notions naïves de nombre naturel et d'ensemble ne soient pas en elles-mêmes contradictoires, la logique du premier ordre nous administre la preuve qu'il existe d'autres réalisations que celles que nous présente l'intuition.

Pour être plus précis, nous avons d'abord acquis les moyens de démontrer que, sous l'hypothèse raisonnable que (L_n, S_n) et (L_e, S_e) sont des théories, ils admettent de multiples modèles. Nous avons appris ensuite qu'il est possible d'étudier l'arithmétique, tout comme les ensembles, dans des systèmes formés de plusieurs modèles emboîtés. Nous sommes ainsi parvenus à la conception de notions moins naïves que celles dont nous sommes partis.

Rien n'empêche d'imaginer qu'on reprenne la présentation de la logique du premier ordre à partir des nombres naturels et des ensembles moins "naïfs". En définissant la notion de «modèle ensembliste" à l'aide des éléments d'un modèle ordinaire de (L_e, S_e), on accèderait à une logique du premier ordre à son tour "moins naïve".

8.2.14 Remarque

Ajoutons une autre remarque sur la théorie des ensembles. Les symboles propres de L_e se réduisent à deux: $\emptyset$ et $\in$. Donc For(L_e) est dénombrable. D'autre part, il résulte de l'axiome de l'infini qu'aucun modèle de (L_e, S_e) n'est fini. Il résulte alors du théorème de Löwenheim – Skolem – Tarski que (L_e, S_e) admet des modèles de cardinal infini arbitraire.

Le fait qu'il existe un modèle dénombrable (E, J) de la théorie des ensembles (L_e, S_e) – pour autant qu'elle en soit une – a beaucoup surpris les mathématiciens lors de sa découverte, En effet, l'axiome de l'infini implique qu'il existe dans le modèle (E, J) un ensemble infini a. En vertu du théorème de Cantor (cf. n° 7.0.2), qui admet une preuve dans (L_e, S_e), le cardinal de $\mathscr{P}(a)$ est infini non dénombrable. Les éléments de $\mathscr{P}(a)$ sont des éléments distincts de E. Comment peut-on trouver dans l'ensemble dénombrable E, un sous-ensemble infini dont le cardinal excède celui de E?

Le paradoxe disparaît quand on dissipe la confusion que nous venons de faire entre les ensembles "naïfs" où figure E et les ensembles dans le modèle (E, J). En effet, si deux parties infinies U et V de l'ensemble "naïfs" E sont dénombrables au sens "naïf", il existe une bijection $\alpha: U \to V$ au sens naïf. En revanche, si on considère dans E deux éléments u et v représentant des ensembles infinis au sens de la théorie (L_e, S_e), toute application $f: u \to v$ est un *ensemble* de couples (x, y) où $x \in u$ et $y \in v$: f est donc un élément de E. Il peut fort bien arriver qu'aucun élément de E ne soit le représentant d'une *bijection* de u sur v, au sens de (L_e, S_e). Dès lors, u et v n'auraient pas le même cardinal au sein du modèle (E, J). L'un d'eux au moins serait infini non dénombrable dans (E, J).

Relevons en passant que quelques-uns des résultats les plus révélateurs sur les fondements des mathématiques ont été obtenus à partir de modèles dénombrables – au sens naïf – de (L_e, S_e).

8.2.15 Remarque

Formulons une dernière observation de caractère plus général. Les langages du premier ordre que nous avons employés pour formaliser l'arithmétique et la théorie des ensembles sont remarquablement simples. Toutefois les axiomes nécessaires ont un aspect rébarbatif. C'est avec inquiétude qu'on constate la longueur des formules qui apparaissent quand on introduit ces axiomes dans la preuve de théorèmes même élémentaires. On pourrait évidemment utiliser une machine convenablement programmée pour corriger les fautes de copie ou d'"orthographe". Mais il resterait encore à une personne humaine l'obligation d'imaginer quelles règles d'inférence il faut faire intervenir, à quel endroit et dans quelle intention. La complexité des formules deviendrait rapidement un obstacle insurmontable. Personne ne peut lire et "comprendre" une formule de deux cents symboles dans L_n ou L_e comme on le fait d'une phrase de même longueur dans un roman.

Heureusement, le théorème de complétude de la logique du premier ordre vient à notre aide. Comme il n'y a aucune divergence entre le jeu des formules dans L_n ou L_e et leurs interprétations dans n'importe quel modèle de $(L_n\ S_n)$ ou de $(L_e,\ S_e)$, respectivement, il est possible de jouer alternativement sur les deux tableaux. C'est ce que nous avons fait lorsque nous avons interprété et commenté les axiomes de Zermelo – Fraenkel. Dès lors, il devient possible d'élaborer ***pratiquement*** une théorie axiomatique de l'arithmétique ou des ensembles. Les formules peuvent être contrôlées indifféremment sous leur aspect syntaxique ou dans leur contenu sémantique. Cette remarque s'étend évidemment à toutes les théories du premier ordre qu'on voudra, pour autant qu'elles admettent des modèles suffisamment intuitifs.

8.3 LOGIQUE "NAÏVE" ET LOGIQUE DU PREMIER ORDRE. LOGIQUE PRATIQUE

8.3.0 Remarques sur la logique "naïve"

Nous venons de constater qu'au cours de notre exposé, les notions de nombre naturel et d'ensemble ont passé d'un stade "naïf" à un statut plus élaboré. Qu'en est-il de la logique elle-même que nous avons mise à contribution tout au long de nos démonstrations? Nous allons essayer de montrer que nous nous sommes servis d'une logique qu'on peut aussi qualifier de "naïve" par comparaison avec la logique du premier ordre.

A la manière des mathématiciens, nous avons employé des locutions telles que "et", "ou", "quel que soit", "si... , alors..." qui évoquent clairement des symboles logiques $\wedge$, $\vee$, $\forall$, $\rightarrow$. Examinons de plus près les ressemblances et les différences entre ces deux familles d'objets.

A priori, les symboles logiques n'ont aucune signification. Ils prennent figure peu à peu, lorsqu'on considère les interprétations ensemblistes, lorsqu'on introduit la logique des propositions et enfin lorsqu'on pose les règles d'inférence. Très tôt, les symboles $\neg$, $\wedge$, $\vee$ sont mis en relation étroite avec la négation, les conjonctions et, ou:

$(E, J) \models (\neg\varphi)$ est la négation de $(E, J) \models \varphi$
$(E, J) \models \varphi \wedge \psi$ a le même sens que $((E, J) \models \varphi$ *et* $(E, J) \models \psi)$
$(E, J) \models \varphi \vee \psi$ a le même sens que $((E, J) \models \varphi$ *ou* $(E, J) \models \psi)$

Notons que "*et*" et "*ou*" ont la même acception qu'en mathématiques.

Le symbole logique $=$ est interprété dans toute L-structure comme en mathématiques: placé entre deux signes, il signifie qu'ils désignent un seul et même objet. Cette proximité de sens nous a conduit, par souci de clarté, à introduire le signe typographique $\equiv$ pour indiquer que deux notations désignent le même agrégat de symboles.

Venons-en au symbole d'implication $\rightarrow$ et à $\leftrightarrow$ qui lui est lié. Pour les besoins de nos raisonnements, nous avons introduit les signes $\Rightarrow$ et $\Leftrightarrow$. Malgré les apparences, $\rightarrow$ et $\Rightarrow$ ont des emplois différents. Dans un langage du premier ordre, quelles que soient les formules α et β, on peut former la formule $\alpha \rightarrow \beta$. En outre, $\alpha \rightarrow \beta$ a les mêmes interprétations et les mêmes valeurs de vérité que $\beta \vee (\neg\alpha)$ qui n'évoque pas l'idée d'une implication active. En revanche, dans nos raisonnements, $\Rightarrow$ est toujours placé entre des assertions qui ont quelque chose à voir ensemble dans leur contexte, comme:

"α est une formule de L" $\Rightarrow$ "$(\neg\alpha)$ est une formule de L".

Nous n'avons pas été tentés d'exploiter des "implications" telles que:

"il pleut" $\Rightarrow$ "Socrate est mortel",

ou encore:

"α est une formule" $\Rightarrow$ "6 est un nombre naturel".

En outre, nous nous sommes toujours placés dans l'hypothèse où la prémisse *et* l'implication sont toutes deux valides. Donc notre signe $\Rightarrow$ évoque une sorte de *causalité* qu'il ne faut pas confondre avec la stricte implication logique. Il traduit une règle pratique qu'on peut rapprocher de "*modus ponens*".

L'écart se creuse entre la logique du premier ordre et la logique naïve du mathématicien quand on passe aux quantificateurs. La parenté peut paraître étroite entre $\forall$ et la locution "quel que soit". En revanche, notre "il existe" n'est que très partiellement rendu par $\exists$. En effet, $\exists x$ admet les mêmes interprétations que $\neg\forall x \neg$, qui revient à nier une absence. Tandis que, lorsque nous affirmons: "il existe une fonction de vérité V ayant telle propriété P", nous voulons dire: "nous savons décrire une procédure effective permettant de construire une fonction de vérité V ayant la propriété P". La différence est essentielle. Pendant longtemps, les mathématiciens n'ont admis l'existence d'un objet mathématique (nombre, fonction, forme géométrique) que lorsqu'ils étaient en mesure de le décrire expressément. Les mathématiques ont pris un tournant historique lorsque les mathématiciens ont accepté le principe suivant, qu'on peut qualifier d'hilbertien: ***l'existence d'un objet mathématique est assurée lorsqu'elle ne provoque pas de contradiction***. Ainsi l'axiome du choix (cf. n° 8.2.8) qui permet d'affirmer qu'il existe un bon ordre sur les nombres réels a conduit à des progrès considérables en analyse, alors même que personne n'est capable de décrire un tel bon ordre.

Rappelons à ce propos la proposition 6.3.10. Elle nous enseigne que si un système formel du premier ordre (L, S) est consistant, il admet un modèle. La non-contradiction (de L, S)) entraîne l'existence (d'un modèle de (L, S)). Nous constatons que la logique du premier ordre s'adapte à une conception hilbertienne des mathématiques. En revanche, la logique naïve dont nous nous sommes servis tout au long de nos démonstrations relève d'une vision traditionnelle des mathématiques.

Formulons encore une dernière remarque au sujet des quantificateurs. Dans le langage ordinaire, "il existe un animal qui avale des cailloux" ou "toute peine mérite salaire" renvoient implicitement à des référentiels: les animaux vivant sur la Terre ou les travaux effectués consciemment par des êtres humains. Il en est de même en mathématiques. Ce n'est pas le cas en logique du premier ordre. $\forall$ et $\exists$ sont employés même en l'absence de tout modèle. "$\forall x(x=x)$" et "$\exists x \neg(x=y)$" sont des énoncés qui ne sont attachés à aucun modèle en particulier. Nous mettons là le doigt sur l'une des différences majeures entre la logique formelle et la logique "naïve". Celle-ci s'exerce toujours au sein d'*une* interprétation particulière. C'est pourquoi la logique naïve est *a priori* plus intuitive, plus facile. Le bon sens permet de laisser tomber des morceaux de preuves évidentes, ce qui allège les raisonnements. Mais il arrive à ce même "bon sens" de dissimuler des lacunes logiques graves. L'histoire des mathématiques en fournit des exemples remarquables.

8.3.1 Remarques sur la logique pratique

Pour terminer ce numéro, disons quelques mots de la "logique pratique", celle de l'artisan, du politicien et de l'homme de la rue. Elle a en commun avec la logique naïve du mathématicien d'être toujours "en situation". Contrairement à ce qu'on exige de la logique du premier ordre, de la logique formelle en général, les arguments de la logique pratique tirent une part importante de la pertinence de l'interprétation des termes qui y figurent. Mais tandis que les mathématiciens adoptent à peu près constamment les mêmes critères de validité, qu'ils fassent de l'algèbre, de la topologie ou de la logique, le raisonnement pratique procède de manières très différentes selon qu'il s'agit de gagner les voix des électeurs, d'innocenter un prévenu ou de rechercher la cause d'une panne de voiture. Toute théorie de l'argumentation doit donc prendre en compte, outre une bonne connaissance de la logique formelle, les acquis de la sociologie, de la psychologie, de l'histoire, de la linguistique, etc. Il n'est pas question d'aborder ici ces vastes problèmes qui sont encore largement ouverts. Nous nous bornerons à quelques remarques très élémentaires.

Ce que nous avons dit de l'implication et des quantificateurs en logique naïve vaut aussi pour la logique pratique. On pourrait d'ailleurs aller plus loin en notant que le langage ordinaire ne dispose pas d'une notion claire de "variable". Par exemple, les règles de généralisation n'ont pas d'équivalent en logique pratique.

L'emploi même des quantificateurs dans la langue commune n'est pas facile à décrire. "Le loup mange l'agneau" équivaut à "l'agneau est mangé par le loup". Mais "tous les enfants boivent une tasse de lait" équivaut-il à "une tasse de lait est bue par tous les enfants"?

Examinons plutôt la signification pratique de l'égalité, de la négation et des conjonctions "et" et "ou". Le signe " = " peut avoir une acception très large: "santé = sobriété". Mais il lui arrive d'avoir un sens très restreint. En leçons de calcul, la question "$3\times 4=?$" appelle la réponse 12. $(5+7)$ ou (2×6) seraient considérées comme inexactes, voire déplacées.

La négation a ordinairement une connotation dépréciative. Elle correspond souvent à une perte d'information. "Le chat n'est pas noir" nous donne moins de renseignements que "le chat est noir". On a parfois de la peine à comprendre une accumulation de négations: " non qu'il ne soit pas vain de nier que la suppression des interdictions de s'abstenir n'est pas illégale". En logiques naïve et du premier ordre, il est possible de nier n'importe quelle formule. Ce n'est pas toujours facile en pratique. La négation de "Platon est un triangle équilatéral" est-elle bien "Platon n'est pas un triangle équilatéral"? Le statut ambigu de la négation apparaît dans le dialogue suivant:

- Et vous, que dites-vous?
- Je ne dis rien!
- Mais vous le dites!
- Je ne dis rien, et je le dis!

Cette dernière exclamation, qu'on attribue au musicien John Cage, n'est pas dénuée de sens, bien qu'elle contrevienne à la tautologie de non-contradiction. Notons en passant qu'Aristote ne considérait pas l'opération logique consistant à nier une proposition. Ce sont apparemment les Stoïciens qui l'introduisirent méthodiquement.

En français, la conjonction "et" a des acceptions très diverses, que ne connaissent ni la logique du premier ordre, ni la logique "naïve":

- le joueur a un maillot rouge *et* un maillot blanc
- le joueur a un maillot rouge *et* blanc
- le maillot du joueur est rouge *et* il est blanc
- tu me téléphones *et* je viens t'aider
- il arrive à Genève *et* il prend l'avion
- il prend l'avion *et* il arrive à Genève.

On constate sur ces deux derniers exemples que la permutation des deux assertions conjointes traduit une intervertion temporelle des événements correspondants. Un tel phénomène ne se produit pas en logique du premier ordre, pas plus qu'en mathématiques où le temps est absent.

En français, la conjonction "ou" est généralement prise dans son sens exclusif. La devise "vaincre ou mourir" ne semble pas tout à fait observée quand on exécute les deux à la fois; on entend bien "soit vaincre, soit mourir". Il faut un effort pour admettre qu'un chapeau noir est noir ou gris. Beaucoup d'écoliers refusent de croire que si $x<0$, alors $x \leqq 0$. Il y a lieu de penser que, parfois, "ou" est mis pour "et", comme le suggère cet avertissement apposé à l'entrée d'un établissement thermal: "Les enfants non accompagnés ou sans ordonnance ne sont pas admis dans l'établissement.".

René Thom a mis en évidence les comportements sémantiques différents de "et" et "ou". Imaginons les exemples suivants:

- Il déplie son journal *et* le train démarre.
- Il déplie son journal *ou* le train démarre.
- Mange ton gâteau *et* garde-le pour ce soir.
- Mange ton gâteau *ou* garde-le pour ce soir

Selon René Thom, les propositions "α *et* β", d'une part, "α *ou* β" d'autre part, ne sont pas simultanément acceptables du point de vue de la signification. Cette "règle" n'est pas d'une application universelle, comme on le constate sur "la bonne est sourde ou (resp. et) le voleur est entré par la fenêtre". Mais elle nous fait sentir ce qui sépare la logique pratique de ce que nous avons appelé la logique "naïve", et, *a fortiori*, de la logique formelle du premier ordre. Pour sa part, le mathématicien ne donne pas moins de sens à "b est pair *et* c est divisible par 7" qu'à "b est pair *ou* c est divisible par 7".

8.4 ARITHMÉTIQUE ET LOGIQUE DU PREMIER ORDRE LES THÉORÈMES D'INCOMPLÉTUDE DE GÖDEL (ÉNONCÉS ET REMARQUES)

8.4.0 Préambule

Nous avons consacré le § 8.1 à la description d'un système formel du premier ordre (L_n, S_n) pour les entiers naturels. Nous avons relevé à cette occasion certaines analogies entre les numéraux et les formules d'un langage du premier ordre, comme (L_n, S_n) en particulier. L'axiomatisation de l'arithmétique est d'une importance primordiale pour les mathématiques. On peut toutefois imaginer que les logiciens aient eu, pour leur part, des raisons de s'y intéresser. C'est ce que nous allons essayer de faire voir d'une manière intuitive en évoquant les théorèmes dits d'incomplétude de Gödel.

8.4.1 Définition

Une théorie du premier ordre (L, S) est dite *complète* quand, pour tout énoncé α de L, ou bien $S \vdash \alpha$ ou bien $S \vdash (\neg\alpha)$. Dans ce cas, soit (E, J) un modèle quelconque de (L, S) et soit β un énoncé de L: si $(E, J) \models \beta$, alors $S \vdash \beta$. En revanche, si (L, S) est une théorie du premier ordre *incomplète*, il existe un énoncé γ de L et deux modèles (E_1, J_1), (E_2, J_2) de (L, S) tels que $(E_1, J_1) \models \gamma$ et $(E_2, J_2) \models (\neg \gamma)$. Le bon sens suggère que (L_n, S_n) ne peut être autre chose qu'une théorie du premier ordre complète.

8.4.2 Première approche du premier théorème d'incomplétude

En 1931, un an après la publication du théorème de complétude de la logique du premier ordre, le monde des logiciens et des philosophes des sciences fut secoué par les fameux théorèmes d'incomplétude de Gödel. Celui-ci montrait en effet que, sous réserve qu'elle soit une théorie, (L_n, S_n) était incomplète.

Schématiquement, Gödel s'y prenait de la manière suivante. Dans (L_n, S_n), abrégeons $1+1$ par 2, $(1+1)+1$ par 3, etc. Les numéraux 0, 1, 2, 3, ... sont des termes clos dans L_n. Nous savons qu'ils permettent de numéroter les formules de L_n comportant exactement un symbole de variable libre x: $A_0(x)$, $A_1(x)$, $A_2(x)$, ... , $A_p(x)$, ...Dans la p-ième formule $A_p(x)$, substituons à x le numéral p. On obtient ainsi une suite d'énoncés: $A_0(0)$, $A_1(1)$, ... , $A_p(p)$, ... dans L_n.

Considérons l'assertion:

$B(p) \equiv$ "$A_p(p)$ n'admet pas de preuve dans (L_n, S_n)".

Essayons de nous convaincre que $B(p)$ est une formule de L_n, comportant un symbole de variable libre p. Alors $B(x) \equiv B(p)^p_x$ apparaît parmi les formules numérotées au début: il existe un numéral r tel que $B(x) \equiv A_r(x)$. Considérons l'énoncé $B(r)$.

Si $B(r)$ admet une preuve dans (L_n, S_n), cela signifie qu'on peut prouver dans (L_n, S_n) que $A_r(r)(\equiv B(r))$ n'admet pas de preuve dans (L_n, S_n). Si (L_n, S_n) est consistant, il est alors vrai que $B(r)$ n'admet pas de preuve dans (L_n, S_n). Nous sommes conduits à une contradiction.

Si $(\neg B(r))$ admet une preuve dans (L_n, S_n), cela signifie qu'on peut prouver dans (L_n, S_n) qu'il est faux que $A(r)$ soit sans preuve dans (L_n, S_n). (L_n, S_n) étant supposé consistant, il existe donc une preuve de $A_r(r)(\equiv B(r))$ dans (L_n, S_n). Cela n'est pas possible si (L_n, S_n) est consistant.

Par suite, ***si*** (L_n, S_n) ***est une théorie, ni*** $B(r)$***, ni*** $\neg B(r)$ ***n'admettent de preuve dans*** (L_n, S_n)***.*** (L_n, S_n) est alors une théorie incomplète. D'après la proposition 6.3.12, il existe deux modèles nécessairement distincts de (L_n, S_n), l'un satisfaisant $B(r)$, l'autre $\neg B(r)$. Ainsi, non seulement il existe des modèles distincts de l'arithmétique comme le montre le théorème de Löwenheim – Skolem – Tarski, mais il existe des arithmétiques différentes. Ce phénomène a beaucoup choqué à l'époque.

8.4.3 L'idée de l'arithmétisation de la syntaxe

Telle que nous l'avons présentée ci-dessus, l'argumentation n'est qu'à moitié convaincante. Gödel procédait avec beaucoup plus de soin! Toutefois, faisant sienne une idée de Herbrand, Gödel mit au point une nouvelle démonstration extrêmement intéressante, qui parut en 1934. Elle était fondée sur un principe qu'on a appelé l'*arithmétisation de la syntaxe*. Jusqu'ici, la "théorie" des nombres naturels était subordonnée aux lois de la logique du premier ordre. La méthode de Gödel revient à appliquer à la logique de premier ordre les règles de l'arithmétique.

Essayons de suggérer cela.

Pour écrire les formules d'un langage du premier ordre quelconque L, il suffit de seize signes typographiques. Attachons à chacun d'eux un numéro, à notre gré. Par exemple:

$$\begin{array}{cccccccccccccccc} c & x & = & \neg & \wedge & \vee & \rightarrow & \leftrightarrow & ' & f & R & (& , &) & \forall & \exists \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{array} \tag{8.19}$$

A toute formule $\varphi \in \mathrm{For}(L)$, on peut assigner un numéral $G(\varphi)$ bien déterminé appelé *nombre de Gödel* de φ. Pour simplifier, montrons cela sur un exemple.

Considérons $\varphi \equiv \forall x(c' = x)$

$$\begin{array}{cccccccc} \forall & x & (& c & ' & = & x &) \\ 15 & 2 & 12 & 1 & 9 & 3 & 2 & 14 \end{array}$$

Posons: $G(\varphi) = 2^{15} \cdot 3^2 \cdot 5^{12} \cdot 7^1 \cdot 11^9 \cdot 13^3 \cdot 17^2 \cdot 19^{14}$. Ce nombre est obtenu en élevant les nombres premiers successifs à des puissances respectivement données par les numéros des signes apparaissant dans φ et en formant le produit des nombres qui en résultent. Tout nombre naturel supérieur à 1 admet une unique décomposition en puissances positives de nombres premiers croissants. La donnée de $G(\varphi)$ permet donc de retrouver φ. A toute suite finie T de formules de L, $\varphi_1, \varphi_2, \ldots, \varphi_r$, on peut associer un nombre $G(T)$ par le même procédé, à condition de marquer les virgules à l'aide du chiffre 13. On peut ainsi coder par des nombres de Gödel les preuves de tout système du premier ordre (L, S).

Imaginons un petit segment d'une telle preuve, obtenu, par exemple, par la règle *modus ponens*: $\ldots, \alpha, \alpha \rightarrow \beta, \beta, \ldots$ où α et β sont des formules de L. Lorsqu'on connaît les numéraux $G(\alpha)$ et $G(\alpha \rightarrow \beta)$, il semble possible de calculer le nombre de Gödel de β. Mais qu'entend-on au juste par "calculer"?

8.4.4 L'idée de fonction récursive générale

Suivons toujours l'idée de Gödel. Il définit maintenant une classe de fonctions qu'on pourrait appeler "calculables" et qu'on désigne plutôt du terme de *fonctions récursives générales*. Il s'agit là d'une notion assez subtile que nous allons essayer de suggérer. Considérons à titre d'exemple, la fonction binaire f_2 définie sur les couples de numéraux et caractérisée par:

$$\begin{cases} f_2(x, 0)=1 \\ f_2(x, y+1)=f_2(x, y) \cdot x \end{cases} \tag{8.20}$$

Par des substitutions très simples, on obtient successivement:

$$\begin{array}{lll} f_2(0, 0)=1 & f_2(1, 0)=1 & f_2(2, 0)=1 \ \ldots \\ f_2(2, 1)=1 \cdot 2 & f_2(2, 1)=2 & \\ f_2(2, 2)=2 \cdot 2 & f_2(2, 2)=4 & \\ f_2(2, 3)=4 \cdot 2 & f_2(2, 3)=8 \ \ldots & \end{array}$$

On constate bientôt que, pour tout couple de numéraux (m, n), on peut trouver un unique numéral p tel que $p=f(m, n)$ par une suite de "déductions" permettant de déterminer de proche en proche les valeurs intermédiaires de f_2. Dans le cas particulier, $f_2(m, n)=m^n$.

Pour déterminer une fonction récursive (générale) q-aire, on commence par adjoindre au langage L_n des symboles de fonctions, dont celui d'une fonction q-aire. Posons $L'_n=L_n \cup \{f_q, g_i, \ldots\}$. Dans L'_n, on appelle *équation* toute formule de la forme $t_1=t_2$, où t_1 et t_2 sont des termes de L'_n. On adopte d'autre part les règles générales de "déduction" suivantes:

- de l'équation $t_1=t_2$ on peut déduire $t_2=t_1$
- à partir d'une équation comportant un symbole de variable x, on peut déduire une nouvelle équation en substituant à x un terme clos.
- à partir d'une équation comportant le terme clos t_1, on peut déduire une nouvelle équation en substituant à t_1 le terme clos t_2, à condition qu'on ait déjà l'équation $t_1=t_2$.

On se donne enfin une collection finie C d'équations de sorte que, pour tout q-uple de numéraux $(n_1, \ldots, n_q)$, il existe un numéral p et un seul tel que l'équation

$$p=f_q(n_1, \ldots, n_q)$$

puisse être déduite de C par un nombre fini de déductions.

Les systèmes d'équations 8.21, 8.22 et 8.23 déterminent chacun une fonction récursive:

- $$\begin{cases} f_1(0)=0 \\ g_1(0)=0 \\ g_1(x+1)=f_1(x)+1 \\ f_1(x+1)=g_1(x) \cdot f_1(x) \end{cases} \tag{8.21}$$
- $$\begin{cases} f_2(x, 0)=x \\ f_2(x, y) \cdot f_2(y, x)=0 \\ f_2(x+1, y+1)=f_2(x, y)) \end{cases} \tag{8.22}$$
- $$\begin{cases} f_2(x, 0)=x+1 \\ f_2(0, y+1)=y+1 \\ f_2(x+1, y+1)=f_2(x, f_2(x+1, y)) \end{cases} \tag{8.23}$$
- $$\begin{cases} f_2(0, 0)=0 \\ f_2(x+1, y)=f_2(x, y)+1 \\ f_2(x, y+1)=f_2(y, y) \end{cases} \tag{8.24}$$

Le lecteur n'aura aucune peine à identifier la fonction récursive déterminée par (8.22). Il vérifiera également que (8.24) ne détermine pas une fonction.

Convenons de qualifier de *numérale* toute fonction dont les arguments et les valeurs sont des numéraux. Les fonctions récursives générales sont des fonctions numérales très particulières: celles qui sont calculables selon les consignes que nous avons données. Une fonction numérale dont les valeurs seraient tirées au sort ne serait probablement pas récursive. Néanmoins, la classe des fonctions récursives générales est assez vaste pour contenir:

- tous les calculs arithmétiques classiques sur les numéraux: les quatre opérations, la décomposition en facteurs premiers, etc...;
- la vérification qu'un numéral est, ou n'est pas, le nombre de Gödel d'une formule dans un langage formel donné, ou le nombre de Gödel d'une preuve dans un système formel donné;
- le calcul du nombre de Gödel d'une formule sachant qu'elle dérive selon une règle d'inférence donnée de formules dont le nombre de Gödel est connu;
- la détermination, à partir du nombre de Gödel d'une preuve, du nombre de Gödel de la formule prouvée.

Il est facile de se convaincre que la caractérisation que nous avons donnée des fonctions récursives générales peut être traduite dans le langage du premier ordre L_n auquel on adjoint des symboles de fonctions en suffisance. Tout numéral est un terme clos de la forme $((...((1+1)+1)+...)+1)$ comme nous l'avons déjà dit. Les règles de déduction sont des cas particuliers des axiomes de Leibniz et de l'axiome de spécification du type $\forall x\varphi \to \varphi_t^x$ (cf. définition 6.1.0) combiné avec le corollaire 6.2.10 et la règle *modus ponens*. Le caractère fonctionnel de f_q se traduit par:

$$\forall n_1 ... \forall n_q((\exists p f_q(n_1, ... , n_q)=p) \wedge (\forall r \forall s(f_q(n_1, ... , n_q)=r \wedge f_q(n_1, ... , n_q)=s) \to (r=s)))).$$

Désignons par $\overline{L}_n$ le langage du premier ordre obtenu en adjoignant à L_n une collection dénombrable de symboles de fonctions unaires, de symboles de fonctions binaires etc... . $(\overline{L}_n, S_n)$ est encore un système formel du premier ordre pour les nombres naturels. Ce qui précède fait apparaître un fait remarquable: quel que soit le système formel du premier ordre (L, S), la formation des formules de L, la construction des preuves dans (L, S), peuvent être traduites dans $(\overline{L}_n, S_n)$. C'est le phénomène de l'*arithmétisation de la logique* du premier ordre. Il s'étend sans peine à d'autres logiques formelles dont nous donnerons un aperçu au paragraphe suivant. Dès lors il est facile de comprendre l'attention particulière attachée par les logiciens à la notion de nombre naturel.

Poursuivons l'idée de Gödel: on peut "arithmétiser", en particulier, $(\overline{L}_n, S_n)$ lui-même. Il est clair que si (L_n, S_n) est consistant, $(\overline{L}_n, S_n)$ l'est aussi, et réciproquement. Dans ce cas, l'énoncé "$0=1$" n'admet pas de preuve dans $(\overline{L}_n, S_n)$. La phrase:

> "quel que soit n, n n'est pas le nombre de Gödel
> d'une preuve de "$0=1$" dans $(\overline{L}_n, S_n)$".

exprime que $(\overline{L}_n, S_n)$ est consistant. Fait remarquable (mais que les explications précédentes rendent plausible), cette phrase peut être traduite par un énoncé dans $\overline{L}_n$, énoncé que nous abrégerons en "Consis(L_n, S_n)".

En se fondant sur les considérations que nous venons d'évoquer et par un procédé "diagonal" que nous avons fait apparaître au numéro 8.4.2, Gödel démontra ceci:

8.4.5 Premier théorème d'incomplétude

Si (L_n, S_n) est consistant, il existe dans $\overline{L}_n$ un énoncé α tel que ni α, ni $(\neg\alpha)$ n'admettent de preuve dans $(\overline{L}_n, S_n)$.

8.4.6 Deuxième théorème d'incomplétude

Si (L_n, S_n) est consistant, il n'existe pas de preuve de "Consis(L_n, S_n)" dans $(\overline{L}_n, S_n)$.

On doit à la vérité de dire que Gödel commença par établir ces propositions dans des hypothèses de consistance plus restrictives. C'est à Rosser que revient le mérite de les avoir étendues au cas où (L_n, S_n) est supposé consistant au sens de la logique du premier ordre.

Nous avons vu que ces théorèmes d'incomplétude heurtent le bon sens. Leur publication eut, à l'époque, un retentissement considérable parmi les logiciens, les philosophes des sciences et toutes sortes d'essayistes. Certains, oubliant l'hypothèse même de ces deux théorèmes, ont cru pouvoir conclure que l'arithmétique et, partant, toutes les mathématiques étaient contradictoires. Ne manquons pas de relever que l'existence, dans un système formel du premier ordre, d'un énoncé sans preuve entraîne justement sa consistance. De surcroît, il est maladroit de s'appuyer sur les théorèmes d'incomplétude de Gödel pour proclamer la faillite de l'arithmétique, ces théorèmes étant eux-mêmes des théorèmes d'arithmétique. D'autres auteurs, plus circonspects, ont vu dans les théorèmes d'incomplétude de Gödel la marque d'une faille, d'une limitation intrinsèque de la logique du premier ordre et même de la logique symbolique en général. Ces interprétations appellent quelques remarques.

8.4.7 Remarque

Rappelons que, dans une théorie du premier ordre, il est possible de prouver tous les énoncés satisfaits dans tous les modèles de cette théorie. Le fait qu'un énoncé α, satisfait dans un modèle donné de cette théorie, n'admette pas de preuve ne témoigne pas de l'insuffisance de la logique du premier ordre. Il montre que le modèle considéré a pour compagnons d'étranges modèles de la même théorie; des modèles qui satisfont $(\neg\alpha)$ et que notre intuition ne nous montre pas spontanément. Historiquement, une situation analogue s'est présentée à propos de l'axiome des parallèles en géométrie euclidienne. Ce que met en évidence ce genre de phénomènes, c'est plutôt une limitation de notre intuition à certains moments et dans certaines circonstances.

Revenons plus particulièrement au deuxième théorème d'incomplétude de Gödel. Supposons (L_n, S_n) consistant, ce que personne ne semble mettre en doute. Essayons d'imaginer ce qui adviendrait si, par extraordinaire, "Consis(L_n, S_n)" admettait une preuve dans (L_n, S_n). En vertu du théorème de complétude de Gödel, par un pur jeu de signes et selon des règles purement formelles, il serait possible d'établir l'***existence*** d'un objet de pensée tel que le nombre naturel. Ce serait accorder à la logique symbolique une puissance surprenante: un véritable pouvoir de création *ex nihilo*. Observons en outre qu'une preuve dans la théorie (L_n, S_n) de sa propre consistance aurait manifestement un caractère autoréférentiel. Il serait difficile de la mettre à l'actif de la logique du premier ordre qui constitue un effort méthodique pour bannir ce genre de "boucle".

8.4.8 L'idée de système formel récursif

La portée des théorèmes d'incomplétude apparaît plus clairement quand on en considère une version généralisée. Revenons au système formel (L_n, S_n) pour les nombres naturels. La description effective de S_n est compliquée par la présence du schéma d'axiomes $(B_p|p=0, 1, 2, ...)$. Toutefois, si on possède une machine M capable de calculer les fonctions récursives générales, on peut la programmer, au moins théoriquement, de façon qu'elle exécute les opérations suivantes:

1) Prendre le numéral n (qui ne soit ni 0, ni 1). Le décomposer en facteurs premiers. Passer à 2).
2) Si n est le nombre de Gödel d'une formule φ de L_n, passer à 3). Sinon, passer à 1) pour le numéral $n+1$.
3) Si φ comporte x comme symbole de variable libre, passer à 4). Sinon, passer à 1) pour le numéral $n+1$.
4) Ecrire l'axiome du schéma $(B_p|p=0, 1, 2, ...)$ correspondans à φ. Puis passer à 1) pour le numéral $n+1$.

La machine M est donc capable de prendre note des axiomes A_1 à A_5 (qui peuvent être codés par un seul nombre de Gödel) et, de proche en proche, de chaque axiome du schéma $(B_p|p=0, 1, 2, ...)$. On peut dire, et on dit effectivement, que (L_n, S_n) est un *système formel récursif*. Il est alors possible d'étendre les théorèmes d'incompétude de Gödel de la manière suivante:

8.4.9 Théorème d'incomplétude généralisé

Soit (L, S) une théorie du premier ordre telle que:

a) (L, S) soit récursive
b) on puisse définir dans (L, S) les fonctions récursives générales.

Alors:

1) (L, S) est incomplète.
2) Il existe en particulier dans L un énoncé "Consis(L, S)" exprimant que (L, S) est consistant et qui n'admet pas de preuve dans (L, S).

8.4.10 Commentaires

Toute théorie du premier ordre ne comportant qu'une collection finie d'axiomes non logiques est évidemment récursive. C'est le cas, par exemple, de la théorie des groupes. Toutefois, celle-ci ne vérifie pas l'hypothèse b) qui est nécessaire pour assurer dans L l'existence de l'énoncé "Consis(L, S)".

Remarquons que, sous réserve de la consistance de (L_n, S_n), il existe des théories du premier ordre non récursives. Considérons en effet un modèle $(\mathbb{N}, J)$ de (L_n, S_n). Soit T l'ensemble de tous les énoncés de L_n satisfaits dans $(\mathbb{N}, J)$. (L_n, T) est évidemment une théorie du premier ordre complète. En vertu du théorème d'incomplétude généralisé elle n'est pas récursive: aucune machine telle que M n'est capable d'écrire de proche en proche les énoncés de T et eux seulement.

Cette observation nous enseigne un fait important. Nous savons qu'il existe des machines matérielles telles que M. Les ordinateurs actuels et tous ceux qui seront construits à partir des mêmes principes théoriques sont de cette espèce. Ils sont capables – en principe – de vérifier si un agrégat fini quelconque de signes typographiques est une formule ou une preuve dans (L_n, S_n). Mais jamais on n'obtiendra d'eux qu'ils énoncent et, *a fortiori,* qu'ils démontrent de proche en proche tous les théorèmes de l'arithmétique. Nous voyons apparaître là une limite du calcul mécanique et de ce qu'on appelle parfois l'"intelligence artificielle". Cette frontière n'est pas d'ordre matériel: elle concerne aussi la machine idéale M que nous avons décrite plus haut. Mais elle n'en est pas moins infranchissable.

On peut aussi dire que le "nombre naturel" est une notion que notre intuition n'a aucune peine à concevoir, mais qui se situe au-delà de toute matérialisation.

Revenons au reproche exprimé à l'endroit de la logique du premier ordre, à savoir une impuissance intrinsèque mise en évidence par les théorèmes d'incomplétude de Gödel. Pour aboutir à une telle condamnation, il faut adopter les prémisses suivantes:

- Il existe un système "naturel" $\mathbb{N}$ des nombres naturels.
- Il est "naturel" d'exiger d'un système formel du premier ordre (L_n, S_n), admettant $\mathbb{N}$ pour modèle, qu'il soit:
  - récursif (c'est-à-dire qu'on puisse effectivement écrire chacun de ses axiomes, comme on peut écrire effectivement chaque numéral)
  - complet.

Le théorème d'incomplétude généralisé nous montre que cette double exigence est formellement contradictoire, donc absurde. Cela jette un nouveau doute sur ce que l'intuition seule est capable de trouver "naturel".

En bref, les théorèmes d'incomplétude mettent en évidence à la fois des bornes de la logique du premier ordre et certaines aberrations de notre intuition. Les premières n'ont rien de surprenant: on ne peut pas attendre d'un système formel qu'il puisse établir sans autre ingrédient l'existence d'un être mathématique si complexe que le nombre naturel. En revanche, notre intuition, qui est indispensable pour appeler à l'existence des objets de pensée, se révèle capable de graves myopies lorsqu'elle se promène sans précaution aux confins du fini et de l'infini. Ne pas le reconnaître conduit à des interprétations téméraires de certains faits de logique formelle.

8.4.11 Dernières remarques sur le théorème d'incomplétude généralisé

Le théorème d'incomplétude généralisé précise et renforce le deuxième théorème d'incomplétude de Gödel. Supposons en effet que (L_n, S_n) soit une théorie. Il est évidemment impossible d'y prouver $\neg$ ("Consis(L_n, S_n)"). Donc (L_n, S_n∪"Consis(L_n, S_n)") est aussi une théorie et il semble qu'on ait réussi à tourner l'obstacle de l'incomplétude. Toutefois, l'adjonction d'un axiome à S_n ne modifie pas son caractère récursif. En vertu du théorème d'incomplétude généralisé, cette nouvelle théorie est à nouveau incomplète et, plus particulièrement, on ne peut pas y prouver sa consistance.

On peut appliquer le théorème d'incomplétude généralisé au système formel (L_e, S_e) de Zermelo – Fraenkel que nous avons décrit pour les ensembles. (L_e, S_e) est manifestement récursif. Il est possible de montrer qu'on peut y définir les numéraux et les fonctions récursives générales (cf. Paul-J. Cohen, chap. I). En particulier:

$$\Phi, \quad \{\Phi\}, \quad \{\Phi, \{\Phi\}\}, \quad \{\Phi, \{\Phi\}, \{\Phi, \{\Phi\}\}\}, \ldots$$

fournit une succession d'ensembles assimilables aux numéraux. Le système formel (L_e, S_e) est donc incomplet et on ne peut pas y prouver sa consistance. Les mathématiciens sont persuadés qu'il est consistant. C'est pourquoi on parle généralement de "théorie des ensembles".

L'incomplétude du système formel (L_e, S_e) a inspiré autant de commentaires audacieux que celle de (L_n, S_n). Une controverse assez vive s'est engagée entre les zélateurs des "mathématiques modernes", apôtres de la "théorie des ensembles" d'une part, et des philosophes traumatisés par les théorèmes d'incomplétude, d'autre part. Elle a pris à l'occasion des proportions réjouissantes. Elle restera certainement un épisode fameux de l'histoire des mathématiques et de son enseignement.

Il est clair que, dans un certain sens, la théorie des ensembles (L_e, S_e) "contient" la théorie des nombres naturels (L_n, S_n). Moyennant l'hypothèse de consistance de (L_e, S_e), il est possible de prouver celle de (L_n, S_n). Le logicien Gentzen a donné une solution particulièrement élégante de ce problème. Il utilise pour cela une numérotation des formules et des preuves dans (L_n, S_n) à la manière de Gödel, mais avec les éléments d'un "grand" modèle de (L_n, S_n). Ce modèle est dénombrable mais il contient une infinité de modèles emboîtés de (L_n, S_n) (cf. corollaire 8.1.13). La clé de la démonstration réside dans l'emploi de preuves par induction transfinie. Il ne faut cependant pas perdre de vue que le théorème de Gentzen est hypothéqué par l'hypothèse de consistance de (L_e, S_e).

Nous avons évoqué le fait que, dans la théorie des ensembles, c'est-à-dire dans le système formel (L_e, S_e) supposé consistant, il est possible de définir les nombres naturels. Ainsi, dans chaque modèle M (non nécessairement ensembliste) de (L_e, S_e), il existe un ensemble $\mathbb{N}(M)$ des nombres naturels qui est un modèle de (L_n, S_n). Mais il n'est pas possible de montrer dans la théorie (L_e, S_e) que, pour deux modèles quelconques M et M' de la théorie des ensembles, $\mathbb{N}(M)$ et $\mathbb{N}(M')$ sont isomorphes. Ce fait est en accord avec le corollaire 7.2.10 du théorème de Löwenheim–Skolem–Tarski.

8.5 DE QUELQUES AUTRES THÉORÈMES D'IMPOSSIBILITÉ

8.5.0 Préambule

Intuitivement, les théorèmes d'incomplétude affirment que, dans certaines conditions, certains problèmes sont insolubles. La connaissance et la classification de tels problèmes présentent un grand intérêt pour la logique et ses applications. Elles constituent un domaine aujourd'hui grand ouvert à la recherche. Nous allons évoquer quelques-uns de ces problèmes, qui sont assez parlants.

8.5.1 De l'impossibilité de formaliser la vérité

En relation avec les théorèmes d'incomplétude de Gödel, Tarski a établi le résultat suivant:

Soit $(\mathbb{N}_1, J_1)$ un modèle de (L_n, S_n) et soit $\alpha_0, \alpha_1, \dots, \alpha_p, \dots$ les énoncés de L_n numérotés comme nous l'avons suggéré au n° 2.3.5, par exemple. Il n'existe aucune formule $\varphi(x)$ de L_n, avec $\mathrm{VL}(\varphi) = \{x\}$, telle que, pour tout numéral p:

$$(\mathbb{N}_1, J_1) \models \varphi(p) \Leftrightarrow (\mathbb{N}_1, J_1) \models \alpha_p.$$

Cette propriété est interprétée comme l'*impossibilité de formaliser la vérité* dans (L_n, S_n).

■ 8.5.2 Sur le problème des mots

Le *problème des mots* joue un rôle important en mathématiques.

Considérons un ensemble comportant exactement deux éléments, $\{x, y\}$. Posons:

1) $x^0 \equiv 1$ *et* $x^1 \equiv x$
2) $y^0 \equiv 1$ *et* $y^1 \equiv y$
3) pour tous r et s dans $\mathbb{Z}$, $y^r x^s \equiv x^{r+s}$
4) pour tous r et s dans $\mathbb{Z}$, $y^r y^s \equiv y^{r+s}$.

Considérons maintenant l'ensemble $M(x, y)$ des "mots"

$$x^{\alpha}y^{\beta}x^{\alpha'}y^{\beta'} \quad \dots \quad x^{\alpha(i)}y^{\beta(i)}$$

avec $i \in \mathbb{N}$, α, β, α', β', ... , $\alpha^{(i)}$, $\beta^{(i)} \in \mathbb{Z}$, où l'on regarde comme équivalents deux mots tels qu'on puisse passer de l'un à l'autre en appliquant un mombre fini de fois les relations 1), 2), 3) et 4). Par exemple:

$$1x \equiv x^0x^1 \equiv x$$
$$x^2y^5x^0y^{-2} \equiv x^2y^5 1 y^{-2} \equiv x^2y^5y^0y^{-2} \equiv x^2y^5y^{-2} \equiv x^2y^3$$

Chaque élément de $M(x, y)$ est représentable par un mot, et cela de plusieurs manières. Munissons $M(x, y)$ de la "multiplication" naturelle consistant à juxtaposer les mots représentatifs. Par exemple:

$$x^2yxy^0 \cdot x^0y^{-1}xy \equiv x^2yxy^0x^0y^{-1}xy \equiv x^2yxy^{-1}xy$$

Nous obtenons de la sorte un groupe dont l'élément neutre est représentable par 1. C'est le *groupe libre* engendré par $\{x, y\}$, noté $L(x, y)$.

A partir de $L(x, y)$, construisons un autre exemple de groupe. Considérons l'élément r de $M(x, y)$ représenté par le mot $xyx^{-1}y^{-1}$. Convenons de remplacer r par 1, ou réciproquement, dans tous les mots représentant les éléments de $M(x, y)$. Par exemple:

$$yx \equiv ryx \equiv xyx^{-1}y^{-1}yx \equiv xyx^{-1}x \equiv xy$$
$$yx^{-1} \equiv x^{-1}xyx^{-1}y^{-1}y \equiv x^{-1}ry \equiv x^{-1}y, \text{ etc.}$$

Il devient évident que $r \equiv 1$ équivaut à $xy \equiv yx$. Introduisons la même multiplication que précédemment. Nous obtenons un groupe engendré à nouveau par les mots x et y; mais ceux-ci sont soumis à une et une seule condition: ils doivent commuter. C'est le *groupe abélien libre* engendré par $\{x, y\}$. On le note $AL(x, y)$, et on écrit:

$$AL(x, y) = < x, y \,;\, xyx^{-1}y^{-1} >$$

On dit alors que $AL(x, y)$ est *présenté par générateurs et relations*. x et y sont les générateurs; $xyx^{-1}y^{-1}$ est appelé (par abus de langage) une relation. (La relation évoquée est en réalité $xyx^{-1}y^{-1} \equiv 1$.)

Un peu plus généralement, on peut considérer un groupe G présenté par:

$$G = < x, y; r_1, r_2, \dots, r_p >$$

où r_1, r_2, ... , r_p sont des mots de $M(x, y)$. G est alors le quotient de $L(x, y)$ par le sous-groupe normal de $L(x, y)$ engendré par (les éléments représentés par) les mots r_1, r_2, ... , r_p. Par exemple:

$$L(x, y) = < x, y; >$$

Pour $L(x, y)$, le *problème des mots* peut s'énoncer ainsi: un mot s de $L(x, y)$ représente-t-il l'élément neutre de G? Ce problème n'admet pas de solution générale en ce sens qu'il n'existe pas de procédure *effective* permettant, dans tous les cas, de décider si s représente ou non l'élément neutre de G. Le caractère "effectif" de la procédure considérée est traduit par une collection finie de consignes de calculs exprimables par des fonctions récursives générales. L'insolubilité du problème des mots a été établie par P.S. Novikov en 1955.

Bien d'autres problèmes de ce genre se sont révélés insolubles d'une manière générale. A titre d'exemples, mentionnons-en deux qui sont faciles à énoncer:

- un groupe présenté par générateurs et relations est-il abélien?
- deux groupes présentés par générateurs et relations sont-ils isomorphes?

De tels problèmes apparaissent de manière naturelle en géométrie, particulièrement en topologie algébrique. Le fait qu'ils n'admettent pas de solution générale effective revêt une grande importance en mathématiques. ■

8.5.3 Le dixième problème de Hilbert

Enoncé lors du Congrès des Mathématiciens de 1900, ce problème propose la recherche d'une procédure "effective" permettant de décider si une équation de la forme:

$$P(x_1, x_2, \ldots, x_n)=0,$$

où P est un polynôme à coefficients entiers rationnels, admet une solution en nombres entiers rationnels. En 1970, Matijacevič parvint à montrer qu'une telle procédure n'existe pas.

8.5.4 Autres problèmes

D'autres questions d'arithmétique, de géométrie (coloriages de graphes, présentations de variétés topologiques, par exemple) et d'analyse ont conduit à des problèmes sans solution générale. Il est intéressant de noter que l'étude de ces faits requiert des outils forgés initialement pour les besoins de la logique.

8.6 LE PROGRAMME ET LA THÈSE DE HILBERT

8.6.1 Préambule

La logique du premier ordre jette un éclairage révélateur sur quelques-unes des notions fondamentales des mathématiques telles que le fini, l'infini, les nombres naturels, les ensembles. Il serait intéressant d'examiner de plus près les conceptions et les controverses qui ont pris naissance à propos des fondements des mathématiques. C'est là un domaine important de l'histoire et de la philosophie des mathématiques. Il dépasse malheureusement les limites de cet exposé. Cependant, nous évoquerons brièvement quelques-unes des vues d'un mathématicien qui a particulièrement contribué à faire évoluer ces questions.

David Hilbert (1862–1943) avait la passion de réduire la diversité des faits mathématiques à un petit nombre d'éléments et de processus de base. Son traité sur les fondements de la géométrie est déjà très révélateur à ce sujet. Ses travaux sur les idéaux de polynômes répondaient à son souci de ramener tous les théorèmes de géométrie euclidienne à la connaissance d'un nombre fini d'invariants. Les espaces fonctionnels qui portent son nom témoignent de sa volonté d'étendre à l'analyse la terminologie et les méthodes de la géométrie élémentaire.

Mais Hilbert amorça un projet plus ambitieux encore qu'on évoque sous le nom de *programme de Hilbert*. Pour plus de clarté, nous allons présenter cela en deux étapes: d'abord la thèse de Hilbert, puis le programme de Hilbert proprement dit.

8.6.2 La thèse de Hilbert

Hilbert mit à profit les travaux des logiciens de son temps et les acquisitions de la théorie des ensembles. Il dégagea un ensemble de règles qui permettent de décrire les raisonnements de la logique du premier ordre. Nous l'avons présenté sous le nom de système d'inférence de Hilbert (n° 6.1.0). La "*thèse de Hilbert*", qui traduit la conviction à laquelle celui-ci parvint alors, peut s'énoncer à l'aide des deux assertions suivantes:

TH 1: Toutes les théories mathématiques classiques peuvent s'exprimer au moyen de systèmes formels du premier ordre.

TH 2: Dans toute théorie mathématique, chaque théorème admet une preuve formelle selon les règles du système d'inférence de Hilbert.

Le contenu de TH 1 dépend entièrement du sens attribué au qualificatif "classique". Il résulte des recherches mêmes de Hilbert que les mathématiques qu'il pratiquait vérifiaient l'assertion TH 1. Actuellement, tout se passe comme si on considérait comme classiques les mathématiques qui, en fin de compte, peuvent s'exprimer au moyen de systèmes formels du premier ordre. TH 1 serait alors satisfaite par définition. Il convient d'ajouter qu'il existe des mathématiques non classiques. Elles reposent sur des axiomes logiques moins restrictifs. La plupart des mathématiciens les considèrent comme des monstres inélégants!

8.6.3 De la rigueur en mathématiques

L'assertion TH 2 a reçu un contenu bien déterminé et une démonstration éclatante avec le théorème de complétude de Gödel.

En relation avec la thèse de Hilbert, nous pouvons mettre en évidence deux faits importants. D'abord, il existe en mathématiques classiques un critère de validité absolue pour tout théorème au sein d'une théorie: l'existence d'une preuve formelle au sens de Hilbert. Autrement dit, le progrès mathématique consiste à découvrir et démontrer des théorèmes inconnus jusque là. Il ne saurait résider dans un accroissement de la rigueur. Il est vrai que la preuve formelle du moindre théorème comporte des centaines, voire des milliers de pas. Personne n'aurait le courage de la lire entièrement. Une véritable démonstration mathématique consiste à mettre en relief les articulations principales de la preuve formelle. Elle est donc nécessairement lacunaire. L'essentiel est que les lacunes ne soient pas formellement infranchissables. L'art du mathématicien se manifeste dans l'aptitude à choisir les étapes décisives d'une preuve et à suggérer clairement les chaînons de preuve qu'il a omis.

8.6.4 Des nombres naturels non standard

Le deuxième fait important auquel nous faisons allusion plus haut concerne l'apport de la logique du premier ordre aux mathématiques classiques. Pour prendre un exemple concret, considérons un modèle $(\mathbb{N}_1, J_1)$ des entiers naturels satisfaisant le système formel (L_n, S_n) (voir nº 8.1.3). Qualifions de “standard” les éléments de $\mathbb{N}_1$. Nous savons que rien ne nous empêche d'évoquer un modèle $(\mathbb{N}_2, J_2)$ de (L_n, S_n), tel que $\mathbb{N}_2$ inclue $\mathbb{N}_1$ et qu'il comporte des éléments plus grands que tous ceux de $\mathbb{N}_2$ (cf. remarque 8.1.12). Les éléments de $\mathbb{N}_2 - \mathbb{N}_1$ sont alors des nombres naturels *non standard.* L'existence de deux modèles emboîtés de (L_n, S_n) est un phénomène mathématique intéressant et utile, que l'intuition seule n'aurait pas suggéré.

8.6.5 De l'analyse non standard

Une telle situation a été effectivement exploitée dans le cas des nombres réels. Passons sur quelques points techniques d'intérêt secondaire pour notre propos. Soit (L_r, S_r) un système formel du premier ordre pour les nombres réels. On peut considérer un modèle $(\mathbb{R}_1, J_1)$ de (L_r, S_r) baptisé “standard” et un second modèle $(\mathbb{R}_2, J_2)$, dit “*non standard*”, tel que:

- $\mathbb{R}_1 \subset \mathbb{R}_2$, $\mathbb{R}_1 \neq \mathbb{R}_2$
- toutes les “opérations” de $\mathbb{R}_2$ effectuées sur des éléments de $\mathbb{R}_1$ fournissent des éléments de $\mathbb{R}_1$, $(\mathbb{R}_1, J_1)$ étant un sous-modèle de $(\mathbb{R}_2, J_2)$
- il existe dans $\mathbb{R}_2$ des éléments strictement plus grands que tous les éléments de $\mathbb{R}_1$.

Le corollaire 8.1.10 et la remarque 8.1.12 nous assurent que la chose est possible. Il est facile de vérifier que si $\alpha \in \mathbb{R}_2 - \mathbb{R}_1$ est “infiniment grand” par comparaison avec les éléments de $\mathbb{R}_1$, α^{-1} est un élément strictement positif de $\mathbb{R}_2$ “infiniment petit”: il est inférieur à tout élément strictement positif de $\mathbb{R}_1$. L'étude du triple

($\mathbb{R}_2$, $\mathbb{R}_1$; J_2) constitue l'*analyse non standard*. Elle permet de traiter d'une manière formellement correcte des "infiniment petits" introduits par Leibniz. Divers auteurs (Robinson, Keisler, ...) ont montré que ce genre d'objet mathématique permet d'alléger la preuve de certains théorèmes classiques d'analyse. D'autres mathématiciens (Reeb, ...) s'attachent à résoudre par ce moyen des questions d'analyse standard difficiles d'accès par les moyens habituels. L'amusant de l'affaire, c'est que certains mathématiciens peu au courant de la logique du premier ordre s'insurgent contre ces méthodes avec une violence qui pourrait faire croire qu'on les incite à la débauche.

8.6.3 Le programme de Hilbert

La thèse de Hilbert n'a d'intérêt que pour autant que les théories mathématiques envisagées soient des "théories" au sens logique, autrement dit qu'elles soient non contradictoires.

La consistance d'un système formel du premier ordre peut être établie par deux voies. La première consiste à en décrire un modèle ensembliste. Historiquement, on a montré que les géométries non euclidiennes de Riemann et de Lobatchevski constituaient des théories en en donnant des modèles dans la géométrie euclidienne plane. Evidemment la méthode n'est pas tout à fait satisfaisante dans ce cas, puisqu'il faut d'abord établir la consistance de la géométrie euclidienne. Le cas des groupes, que nous avons examiné à l'exemple 2.2.24, est facile à traiter puisqu'il nous a suffi de donner un modèle fini comportant trois éléments (un modèle à un élément conviendrait aussi!). Cela peut se réaliser matériellement. Les choses se gâtent en revanche pour les nombres naturels ou les nombres réels. Là, seuls des modèles infinis sont susceptibles d'intervenir et nous sommes incapables de les donner "effectivement". D'autre part, l'idée de modèle ensembliste impose la notion d'ensemble et nous sommes contraints d'attaquer la consistance de la "théorie des ensembles", qui, elle non plus, ne peut être établie par la donnée effective d'un modèle.

Reste donc la deuxième voie qui consiste à s'assurer par l'étude directe du système formel qu'il comporte des énoncés sans preuve. C'est celle que signala Hilbert pour parachever son programme. Il proposa d'établir la non-contradiction de systèmes formels du premier ordre pour les nombres naturels, les ensembles et les nombres réels. Mais, pour ne pas retomber dans les difficultés précédentes, il fallait exiger que les procédures utilisées soient "finitistes". D'une part, elles doivent admettre une description effective, sous forme d'une nombre fini de consignes écrites; de l'autre, elles doivent conduire à une conclusion par une suite d'opérations effectivement exécutées. Nous reconnaissons au passage les exigences que nous avons évoquées à propos des numéraux et des fonctions récursives.

Ce projet constituait la clé de voûte du *programme de Hilbert*, qui comportait en outre des recherches sur la complétude des systèmes formels considérés, sur l'indépendance de leurs axiomes et des questions de "décidabilité".

Les théorèmes d'incomplétude de Gödel ont mis fin à tout espoir d'accomplir le programme de Hilbert. Nous avons essayé de montrer qu'ils sont loin d'entraîner une catastrophe pour les mathématiques, même hilbertiennes. Ils nous contraignent cependant à admettre que la pratique des mathématiques requiert la conjugaison indissociable de la logique formelle et de l'intuition.

CHAPITRE 9

Aperçus sur d'autres logiques formelles

9.0 INTRODUCTION

9.0.0 La finitude en logique du premier ordre

La logique formelle ne constitue pas toute la logique et la logique (formelle) du premier ordre ne constitue pas toute la logique formelle. Quelques exemples de logiques formelles dont les exigences s'écartent de celle du premier ordre permettent de mieux sentir ce qui fait le propre de celle-ci. Mais il existe évidemment d'autres raisons de créer des logiques formelles nouvelles. Nous allons en donner une.

Nous avons constaté qu'il est difficile d'introduire la notion naïve de finitude en logique du premier ordre (cf. remarque 5.5.5). Pourtant la finitude joue un rôle essentiel partout, en mathématiques et ailleurs. Il serait commode d'exprimer ***simplement*** que tel objet est fini sous un certain rapport.

Relevons qu'on peut introduire la finitude formelle dans la logique du premier ordre. En effet, elle se "mesure" à l'aide des nombres naturels et nous connaissons un système formel du premier ordre (L_n, S_n) qui leur est adapté. A titre d'exemple, montrons comment on peut présenter les *groupes sans torsion* au sens large (cf. exemple 5.5.4).

9.0.1 Exemple

Soit G un groupe noté multiplicativement et soit e son élément neutre. On note a^p le produit dans G de p facteurs égaux à l'élément a de G:

$$a^p = \underbrace{a \cdot (a \cdot (a \cdot (\ldots \cdot (a \cdot a))\ldots)}_{p \text{ facteurs}}.$$

En particulier, $a^0 = e$ et $a^1 = a$. G est un *groupe sans torsion* au sens large si, pour tout élément a de G différent de e et pour tout nombre naturel non nul p, a^p est différent de e. Si, en outre, G ne se réduit pas à $\{e\}$, il est sans torsion au sens étroit.

Pour décrire cela formellement, prenons un langage L du premier ordre comportant les symboles propres suivants:

- constantes: 0, 1, e
- fonctions binaires: $+$, $\cdot$, $*$, f
- relations unaires: N, Γ

$0, 1, +, \cdot$ sont les symboles propres au langage L_n. e et $*$ sont les symboles propres au langage employé pour les groupes (cf. exemple 5.5.4); la loi de composition interne est notée $*$ pour éviter toute confusion avec la multiplication des nombres naturels. Intuitivement, $N(x)$ est interprété comme: "x est un nombre naturel", $\Gamma(y)$ s'interprète comme: "y est un élément d'un groupe". $f(x, y)$ est une notation pour y^x.

Comme système d'axiomes S dans L, prenons:

- un axiome général: $\forall x N(x) \vee \Gamma(x)$
- les axiomes de S_n adaptés au langage L; les axiomes $A_1, A_2, \ldots, A_5$ sont remplacés par cinq axiomes $A'_1, A'_2, \ldots, A'_5$.
  Par exemple:
  $A'_5 \equiv \forall x \forall y((N(x) \wedge N(y)) \rightarrow ((x+1=y+1) \rightarrow (x=y))$
  Le schéma d'axiomes $(B_p | p=0, 1, \ldots)$ engendre:
  $$B'_p \equiv \forall v_1 \ldots \forall v_{m_p}((\varphi_p(0, v_1, \ldots, v_{m_p}) \wedge (\forall z N(z) \rightarrow (\varphi_p(z, v_1, \ldots, v_{m_p}) \rightarrow \varphi_p(z+1, v_1, \ldots, v_{m_p})))) \rightarrow (\forall x N(x) \rightarrow \varphi_p(x, v_1, \ldots, v_{m_p}))),$$
  avec $p=0, 1, \ldots$, et $\varphi_p \in \mathrm{For}(L)$.
- les axiomes des groupes (cf. exemple 5.5.4) transcrits dans le langage L:
  $\varphi'_1 \equiv \forall x \forall y \forall z(\Gamma(x) \wedge \Gamma(y) \wedge \Gamma(z)) \rightarrow x*(y*z) = (x*y)*z$
  $\varphi'_2 \equiv \forall x \Gamma(x) \rightarrow ((x*e=x) \wedge (e*x=x))$
  $\varphi'_2 \equiv \forall x \Gamma(x) \rightarrow (\exists y \Gamma(y) \wedge (x*y=e) \wedge (y*x=e))$
- des axiomes pour f:
  $\forall x \forall y(N(x) \wedge \Gamma(y)) \rightarrow \Gamma(f(x, y))$
  $\forall y \Gamma(y) \rightarrow f(0, y) = e$
  $\forall x \forall y(N(x) \wedge \Gamma(y)) \rightarrow (f(x+1, \mathrm{y}) = y*f(x, y))$
- un axiome (ST) exprimant que "le groupe est sans torsion":
  $(ST) \equiv \forall y(\Gamma(y) \wedge (\neg(y=e)) \rightarrow \neg \exists x(N(x) \wedge (f(x+1, y)=e))$

Admettons que (L_n, S_n) est une théorie. Soit $(\mathbb{N}, J)$ un modèle de (L_n, S_n). On peut construire un modèle $(\mathbb{N}, J')$ de (L, S) en posant:

- $J'(0) = J(0) = 0 \in \mathbb{N}$
  $J'(1) = J(1) = 1 \in \mathbb{N}$
  $J'(e) = 0$
- pour toute spécialisation s de J':
  $\Gamma(x) \Rightarrow s(x) = 0 \qquad x \in \mathrm{Var}$
  $s(t_1 + t_2) = s(t_1) + s(t_2) \qquad t_1, t_2 \in \mathrm{Ter}(L)$
  $s(t_1 \cdot t_2) = s(t_1) \cdot s(t_2)$
  $s(t_1 * t_2) = 0$
  $s(f(t_1, t_2)) = 0.$

Le groupe proprement dit se réduit à $\{0\}$.

La vérification que $(\mathbb{N}, J')$ est un modèle de (L, S) est presque banale.

Cet exemple nous montre plusieurs choses:

- Il est possible d'incorporer la théorie des nombres naturels à la théorie des groupes et, plus généralement, à toute théorie du premier ordre.
- Il est possible d'introduire la notion de finitude dans toute théorie du premier ordre, contrairement à ce que semblait faire croire l'exemple 5.5.4.
- Il serait possible, d'une manière analogue, d'incorporer la théorie des ensembles à toute théorie du premier ordre. De tels exemples militent en faveur de la thèse de Hilbert.
- La théorie (L, S), à laquelle a été incorporée (L_n, S_n), devient au moins aussi complexe que la théorie des nombres naturels. En particulier, elle hérite de toutes les propriétés délicates décrites par le théorème général d'incomplétude.
- Dans chaque modèle de (L, S) apparaît une notion de finitude spécifique liée au choix du modèle de (L_n, S_n) qui a été fait. On peut donc imaginer plusieurs classes de groupes sans torsion correspondant à des types de finitude distincts. Toutefois les théorèmes et les preuves sont les mêmes dans tous les cas.

Cette dernière remarque peut gêner le mathématicien praticien. Celui-ci n'emploie que la finitude naïve exprimée par les numéraux. Il répugne à imaginer d'autres types de finitude. Pour répondre à son attente, on peut introduire d'autres logiques, dont nous allons donner deux exemples.

9.1 COMMENT INTRODUIRE SIMPLEMENT LA FINITUDE DANS LES RAISONNEMENTS?

9.1.0 La $\mathbb{N}$-logique

L'idée de départ est de simplifier l'exemple 9.0.1 de deux manières:

- en n'écrivant pas les axiomes S_n
- en ne faisant intervenir dans les interprétations qu'un modèle unique $(\mathbb{N}, J)$ de (L_n, S_n), choisi une fois pour toutes.

Reprenons cela en détail. Le langage Λ utilisé comporte:

- les symboles logiques habituels: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $=$, $\forall$, $\exists$
- les symboles de constantes, de fonctions et de variables du langage L_n convenant aux nombres naturels: 0, 1, $+$, $\cdot$, x, x', x'', ...
- de nouveaux symboles de constantes, de variables et de relations figurés – par exemple – par des lettres grecques:

$$\underbrace{\gamma, \gamma' \ldots,}_{\text{constantes}} \; \underbrace{\xi, \xi', \ldots,}_{\text{variables}} \; \underbrace{\overset{\text{relation } (p_i,\, q_i)\text{-aire}}{\Omega^i_{p_i,\, q_i}}, \ldots}_{\text{relations}}$$

- les symboles ordinaires de ponctuation: , ( )

Pour plus de simplicité, nous n'introduisons pas de nouveaux symboles de fonctions; nous savons que de tels symboles peuvent être éliminés au profit des symboles de relations.

Dans le langage Λ, les *termes* sont, d'une part, ceux de $\mathrm{Ter}(L_n)$, d'autre part, les symboles grecs de constantes et de variables. Les formules atomiques de Λ sont de la forme:

- $t_1 = t_2 \quad , \quad t_1, t_2 \in \mathrm{Ter}(\Lambda)$
- $\Omega^i_{p_i, q_i}(t_1, t_2, \ldots, t_{p_i} \quad ; \quad \tau_1, \tau_2, \ldots, \tau_{q_i})$

où $t_1, t_2, \ldots, t_{p_i} \in \mathrm{Ter}(L_n)$ et $\tau_1, \tau_1, \ldots, \tau_{q_i}$ sont des symboles grecs de constantes ou de variables. i est un numéro d'ordre de $\Omega^i_{p_i, q_i}$ dans la liste des symboles de relations de Λ.

Les formules de Λ sont construites à partir des formules atomiques de Λ selon les mêmes règles qu'en logique du premier ordre. En particulier, si φ est une formule de Λ (on écrit cela $\varphi \in \mathrm{For}(\Lambda)$):

$$(\forall x\varphi) \quad , \quad (\exists x\varphi) \quad , \quad (\forall \xi\varphi) \quad , \quad (\exists \xi\varphi)$$

sont aussi des formules de Λ.

On constate que Λ n'est pas un langage du premier ordre. Il fait intervenir simultanément plusieurs (ici deux) sortes de symboles de constantes et de variables ainsi que des symboles de relations portant sur des termes de types différents. On peut le qualifier de langage *polytypique* ("many-sorted language" en anglais).

Les notions de variable libre, d'énoncé, les axiomes logiques et les règles d'inférence sont les mêmes qu'en logique du premier ordre. Voilà pour l'aspect formel.

Passons au plan sémantique. On commence par se donner un modèle $(\mathbb{N}, J_0)$ de (L_n, S_n) ***une fois pour toutes*** (moyennant l'hypothèse que de tels modèles existent, évidemment). Une *Λ-structure* s'obtient en se donnant un ensemble E, *a priori* quelconque et une interprétation J telle que:

$J(0) = J_0(0)$	$J(1) = J_0(1)$	
$J(+) = J_0(+)$	$J(\cdot) = J_0(\cdot)$	$(:\mathbb{N} \times \mathbb{N} \to \mathbb{N})$
$J(\gamma) \in E$	pour toute constante grecque γ	
$J(\Omega^i_{p_i, q_i}) \subset \mathbb{N}^{p_i} \times E^{q_i}$	pour tout symbole de relation dans Λ.	

Toute *spécialisation* s de J est une application définie sur l'ensemble des termes de Λ et telle que:

$s(x) \in \mathbb{N}$	x étant un symbole de variable latin
$s(\xi) \in E$	ξ étant un symbole de variable grec.

Les autres définitions: image d'un terme t par une spécialisation s de J, satisfaction d'une formule $\varphi \in \mathrm{For}(\Lambda)$ par cette spécialisation, modèle d'un ensemble S d'énoncés de Λ, se font comme en logique du premier ordre. Elles se notent de la même manière.

9.1.1 Exemple

Ce qui précède caractérise la $\mathbb{N}$-logique. Elle se prête bien à la théorie des groupes, par exemple. Pour cela on introduit un symbole de relation (0, 3)-aire, $\Omega_{0,3}$. Dans toute spécialisation s, τ_1, τ_2, τ_3 étant trois termes "grecs", $\Omega_{0,3}(\tau_1, \tau_2, \tau_3)$ est interprété comme: "$s(\tau_3)$ est le composé de $s(\tau_1)$ et $s(\tau_2)$". Les axiomes non logiques:

$$\forall\xi\forall\xi'\exists\xi''\Omega_{0,3}(\xi, \xi', \xi'')$$
$$\forall\xi\forall\xi'\forall\xi''\forall\xi'''(\Omega_{0,3}(\xi, \xi', \xi'') \wedge \Omega_{0,3}(\xi, \xi', \xi'''))\to(\xi''=\xi''')$$

expriment que $\Omega_{0,3}$ détermine une loi de composition interne. Si γ est un symbole de constante,

$$\forall\xi(\Omega_{0,3}(\xi, \gamma, \xi) \wedge \Omega_{0,3}(\gamma, \xi, \xi))$$

exprime que γ est neutre pour la loi de composition considérée. A titre d'exercice facile le lecteur pourra déterminer les axiomes qui traduisent que la loi est celle d'un groupe.

Pour exprimer qu'on a affaire à un groupe sans torsion au sens large (cf. exemple 5.5.4), on peut introduire un symbole de relation $\Omega'_{1,2}$ satisfaisant les axiomes suivants:

- $\forall x\forall\xi\exists\xi'(\Omega'_{1,2}(x, \xi, \xi'))$
- $\forall x\forall\xi\forall\xi'\forall\xi''(\Omega'_{1,2}(x, \xi, \xi') \wedge \Omega'_{1,2}(x, \xi, \xi''))\to(\xi'=\xi'')$
- $\forall x\forall\xi\forall\xi'\forall\xi''(\Omega'_{1,2}(x, \xi, \xi') \wedge \Omega'_{1,2}(x+1, \xi, \xi''))\to\Omega_{0,3}(\xi, \xi', \xi'')$
- $\forall\xi\,\Omega'_{1,2}(0, \xi, \gamma)$

Les deux premiers axiomes expriment que $\Omega'_{1,2}(x, \xi, \xi')$ détermine ξ' en fonction de x et ξ. Les deux derniers entraînent que, pour toute spécialisation s telle que $s(x)$ soit un numéral, $\Omega'_{1,2}(x, \xi, \xi')$ est interprété comme:

$$s(\xi')=s(\xi)^{s(x)}.$$

Alors l'axiome:

$$\forall x\forall\xi(\neg(\xi=\gamma))\to(\neg(\Omega'_{1,2}(x+1, \xi, \gamma)))$$

exprime que le groupe est sans torsion.

Dans la pratique, on emploie des notations plus commodes. A la place de $\Omega_{0,3}(\xi, \xi', \xi'')$ et de $\Omega'_{1,2}(x, \xi, \xi')$, on met respectivement $\xi''=\xi*\xi'$ et $\xi'=\xi^x$. D'autre part, on admet tacitement que tous les éléments de $\mathbb{N}$ sont des numéraux. On désigne généralement par ω le cardinal de l'"ensemble" des numéraux. Par suite, la $\mathbb{N}$-logique est aussi désignée sous le nom de *ω-logique*.

9.1.2 Remarque

En $\mathbb{N}$-logique, il n'existe pas d'équivalent du théorème de compacité pour la logique du premier ordre. Pour le voir, il suffit de donner un contre-exemple particulier. Soit $(\mathbb{N}, J_0)$ un modèle de (L_n, S_n) considéré comme standard. Considérons alors un langage Λ_1 de $\mathbb{N}$-logique comportant en tout un symbole grec propre: un symbole de constante γ. Prenons l'ensemble d'énoncés, $S=\{A\}\cup\{B_i|_{i\in\mathbb{N}}\}$, où:

$$A \equiv \forall\xi(\xi=\gamma)$$
$$B_i \equiv \exists x(\gamma=i+x),\ i\in\mathbb{N}$$

Tout modèle de $(\Lambda_1, \{A\})$ est de la forme $\mathbb{N}\cup\{q\}$ où q est un élément quelconque pouvant éventuellement appartenir à $\mathbb{N}$. Dès lors (Λ_1, S) n'admet pas de modèle. Car si $(\mathbb{N}\cup\{q\}, J)$ est un modèle de $(\Lambda_1, \{A\})$:

- ou bien $J(\gamma)=q\notin\mathbb{N}$: aucun des axiomes B_i n'est satisfait
- ou bien $J(\gamma)=q'\in\mathbb{N}$: les axiomes B_j où $j>q'$ ne sont pas satisfaits.

En revanche, toute partie finie de S admet un modèle. En effet, soit $i_1, i_2, \ldots, i_n$ un ensemble fini d'indices distincts dans $\mathbb{N}$, et soit m leur maximum. Il suffit de poser $J(\gamma)=m$ pour obtenir un modèle de $\{A, B_{i_1}, \ldots, B_{i_n}\}$ et, *a fortiori*, de $\{B_{i_1}, \ldots, B_{i_n}\}$.

L'absence en $\mathbb{N}$-logique d'un théorème de compacité entraîne celle d'un théorème de complétude. En effet, bien que (Λ_1, S) n'ait pas de modèle, il est faux qu'on puisse y prouver un énoncé de la forme $(\alpha \wedge (\neg\alpha))$. Une telle preuve aurait une longueur finie et elle ferait intervenir un nombre fini d'axiomes de S. Or ces axiomes admettraient un modèle qui ne satisfait pas $(\alpha \wedge (\neg\alpha))$. Ainsi (Λ_1, S) est $\mathbb{N}$-logiquement consistant tout en n'admettant aucun modèle. On peut considérer que la $\mathbb{N}$-logique est plus forte que la logique du premier ordre puisqu'on peut y prouver des théorèmes qui n'ont aucune chance d'être satisfaits dans aucun modèle.

■ 9.1.3 Remarque

Notons en passant qu'on pourrait construire d'une manière analogue une logique à partir d'un modèle $\mathbb{R}$ choisi une fois pour toutes pour les nombres réels. Cette $\mathbb{R}$-logique conviendrait à l'étude de toutes les théories où les nombres réels jouent un rôle: celle des espaces vectoriels réels, l'analyse réelle, la théorie des espaces métriques, par exemple. ■

■ 9.1.4 La logique faible du second ordre

Pour en esquisser la description, nous devons d'abord évoquer une notion ensembliste. Nous dirons qu'un ensemble A est *héréditairement fini* lorsque toute partie finie de A est un élément de A.

Soit E un ensemble quelconque. Désignons par $\mathscr{P}F(E)$ l'ensemble des parties finies de E. Alors $\mathscr{P}F(E)$ est contenu dans un ensemble héréditairement fini. On peut le voir en formant successivement:

$$
\begin{aligned}
HF_0(E) &:= \emptyset \\
HF_1(E) &:= \mathscr{P}F(E) \\
&\vdots \\
HF_{k+1}(E) &:= \mathscr{P}F(E \cup HF_k(E)) \\
&\vdots \\
HF(E) &:= \bigcup_{k=0}^{\infty} HF_k(E)
\end{aligned}
$$

$HF(E)$ contient évidemment $\mathscr{P}F(E)$. Montrons qu'il est héréditairement fini.

Il est clair que, quel que soit $k : HF_0(E) \subset HF_k(E)$. Procédons par récurrence en admettant que pour un certain i,

$$HF_i(E) \subset HF_k(E) \text{ quel que soit } k \geqq i.$$

Supposons $q \geqq i+1$

$$HF_{i+1}(E) = \mathscr{P}F(E \cup HF_i(E)) \subset \mathscr{P}F(E \cup HF_{q-1}(E)) = HF_q(E).$$

Donc, quels que soient i et k, $i \leqslant k \Rightarrow HF_i(E) \subset HF_k(E)$. (9.0)

Prenons maintenant une partie finie (qu'on peut supposer non vide) de $HF(E)$, soit $\{a_1, \dots, a_n\} \subset HF(E)$. Pour chaque $j = 1, 2, \dots, n$, il existe un indice q_j, tel que $a_j \in HF_{q_j}(E)$. Si $q = max(q_1, \dots, q_n)$, $\{a_1, \dots, a_n\} \subset HF_q(E)$, d'après (9.0). Donc $\{a_1, \dots, a_n\} \in HF_{q+1}(E) \subset HF(E)$. Cela établit que $HF(E)$ est héréditairement fini.

La construction nous montre que $HF(E)$ est le plus petit ensemble héréditairement fini contenant $\mathscr{P}F(E)$. On peut l'appeler la *clôture héréditairement finie de* $\mathscr{P}F(E)$.

Manifestement $E \subset F \Rightarrow HF(E) \subset HF(F)$. Donc le plus petit ensemble héréditairement fini est la clôture héréditairement finie de l'ensemble $\{\emptyset\}$ des parties finies de l'ensemble vide $\emptyset$: en effet, si F est héréditairement fini, $HF(F) \subset F$, donc $HF(\emptyset) \subset HF(F) \subset F$. On peut écrire:

$$HF(\emptyset) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{\{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \dots\}.$$

Cette notion ensembliste étant introduite, considérons un langage du premier ordre L. Formons un nouveau langage L^* en y adjoignant des symboles "grecs": une collection de variables $\xi, \xi', \xi'', \dots$ et un symbole de relation binaire $\in$. Les *termes de* L^* sont:

- les termes de L
- les symboles $\xi, \xi', \xi'', \dots$

Les *formules atomiques de* L^* sont:

- les formules atomiques de L
- les formules du type $t_1 \in t_2$ où t_1 et t_2 sont des termes de L^*, t_2 étant plus particulièrement l'un des symboles $\xi, \xi', \xi'', \dots$

Les *formules de* L^* sont formées à partir des formules atomiques de L^* suivant les règles habituelles de la logique du premier ordre. En particulier, si $\varphi \in \mathrm{For}(L^*)$, $(\forall x \varphi)$ et $(\forall \xi \varphi)$ sont aussi des formules de L^*. Mais il est clair que L^* n'est pas un langage du premier ordre.

Une L^*-*structure* est un quadruple $(E, J; HF(E), \Omega)$,
où:

- (E, J) est une L-structure
- Ω est l'ensemble des couples (a, b) tels que a appartient à $E \cup HF(E)$, b appartient à $HF(E)$ et a appartient à b.

En outre:

- toute spécialisation s de J envoie les symboles de variables latins $x, x', x'', \ldots$ de L dans E et les symboles de variables grecs dans $HF(E)$
- toute formule atomique de la forme $t_1 \in t_2$ est interprétée selon s par: $(s(t_1), s(t_2))$ appartient à Ω
- pour le surplus, la satisfaction des formules de L^* dans la spécialisation s se définit comme à l'ordinaire.

Les règles qui précèdent caractérisent ce qu'on appelle la *logique faible du second ordre*. Sans entrer dans plus de détail, on peut constater qu'elle apporte de nouvelles ressources aux possibilités de la logique du premier ordre. En particulier, les numéraux apparaissent dans $HF(\varnothing) \subset HF(E)$:

0 est le cardinal de $\varnothing$
1 est le cardinal de $\{\varnothing\}$
2 est le cardinal de $\{\varnothing, \{\varnothing\}\}$
3 est le cardinal de $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$
⋮
n est le cardinal de l'ensemble des numéraux qui le précèdent.

Ce type de logique présente des analogies avec la $\mathbb{N}$-logique. Comme elle, elle introduit une notion préétablie de finitude. Cela peut s'observer à deux stades de la "construction" des ensembles héréditairement finis. Une première fois lorsqu'on évoque les parties finies d'un ensemble; on peut admettre qu'on se réfère à la finitude au sens naïf: un ensemble est fini quand on peut le compter, c'est-à-dire quand son cardinal est un numéral. La deuxième occasion se présente quand on décrit la clôture héréditairement finie de $\mathscr{P}F(E)$; la procédure est donnée par une récurrence complète qui n'a de sens que dans un modèle préexistant des entiers naturels. ■

9.2 LOGIQUES D'ORDRE SUPÉRIEUR

9.2.0 Préambule

Il est temps de présenter brièvement les logiques d'ordre supérieur au premier. Cela nous aidera à situer la logique du premier ordre.

Partons d'une constatation. Soit L^1 un langage du premier ordre comportant un symbole de fonction unaire f_1. En vertu des axiomes de Leibniz:

$$\vdash (x=x') \rightarrow (f_1(x)=f_1(x)).$$

En vertu du corollaire de la proposition 6.3.3, on peut quantifier sur les symboles de variables x et x':

$$\vdash \forall x \forall x'((x=x') \rightarrow (f_1(x)=f_1(x'))).$$

Ainsi, dans toutes les L^1-structures et ***quel que soit*** le symbole f_1, l'énoncé précédent est satisfait. On est tenté d'écrire:

$$\vdash \forall f_1 \forall x \forall x'((x=x') \rightarrow (f_1(x)=f_1(x'))).$$

Malheureusement, ce qui suit $\vdash$ n'est pas une formule de L^1, ni de tout autre langage du premier ordre. Nous allons voir qu'en revanche, c'est une formule du second ordre.

9.2.1 Langages du deuxième ordre

On décrit un *langage du deuxième ordre* L^2 en donnant:

9.2.1.0 les symboles logiques: $\neg \quad \wedge \vee \rightarrow \leftrightarrow \; = \; \forall \; \exists$

9.2.1.1 les signes de ponctuation: ( ) ,

9.2.1.2 des symboles de constantes:

a) *constantes individuelles*: c, c', c'', ...
b) *constantes-fonctions*: f_n, $f'_{n'}$, ...
c) *constantes-relations*: r_m, $r'_{m'}$, ...

9.2.1.3 les symboles de variables:

a) *variables individuelles*: x, x', ...
b) *variables-fonctions*: F_n, $F'_{n'}$, ...
c) *variables-relations*: R_m, $R'_{m'}$, ...

Comme on le verra plus loin, seuls 9.2.1.3 b) et c) sont nouveaux par rapport aux langages du premier ordre. Les symboles 9.2.1.2 sont dits *propres* à L^2.
Les *termes* de L^2 sont obtenus par les règles suivantes:

- Si c est un symbole de constante individuelle, c est un terme.
- Si x est un symbole de variable individuelle, x est un terme.
- Si t_1, t_2, ... , t_n sont des termes et f_n un symbole de constante-fonction, $f_n(t_1, t_2, \ldots, t_n)$ est un terme.
- Si t_1, t_2, ... , t_m sont des termes et F_m un symbole de variable-fonction, $F_m(t_1, t_2, \ldots, t_m)$ est un terme.

Les *formules atomiques* de L^2 sont de la forme

- $(t_1=t_2)$

- $r_n(t_1, t_2, \dots, t_n)$
- $R_m(t_1, t_2, \dots, t_m)$

où $t_1, t_2, \dots, t_n, t_m$ sont des termes, r_n un symbole de constante-relation n-aire, R_m un symbole de variable-relation m-aire.

Les *formules* de L^2 s'obtiennent en appliquant les règles suivantes:

- les formules atomiques de L^2 sont des formules de L^2
- si α et β sont des formules de L^2, $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \wedge \beta)$, $(\alpha \mapsto \beta)$, $(\alpha \leftrightarrow \beta)$ aussi
- si φ est une formule de L^2 et si x, F_n et R_m sont des symboles de variables, $(\forall x\varphi)$ $(\forall F_n\varphi)$ $(\forall R_m\varphi)$ $(\exists x\varphi)$ $(\exists F_n\varphi)$ $(\exists R_m\varphi)$ sont des formules de L^2.
- il n'y a pas d'autres formules de L^2 que celles qu'on obtient par l'application des règles précédentes.

Les formules de L^2 qui ne comportent aucun symbole de variable-fonction ni de variable-relation sont les formules d'un langage du premier ordre ayant les mêmes symboles propres que L^2.

Le décompte des *variables libres* d'une formule de L^2 se fait exactement selon les mêmes règles qu'en logique du premier ordre. Un *énoncé* de L^2 est une formule de L^2 sans variable libre.

9.2.2 Interprétation ensembliste d'un langage du deuxième ordre

Passons à l'aspect sémantique de la logique du second ordre. Les définitions que nous allons donner généralisent naturellement celles qui concernent la logique du premier ordre. Une *L^2-structure ensembliste* (E, J) est un couple où E est un ensemble non vide et J une application associant à toute constante individuelle c un élément $J(c)$ de E, à toute constante-fonction f_n une application $J(f_n): E^n \to E$ et à toute constante-relation r_m une partie $J(r_m)$ de E^m.

Une *spécialisation* s de (E, J) est donnée par une application définie sur l'ensemble des variables:

- si x est une variable individuelle, $s(x) \in E$;
- si F_n est une variable-fonction n-aire, $s(F_n)$ est une fonction $s(F_n): E^n \to E$;
- si R_m est une variable-relation m-aire, $s(R_m)$ est une partie de E^m.

s s'étend à tous les termes de L^2 par le moyen des règles suivantes:

- si c est une constante individuelle, $s(c) := J(c)$;
- si f_n est une constante-fonction n-aire et si $t_1, t_2, \dots, t_n$ sont des termes, $s(f_n(t_1, t_2, \dots, t_n)) := J(f_n)(s(t_1), s(t_2), \dots, s(t_n))$;
- si F_n est une variable-fonction n-aire et si $t_1, t_2, \dots, t_n$ sont des termes, $s(F_n(t_1, t_2, \dots, t_n)) := s(F_n)(s(t_1), s(t_2), \dots, s(t_n))$.

Ces règles permettent de déterminer $s(t)$ pour tout terme t de L^2 par récurrence sur la construction de t.

Il faut encore définir l'expression: $(E, J) \models \varphi[s]$, où φ est une formule de L^2, et qui se lit:" "*La L^2-structure (E, J) satisfait la formule φ pour la spécialisation s*". Il suffit de reprendre la définition 2.2.11 et de lui adjoindre quelques nouvelles règles. D'abord, si $\Phi_n : E^n \to E$ est une fonction n-aire sur E, si F_n est un symbole de variable-fonction n-aire, $s\left(\frac{F_n}{\Phi_n}\right)$ est la spécialisation de (E, J) qui coïncide avec s sur les symboles de variables, sauf éventuellement en F_n, et qui envoie F_n sur Φ_n. De même, si $\Omega_m \subset E^m$ et si R_m est un symbole de variable-relation m-aire, $s\left(\frac{R_m}{\Omega_m}\right)$ désigne la spécialisation coïncidant avec s, sauf éventuellement en R_m, et qui envoie R_m sur Ω_m. Reprenons alors les 9 règles de la définition 2.2.11; récrivons la règle 2:

2′) si r_m est constante-relation et $t_1, t_2, \dots, t_m$ des termes de L^2:
$(E, J) \models r_m(t_1, t_2, \dots, t_m)[s]$ signifie: $(s(t_1), s(t_2), \dots, s(t_m)) \in J(r_m)$.

Puis posons les nouvelles règles suivantes, où F_n et R_m sont respectivement une variable-fonction et une variable-relation:

10) $(E, J) \models (\forall F_n \varphi)[s]$ signifie: quelle que soit la fonction $\Phi_n : E^n \to E$, $(E, J) \models \varphi[s\left(\frac{F_n}{\Phi_n}\right)]$.

11) $(E, J) \models (\exists F_n \varphi)[s]$ signifie: il existe une fonction $\Phi_n : E^n \to E$ telle que $(E, J) \models \varphi[s\left(\frac{F_n}{\Phi_n}\right)]$.

12) $(E, J) \models (\forall R_m \varphi)[s]$ signifie: quelle que soit $\Omega_m \subset E^m$, $(E, J) \models \varphi[s\left(\frac{R_m}{\Omega_m}\right)]$.

13) $(E, J) \models (\exists R_m \varphi)[s]$ signifie: il existe $\Omega_m \subset E^m$ telle que $(E, J) \models \varphi[s\left(\frac{R_m}{\Omega_m}\right)]$.

Lorsque α est un énoncé de L^2, $(E, J) \models \alpha[s]$ entraîne que $(E, J) \models \alpha[s']$ pour toute spécialisation s' de (E, J). On note alors simplement $(E, J) \models \alpha$.

N'allons pas plus loin dans la description de la logique du deuxième ordre. Cela suffit pour faire apparaître quelques ressemblances et quelques écarts relativement à la logique du premier ordre.

Faisons cependant quelques remarques.

9.2.3 Remarque

Soit α une formule du langage L^2 ne comportant comme variable libre que le symbole de variable-relation unaire R_1 et soit (E, J) une L^2-structure. Désignons par s une spécialisation de (E, J). Pour vérifier que $(E, J) \models (\forall R_1 \alpha)$, il faut considérer que $s(R_1)$ parcourt l'ensemble des parties de E, soit $\mathscr{P}(E)$. Lorsque E est dénombrable, $\mathscr{P}(E)$ est infini non dénombrable. Il en résulte que la logique du deuxième ordre ne convient pas à l'étude des fondements du nombre naturel.

Précisons un peu ce point. La notion de nombre naturel est l'une des premières qui se présentent lorsqu'on aborde les mathématiques. L'étude des fondements des mathématiques a pour but de reconnaître la nature de telles notions et de les ramener, si possible, à des notions plus élémentaires. La connaissance du nombre naturel équivaut à celle de l'ensemble $\mathbb{N}$, ou si on préfère, à celle du dénombrable. La logique du premier ordre essaie vainement de la ramener à des procédures finitistes. La logique du second ordre, qui paraît plus heureuse pour aborder $\mathbb{N}$, nécessite l'emploi de l'ensemble $\mathscr{P}(\mathbb{N})$ des parties de $\mathbb{N}$. Or $\mathscr{P}(\mathbb{N})$ est une notion beaucoup moins claire encore que $\mathbb{N}$. Pour le voir, partons des hypothèses intuitives suivantes:

- (L_e, S_e) est une théorie du premier ordre pour les ensembles.
- $\mathbb{N}$, ensemble des nombres naturels, est bien déterminé.

D'après l'axiome C_6 de (L_e, S_e), l'axiome de l'ensemble des parties, il existe un ensemble $\mathscr{P}(\mathbb{N})$ des parties de $\mathbb{N}$. Nous avons montré que le cardinal de $\mathbb{N}$, $\#(\mathbb{N})$, est strictement inférieur à celui de $\mathscr{P}(\mathbb{N})$. Existe-t-il des ensembles dont le cardinal est strictement supérieur à $\#(\mathbb{N})$ et strictement inférieur à $\#(\mathscr{P}(\mathbb{N}))$? Pendant longtemps, la conjecture la plus plausible fut qu'il n'y en avait pas. C'est l'*hypothèse du continu.* En 1963, Paul J. Cohen établit un résultat surprenant. Il donna une suite illimitée de cardinaux distincts:

$$\alpha_0=0,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \ldots,\ \alpha_i,\ \ldots \qquad i=0,\ 1,\ 2,\ 3,\ \ldots$$

tels que l'on puisse adjoindre à (L_e, S_e) l'un quelconque des axiomes:

H_i: l'ensemble des cardinaux strictement compris entre $\#(\mathbb{N})$ et $\#(\mathscr{P}(\mathbb{N}))$ a le cardinal α_i.

Plus précisément, si (L_e, S_e) est une théorie, $(L_e, S_e \cup \{H_i\})$ est aussi une théorie. Lorsque $i=0$, on obtient une théorie des ensembles satisfaisant l'hypothèse du continu. Lorsque $i=0, 1, 2, 3, \ldots$, on obtient autant de théories des ensembles distinctes; car si $i \neq k$, H_i et H_k sont manifestement incompatibles.

En conséquence, il existe une infinité de manières distinctes de concevoir $\mathscr{P}(\mathbb{N})$ à partir d'un même $\mathbb{N}$. Pour certains mathématiciens, la façon la plus "naturelle" est de prendre $i=0$. Paul J.Cohen estime, au contraire, que l'hypothèse du continu est "évidemment fausse"! Ainsi, même quand on considère $\mathbb{N}$ comme un ensemble "naturel", on n'a pas d'idée claire sur ce que représente $\mathscr{P}(\mathbb{N})$. Plus généralement, le passage d'un ensemble infini E à l'ensemble $\mathscr{P}(E)$ de ses parties est une opération forte qui défie l'intuition. Par suite, on ne peut pas se référer à $\mathscr{P}(\mathbb{N})$ pour éclairer $\mathbb{N}$. Autrement dit, la logique du second ordre n'est pas de nature à nous aider dans l'étude des fondements du nombre naturel.

9.2.4 Remarque

Pour autant qu'on ne se préoccupe plus de questions de fondements, la logique du deuxième ordre ouvre des perspectives intéressantes, parce qu'elle s'adapte bien à certaines situations naïves. Par exemple, l'axiome original de Peano, que nous avons vainement essayé de traduire en langage du premier ordre sous la désignation Ω (cf. formule (8.1), peut s'écrire sous la forme:

$$\forall R_1((R_1(0) \wedge \forall x(R_1(x) \rightarrow R_1(x+1))) \rightarrow \forall x R_1(x))$$

dans tout langage du deuxième ordre comportant des constantes individuelles 0 et 1, et une constante-fonction notée $+$.

9.2.5 Remarque

Dans la même perspective, la logique du deuxième ordre permet d'exprimer facilement qu'un ensemble est infini: il suffit d'affirmer qu'il existe une bijection de cet ensemble sur une de ses parties propres:

$$\alpha_\infty \equiv \exists F_1((\forall x \forall x'(F_1(x) = F_1(x')) \rightarrow (x = x')) \wedge (\exists x \forall x'(\neg(F_1(x') = x)))).$$

Cette formule appartient à tout langage du deuxième ordre L^2 et toute L^2-structure (E, J) satisfaisant α_∞ est telle que E soit infini. Il est clair que $(\neg\alpha_\infty)$ exprime, au contraire, que E est fini. Ainsi, à l'opposé de la logique du premier ordre, la logique du deuxième ordre a prise sur la finitude et l'infinitude.

9.2.6 Remarque

D'un côté, la logique du deuxième ordre se prête bien au traitement d'une notion naïve de finitude. De l'autre, elle s'appuie sur une notion de modèle qui exige une théorie non naïve des ensembles. Formulons une observation à ce propos.

Nous savons que la "théorie" des ensembles du premier ordre de Zermelo-Fraenkel admet un modèle dénombrable $(\mathbb{E}, J)$ – pour autant que ce soit une théorie. Dans $\mathbb{E}$ figurent des éléments correspondant aux ensembles $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, ... ayant respectivement 0, 1, 2, ... éléments; et plus généralement, des ensembles dont le cardinal est un numéral.

En vertu de l'axiome de l'infini, il existe dans $\mathbb{E}$ des ensembles dont le cardinal n'est pas un numéral; soit A l'un d'entre eux. Les applications de A dans lui-même (au sens de $\mathbb{E}, J$)) sont des ensembles de couples, donc des éléments de $\mathbb{E}$. $\mathbb{E}$ étant dénombrable, elles ne représentent qu'une portion négligeable de toutes les applications *au sens naïf* de A dans lui-même (on vérifie facilement que l'ensemble des applications "naïves" de A dans lui-même a un cardinal au moins égal à celui de $\mathscr{P}(A)$). Il est donc imprudent d'affirmer *a priori* l'existence dans $\mathbb{E}$ d'un élément représentant une bijection de A sur une de ses parties propres.

En bref, la "naïveté" consiste ici à identifier les ensembles dont le cardinal est un numéral avec les ensembles vérifiant l'axiome $(\neg\alpha_\infty)$. Cette identification n'implique probablement aucune contradiction; mais le fait échappe à toute preuve élémentaire, en particulier à cause du caractère informel de la notion de numéral.

9.2.7 Remarque

Pour ce qui suit, nous convenons d'adopter l'identification mentionnée ci-dessus. Dans tout langage du 2e ordre L^2 (comme d'ailleurs dans tout langage du premier ordre), on peut écrire les formules suivantes:

$$\alpha_2 \equiv \exists x' \exists x'' (\neg (x' = x''))$$
$$\alpha_3 \equiv \exists x' \exists x'' \exists x''' (\neg ((x' = x'') \vee (x' = x''') \vee (x'' = x''')))$$
$$\vdots$$
$$\alpha_n \equiv \exists x' \exists x'' \ldots \exists x^{(n)} (\neg ((x' = x'') \vee (x' = x''') \vee \ldots \vee (x' = x^{(n)}) \vee \ldots \vee (x^{(n-1)} = x^{(n)}))).$$
$$\vdots$$

La traduction intuitive de α_n est: "il existe n éléments distincts". En vertu de la convention initiale, la collection d'axiomes:

$$S = \{\alpha_2, \alpha_3, \ldots, \alpha_n, \ldots, (\neg \alpha_\infty)\}$$

n'admet aucun modèle. En revanche, toute partie finie T de S admet un modèle: si $T \subset \{\alpha_2, \alpha_3, \ldots, \alpha_m, (\neg \alpha_\infty)\}$, on peut construire un modèle de T ayant exactement $(m+1)$ éléments. Le théorème de compacité de la logique du 1er ordre n'a donc pas d'équivalent en logique du 2e ordre.

On peut aussi remarquer – toujours sous réserve de la convention du début – que tout modèle de

$$T' = \{\alpha_2, \alpha_3, \ldots, \alpha_n, \ldots\}$$

satisfait α_∞. Mais cela n'est vrai qu'à condition de prendre en compte une infinité d'axiomes de T'. Cela exclut toute possibilité de preuve finitiste de α_∞ à partir de T': le théorème de complétude de la logique du 1er ordre n'est donc pas transportable tel quel à la logique du 2e ordre.

9.2.8 Remarque

La remarque 9.2.4 suggère que la logique du 2e ordre se prête bien à la description de l'arithmétique. C'est bien le cas, en effet. Elle convient aussi à la topologie générale et à l'analyse (i.e. la théorie des nombres réels). Il est facile de donner un langage du 2e ordre L^2 comportant un nombre fini de symboles propres et un système d'axiomes de L^2 pour décrire les nombres réels. Cela fournit en passant un exemple de système formel du 2e ordre comportant un nombre fini de symboles propres, mais n'admettant aucun modèle dénombrable. Donc le théorème de Löwenheim – Skolem n'est pas valide tel quel en logique du 2e ordre.

9.2.9 Logiques d'ordre supérieur à 2

On peut considérer des logiques d'ordre supérieur au deuxième. Il suffit d'introduire de nouveaux symboles de constantes et de variables pour des fonctions ou des relations dont les arguments sont, au moins en partie, des fonctions ou des relations.

Par exemple, soit R_m un symbole de variable-relation m-aire du 2^e ordre. Considérons un symbole de fonction unaire $\bar{F}_1$ caractérisé ainsi: x étant un symbole de variable individuelle,

$$\bar{F}_1(R_m)(x) \leftrightarrow R_m(\underbrace{x, x, \dots, x}_{\mathrm{m}})$$

$\bar{F}_1(R_m)$ apparaît comme une relation unaire du premier ordre. $\bar{F}_1$ peut donc être considéré comme une constante-fonction à un argument du type variable-relation m-aire du 2^e ordre, dont la valeur est une relation unaire du 1er ordre. $\bar{F}_1$ est un symbole du 3^e ordre. Plus généralement, un symbole de constante-relation ou de variable-relation du *n-ième ordre* a pour argument des symboles d'ordre (n-1) au plus, l'un d'eux au moins étant effectivement d'ordre (n-1).

Considérons quelques exemples simples: supposons d'abord qu'on veuille ordonner par inclusion l'ensemble des parties d'un ensemble. On commence par décrire ces parties à l'aide d'un symbole de variable-relation unaire R_1 du 2^e ordre. On introduit ensuite un symbole de variable-relation du 3^e ordre $\bar{R}_2$ (.,.) à deux arguments du type variable-relation unaire du 2^e ordre, satisfaisant la condition:

$$\bar{R}_2(R_1,\ R'_1) \leftrightarrow (\forall x(R'_1(x) \rightarrow R_1(x))).$$

Ce qui veut dire: l'ensemble des x tels que $R'_1(x)$ est inclus dans celui des x tels que $R_1(x)$.

Donnons un autre exemple. Soit $\leqq$ un symbole de relation binaire du premier ordre ayant les propriétés formelles d'un ordre total (voir n° 2.1.10). Nous aimerions exprimer formellement que $\leqq$ est un *bon ordre*. Cela peut se faire dans un langage du 3^e ordre L^3, en posant:

$$\exists \bar{F}_1(\forall R_1((\exists x R_1(x)) \rightarrow (R_1(\bar{F}_1(R_1)) \wedge (\forall y R_1(y) \rightarrow (\bar{F}_1(R_1) \leqq y)))))$$

Dans cette formule, x et y sont des variables individuelles; R_1 est une variable-relation unaire du 2^e ordre servant à décrire les parties d'un ensemble; $\bar{F}_1$ est une variable-fonction du 3^e ordre, à un argument du type R_1 et à valeur de type "individu". Autrement dit, dans toute L^3-structure (E, J), $\bar{F}_1$ est interprétée comme une fonction attachant à toute partie de E un élément de E. La formule ci-dessus exprime qu'il existe une telle fonction attachant à toute partie non vide de E un élément minimal de cette partie. On constate que, dans le cas particulier, le langage du 3^e ordre L^3 suit d'assez près la langue ordinaire. On pourrait parler du bon ordre dans un langage du premier ordre L^1, mais il est facile de se convaincre que la traduction est plus laborieuse.

9.3 SUR LA LOGIQUE INTUITIONNISTE

9.3.0 Préambule

La complétude de la logique du premier ordre donne une base juridique solide à un principe aujourd'hui accepté par la quasi-totalité des mathématiciens:

un objet mathématique existe dès que les deux conditions suivantes sont satisfaites:

- l'existence de cet objet n'implique pas contradiction;
- cet objet a été évoqué par un mathématicien au moins.

Ainsi les nombres complexes existent parce qu'on peut montrer que leur existence n'introduit pas de contradiction dans la théorie des nombres réels; mais ils n'existaient pas à l'époque d'Euclide, parce qu'aucun mathématicien ne les avait évoqués (pourtant les similitudes centrales positives du plan étaient certainement connues en ce temps-là).

Ce principe conduit à admettre des démonstrations d'existence non constructives. Donnons-en un exemple:

Proposition: il existe deux nombres (réels) irrationnels a et b tels que a^b soit rationnel.

Démonstration: soit $a_1=b_1=\sqrt{2}$. Si $a_1^{b_1}$ est rationnel, la démonstration est achevée. Sinon, posons $a_2=a_1^{b_1}$ et $b_2=\sqrt{2}$. Alors $a_2^{b_2}=2$. C.q.f.d.

L'une exactement des deux éventualités convient, mais il est difficile de savoir laquelle. Les tenants de la logique intuitionniste ne se déclarent pas satisfaits par ce genre de démonstration.

9.3.1 L'idée de logique intuitionniste

La logique intuitionniste admet les mêmes règles syntaxiques que la logique du premier ordre. Elle accepte à peu près les mêmes axiomes logiques, mais elle rejette la tautologie: $\alpha\leftrightarrow(\neg(\neg\alpha))$. Elle la remplace par les deux tautologies suivantes:

$$\alpha\rightarrow(\neg(\neg\alpha))$$
$$\neg\alpha\rightarrow(\alpha\rightarrow\beta)$$

Elle admet les mêmes règles d'inférence que la logique du premier ordre. Cela implique que tous les théorèmes intuitionnistes sont valides en logique du premier ordre. Toutefois la réciproque est fausse, puisque la logique intuitionniste n'admet pas le principe du tiers exclu.

En logique du premier ordre, les tautologies sont définies à l'aide des fonctions de vérité. Celles-ci sont à valeurs 0 ou 1, soit le faux ou le vrai. Ce n'est pas le cas de la logique intuitionniste qui, outre le faux et le vrai, connaît une troisième éventualité: l'*indécidable*. Elle se prête ainsi à la description, ***de l'extérieur***, d'un système formel du premier ordre incomplet tel que (L_n, S_n) ou (L_e, S_e), où apparaissent des théorèmes, des négations de théorèmes et des énoncés α indécidables, ni α ni $(\neg\alpha)$ n'étant des théorèmes.

9.3.2 L'idée de mathématiques intuitionnistes

Les mathématiques intuitionnistes se développent à partir de la logique intuitionniste comme les mathématiques classiques le font pour la logique du premier ordre. Toutefois elles sont caractérisées par le principe suivant: un objet mathématique intuitionniste n'existe que si l'on donne une procédure permettant de déterminer effectivement tous les paramètres qui le fixent. Ainsi tout numéral est un objet mathématique intuitionniste; tout quotient de numéraux aussi. Il existe des nombres réels intuitionnistes et d'autres qui ne le sont pas. Par exemple, π est un nombre réel intuitionniste car:

$$\pi = 4\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \ldots\right)$$

Au bout d'un nombre fini (numéral) d'opérations effectives sur des numéraux, on trouve que la partie entière de π est 3 parce que

$$4\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15}\right) < \pi < 4.$$

Au bout d'un nombre fini de nouveaux calculs, on découvre le chiffre des dixièmes, puis celui des centièmes et ainsi de suite. On donne π comme le "quadruple de la somme alternée des inverses des numéraux impairs". C'est là une consigne de calcul qui s'énonce par une phrase finie traduisible dans le langage de l'arithmétique. Il en est de même, par définition, de tous les nombres réels au sens intuitionniste. Ils forment un ensemble dénombrable car tel est le cardinal de l'ensemble des consignes effectivement exprimables en arithmétique. Comme les nombres réels au sens ordinaire forment un ensemble qui a la puissance du continu, il en existe certainement qui ne le sont pas au sens intuitionniste. Notons en passant la parenté entre les nombres réels intuitionnistes et les fonctions "calculables", c'est-à-dire les fonctions récursives générales.

Chose remarquable, il existe des nombres réels au sens intuitionniste dont il est impossible de savoir s'ils sont nuls ou non. Donnons-en un exemple. Abrégeons par $P(n)$ l'assertion: "n est un numéral tel que les n premières décimales de π à droite de la virgule se terminent par dix chiffres 7 consécutifs:

$$3,\underbrace{141\ldots\quad\ldots7777777777}_{n \text{ décimales}}.$$

Posons alors:

$$a_m = \begin{cases} 0 & \text{si } \forall n((n \leqq m) \to (\neg P(n))) \\ \dfrac{1}{2^n} & \text{si } (n \leqq m) \wedge P(n) \wedge (\forall p((n < p \leqq m) \to (\neg P(p)))). \end{cases}$$

(Traduction: a_m est nul si les m premières décimales de π ne comportent pas de séquence formée de dix 7 consécutifs; dans le cas contraire, $a_m = \frac{1}{2^n}$, où n est le plus grand numéral inférieur ou égal à m tel que $P(n)$.)

La suite $(a_0, a_1, a_2, \ldots, a_m, \ldots)$ est formée de termes calculables. Elle converge vers un nombre réel a au sens intuitionniste qui est nul si la partie décimale de π ne comporte aucune séquence de dix 7 consécutifs ou si elle en comporte une infinité. Si la partie décimale de π comporte exactement une collection finie non vide de telles séquences, a est de la forme $\frac{1}{2^p}$ pour un numéral $p > 0$ convenable. Selon les exigences de l'intuitionnisme, il n'existe aucun moyen de savoir si a est nul ou non. Dans un certain sens, l'équation $ax = 0$ est indécidable.

9.3.3 Remarque

L'intuitionnisme s'appuie sur des considérations de type philosophique. Il développe une logique et une mathématique propres. Il n'admet que des objets qu'on peut effectivement décrire: un numéral, une collection finie de numéraux. Il nie l'existence réelle des ensembles infinis, des classes d'infinitude distinctes. A ce propos, Paul J. Cohen formule une observation intéressante. Il note que Consis (L_e, S_e) est un énoncé arithmétique dans L_n qui n'admet pas de preuve dans (L_n, S_n), bien qu'il soit certainement valide. Cela signifie que Consis (L_e, S_e) ne peut être prouvé sans raisonner sur des ensembles de cardinal supérieur au dénombrable, qui peuvent être décrits dans (L_e, S_e). Si on dénie à ces ensembles toute signification pour les mathématiques, on renonce à tout espoir de prouver certains faits arithmétiques. Selon Cohen, “cela constitue la plus grande faiblesse de la position intuitionniste puisque des énoncés que ses tenants considèrent comme significatifs n'ont aucun espoir d'être jamais tranchés selon leurs propres exigences”.

9.3.4 Remarque

Il est peut-être utile de formuler une dernière remarque. La logique intuitionniste considère le vrai, le faux et l'indécidable. Mais le discours sur cette logique ne connaît que le vrai et le faux. Un théorème de mathématiques intuitionnistes n'est pas lui-même indécidable, pas plus qu'un théorème de calcul des probabilités n'est simplement probable. En revanche la logique du premier ordre et la logique naïve ont la même échelle de valeurs de vérité. C'est une simplification bienvenue, mais peut-être aussi une source de confusion.

9.4 SUR LA LOGIQUE MODALE

9.4.0 Préambule

La logique formelle s'efforce de réduire au minimum le rôle de la sémantique en faveur de l'aspect syntaxique. La logique du premier ordre est l'exemple d'une réussite absolue dans ce sens, en vertu du théorème de complétude. En effet, les interprétations ensemblistes n'ajoutent rien aux possibilités de la pure syntaxe. Elles n'en ôtent rien non plus et c'est heureux! La logique formelle apparaît comme un moyen, parmi d'autres, pour affermir une présomption, pour transformer une conjecture en certitude et, plus généralement, comme une voie permettant d'éclairer et de consolider une construction de la pensée. C'est le cas de la pratique des mathématiques en particulier et de bien d'autres disciplines scientifiques ou non.

On peut toutefois essayer d'intégrer volontairement à la logique des éléments d'interprétation. On parle alors de *logique intentionnelle*: elle prend en compte l'intention de celui qui raisonne. Elle s'oppose à la logique purement formelle, qualifiée d'*extensionnelle*, qui s'intéresse, dans leur extension, à des jeux de signes dénués de contenu. En logique intentionnelle, on peut s'efforcer de garder une certaine maîtrise des éléments subjectifs liés au projet de celui qui raisonne; on essaie de les circonscrire par des formalismes appropriés.

La notion d'implication nous donne un point d'accrochage. "$\alpha \rightarrow \beta$" équivaut formellement à "β ou non α". Mais ordinairement, on l'utilise pour dire: "il est impossible d'avoir α sans β". C'est un exemple simple de proposition modale. Une même assertion peut être énoncée sous divers modes, qui la "modifient": elle peut être taxée de possible ou d'impossible, de nécessaire, de souhaitable, etc. La *logique modale* traite de ce genre de discours. Elle fut étudiée et développée abondamment par les scolastiques médiévaux. Au début du XX^{e} siècle, elle fut remise à l'honneur par Hugh Mac Coll et surtout par Clarence Irving Lewis dès 1918. Nous allons en ébaucher une description.

Dans un langage du premier ordre, la formule

$$(x=x')\rightarrow(f(x)=f(x'))$$

(où f est un symbole de fonction unaire, x et x' deux symboles de variables) semble plus nécessaire que $(x=x')$. La première est satisfaite dans toutes les interprétations convenables; la deuxième semble accidentelle. Inspirons-nous d'une idée de Leibniz: une proposition est *nécessaire* quand elle est vraie dans tous les mondes possibles; elle est *possible* lorsqu'elle est vraie dans un monde au moins, éventuellement le nôtre.

9.4.1 Description d'un langage modal

Partons d'un langage du premier ordre L comportant un ensemble fini ou dénombrable de symboles propres. Soit I une section commençante de $\mathbb{N}=\{0, 1, 2, 3, \ldots\}$ et soit

$$\Pi = \{p_i | i \in I\} = \{p_0, p_1, \dots, p_n, \dots\}$$

un ensemble non vide, fini ou dénombrable d'*énoncés* dans L. Introduisons deux nouveaux symboles $\square$ et $\diamond$. A partir des énoncés de Π et de ces deux symboles, nous allons former l'ensemble $\Omega(\Pi)$ des *formules modales* sur Π. Nous procédons exactement comme pour la construction des formules du premier ordre à partir des formules atomiques (cf. déf. 1.0.8).

Posons en effet les règles suivantes:

F_1) $\Pi \subset \Omega(\Pi)$
F_2) si $\alpha, \beta \in \Omega(\Pi)$, $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \to \beta)$, $(\alpha \leftrightarrow \beta)$ sont dans $\Omega(\Pi)$
F_3) si $\alpha \in \Omega(\Pi)$, $(\square\alpha)$ et $(\diamond\alpha)$ sont dans $\Omega(\Pi)$
F_4) il n'y a pas d'autres formules dans $\Omega(\Pi)$ que celles qui résultent de l'application des règles F_1, F_2 et F_3.

$(\square\alpha)$ se lit "il est nécessaire que α"; $(\diamond\alpha)$ se lit "il est possible que α".

L'introduction des parenthèses nous assure l'unique lisibilité des formules modales sur Π. Par la suite, nous nous permettrons quelques libertés dans l'emploi des parenthèses, afin d'alléger les écritures.

Les *formules modales premières* de $\Omega(\Pi)$ sont:

- les formules de Π
- les formules de $\Omega(\Pi)$ de la forme $(\square\alpha)$ ou $(\diamond\alpha)$, où $\alpha \in \Omega(\Pi)$.

Désignons par $PM(\Pi)$ l'ensemble des formules modales premières de $\Omega(\Pi)$. On peut écrire:

$$\Omega(\Pi) = \Phi(PM(\Pi)) \qquad \text{(cf. définition 3.1.2)}$$

Autrement dit, $\Omega(\Pi)$ est l'ensemble des formes propositionnelles construit sur $PM(\Pi)$. On peut donc définir les *fonctions de vérité* sur $\Omega(\Pi)$ (cf. définition 3.1.8) et, par suite, les *tautologies modales* sur Π (cf. définition 3.1.14).

9.4.2 Mondes et modèles

Définissons maintenant l'idée de *modèle de* $\Omega(\Pi)$.

Donnons-nous une fois pour toutes un "grand ensemble" Σ; nous entendons que Σ est au moins dénombrable. Nous appellerons *L-Σ-monde*, ou tout simplement *monde*, toute L-structure (E, J) où E est un sous-ensemble de Σ. On vérifie sans peine que les L-Σ-mondes forment un ensemble que nous appellerons $M(L, \Sigma)$, ou plus simplement M. Désignons encore par P_i l'ensemble des mondes satisfaisant l'énoncé p_i, $p_i \in \Pi$; et posons:

$$P = \{P_0, P_1, \dots\} = \{P_i | i \in I\}.$$

Alors, par définition, (P, M) est un *modèle de* $\Omega(\Pi)$.

9.4.3 Règles de satisfaction modales

Notons que la terminologie utilisée ici s'écarte de celle à laquelle la logique du premier ordre nous a habitués. Elle va révéler son utilité dans les *règles de satisfaction modales*. Prenons $\alpha \in \Omega(\Pi)$ et $A \in M$. L'assertion: "*α est satisfait dans A*", qu'on note $(M, A) \vDash \alpha$, est définie par les règles suivantes:

1) $(M, A) \vDash p_i \Leftrightarrow A \in P_i \qquad (i \in I)$
2) $(M, A) \vDash (\neg\alpha) \Leftrightarrow$ il est faux que $(M, A) \vDash \alpha$
   $(M, A) \vDash (\alpha \wedge \beta) \Leftrightarrow (M, A) \vDash \alpha$ *et* $(M, A) \vDash \beta$
   $(M, A) \vDash (\alpha \vee \beta) \Leftrightarrow (M, A) \vDash \alpha$ *ou* $(M, A) \vDash \beta$
   $(M, A) \vDash (\alpha \rightarrow \beta) \Leftrightarrow (M, A) \vDash \beta$ *ou* $(M, A) \vDash (\neg\alpha)$
   $(M, A) \vDash (\alpha \leftrightarrow \beta) \Leftrightarrow (M, A) \vDash (\alpha \rightarrow \beta)$ *et* $(M, A) \vDash (\beta \rightarrow \alpha) \qquad \alpha, \beta \in \Omega(\Pi)$
3) $(M, A) \vDash (\Box\alpha) \Leftrightarrow$ pour tout $B \in M$, $(M, B) \vDash \alpha$
4) $(M, A) \vDash (\Diamond\alpha) \Leftrightarrow$ il existe $B \in M$, tel que $(M, B) \vDash \alpha$.

Il convient de lire attentivement les règles 3) et 4) afin de se convaincre qu'elles s'accordent avec les locutions "il est nécessaire que α" et "il est possible que α". Ainsi la règle 3 exprime que α est nécessaire quand elle est satisfaite dans tous les mondes possibles, conformément à la conception de Leibniz.

9.4.4 Quelques formules modales valides

On dit que la formule modale $\alpha \in \Omega(\Pi)$ est *valide* et on note $\vDash \alpha$ si, pour tout modèle (M, P) et pour tout monde $A \in M$, $(M, A) \vDash \alpha$.

Les définitions et les conventions précédentes vont s'éclairer lorsque nous considérerons les formule modales valides suivantes.

$$(NE) \quad \text{pour tout } \alpha \in \Omega(\Pi) : \vDash \Box\alpha \rightarrow \alpha \tag{9.1}$$

(Intuitivement: tout ce qui est nécessaire, est (*necesse ad esse*).) Etablissons-le. Nous devons montrer que, dans tout modèle (M, P) de $\Omega(\Pi)$ et pour tout monde $A \in M : (M, A) \vDash \Box\alpha \rightarrow \alpha$.
Or:

$$(M, A) \vDash \alpha \quad ou \quad (M, A) \vDash (\neg\alpha).$$

Dans le second cas, il est faux que $(M, A) \vDash (\Box\alpha)$. D'où (NE).

Signalons en passant que les désignations de ces formules modales valides ont été introduites par Irving Lewis.

$$(5) \quad \text{pour tout } \alpha \in \Omega(\Pi) : \vDash \Diamond\alpha \rightarrow \Box\Diamond\alpha, \tag{9.2}$$

(ce qui est possible est nécessairement possible).
En effet, soit (M, P) un modèle de $\Omega(\Pi)$ et soit $A \in M$.

$$(M, A) \vDash \Box\Diamond\alpha \quad ou \quad \text{il est faux que } (M, A) \vDash \Box\Diamond\alpha.$$

Dans le second cas, il existe $B \in M$ tel que $(M, B) \vDash \neg\Diamond\alpha$.
Par suite, il est faux que $(M, A) \vDash \Diamond\alpha$. D'où (5).

(déf. $\Diamond$) pour tout $\alpha\in\Omega(\Pi)$: $\models\Diamond\alpha\leftrightarrow\neg(\Box(\neg\alpha))$ (9.3)

(intuitivement, est possible tout ce dont la négation n'est pas nécessaire).

En effet, soit (M, P) un modèle de $\Omega(\Pi)$ et $A\in M$. Nous devons montrer que: $(M, A)\models\Diamond\alpha\leftrightarrow\neg(\Box(\neg\alpha))$, soit que

$$et \begin{cases} (M, A)\models\Diamond\alpha\rightarrow\neg(\Box(\neg\alpha)) & (9.5)\\ (M, A)\models\neg(\Box(\neg\alpha))\rightarrow\Diamond\alpha & (9.6)\end{cases}$$

- Si $(M, A)\models\neg(\Box(\neg\alpha))$, (9.5) est satisfait.
- Si $(M, A)\models\Box(\neg\alpha)$, pour tout monde $B\in M$, $(M, B)\models(\neg\alpha)$; autrement dit, il est faux que $(M, B)\models\alpha$. Par suite, il est faux que $(M, A)\models\Diamond\alpha$. Donc $(M, A)\models\neg(\Diamond\alpha)$ et (9.5) est satisfait dans tous les cas.
- Si $(M, A)\models\Diamond\alpha$, (9.6) est satisfait.
- Si $(M, A)\models(\neg\Diamond\alpha)$, il est faux que $(M, A)\models\Diamond\alpha$. Donc pour tout monde $B\in M$, $(M, B)\models(\neg\alpha)$. Par suite $(M, A)\models\Box(\neg\alpha)$ et (9.6) est satisfait dans tous les cas.

Il résulte de (déf. $\Diamond$) qu'on pourrait se contenter du symbole $\Box$ et faire l'économie de $\Diamond$. On observe là une analogie marquée avec le jeu des quantificateurs.

(K) pour tous α, $\beta\in\Omega(\Pi)$: $\models\Box(\alpha\rightarrow\beta)\rightarrow(\Box\alpha\rightarrow\Box\beta)$, (9.7)

(s'il est nécessaire que α implique β, la nécessité de α implique celle de β).

En effet, soit (M, P) un modèle de $\Omega(\Pi)$ et $A\in M$:

- Si $(M, A)\models\Box\alpha\rightarrow\Box\beta$, alors $(M, A)\models\Box(\alpha\rightarrow\beta)\rightarrow(\Box\alpha\rightarrow\Box\beta)$.
- Si $(M, A)\models\neg(\Box\alpha\rightarrow\Box\beta)$, alors $(M, A)\models\neg(\Box\beta)$ *et* $(M, A)\models\Box\alpha$.
  Il existe donc $B\in M$ tel que $(M, B)\models(\neg\beta)$; en outre $(M, B)\models\alpha$.
  Donc il est faux que $(M, B)\models(\alpha\rightarrow\beta)$. Par suite, $(M, A)\models\neg(\Box(\alpha\rightarrow\beta))$ et $(M, A)\models\Box(\alpha\rightarrow\beta)\rightarrow(\Box\alpha\rightarrow\Box\beta)$. D'où ($K$).

(PL) si α est une tautologie modale de $\Omega(\Pi)$, $\models\alpha$. (9.8)

Cela exige une explication. Montrons qu'à tout modèle (M, P) de $\Omega(\Pi)$ et à tout monde $A(=(A, J))$ dans M, on peut attacher une fonction de vérité V bien déterminée sur $\Omega(\Pi)$.

Posons:

(I) si $p_i\in\Pi$, $V(p_i):=\begin{cases}1 & \text{si } (A, J)\models p_i\\ 0 & \text{si } (A, J)\models(\neg p_i).\end{cases}$ (9.9)

(II) si α, $\beta\in\Omega(\Pi)$,
a) $V(\neg\alpha):=1+V(\alpha)$
b) $V(\alpha\wedge\beta):=V(\alpha)\cdot V(\beta)$
c) $V(\alpha\vee\beta):=V(\alpha)+V(\beta)+V(\alpha)\cdot V(\beta)$ (9.10)
d) $V(\alpha\rightarrow\beta):=1+V(\alpha)+V(\alpha)\cdot V(\beta)$
e) $V(\alpha\leftrightarrow\beta):=1+V(\alpha)+V(\beta)$
(cf. 3.1.2, formules a), b), c), d), e)).

$$\text{(III)}\quad \text{si } \alpha\in\Omega(\Pi),\ V(\Box\alpha):=\begin{cases} 1 & \text{si, quel que soit } (B,J')\in M,\ (B,J')\models\alpha \\ 0 & \text{dans le cas contraire.}\end{cases} \tag{9.11}$$

$$\text{(IV)}\quad \text{si } \alpha\in\Omega(\Pi),\ V(\Diamond\alpha):=\begin{cases} 1 & \text{s'il existe } (B,J')\in M \text{ tel que } (B,J')\models\alpha \\ 0 & \text{dans le cas contraire.}\end{cases} \tag{9.12}$$

En vertu de l'unique lisibilité de formules modales de Π en fonction des formules modales premières, la fonction

$$V:\Omega(\Pi)\to\mathbb{F}_2$$

est bien déterminée. Les règles (II) nous assurent que V est bien une fonction de vérité sur $\Omega(\Pi)$. On vérifie aisément, en comparant les règles (I), (II), (III), (IV) et les règles 1), 2), 3), 4) que, si $\alpha\in\Omega(\Pi)$,

$$(M,\ A)\models\alpha\Leftrightarrow V(\alpha)=1.$$

Si α est une tautologie modale de $\Omega(\Pi)$, $V(\alpha)=1$. Donc $(M,\ A)\models\alpha$. Cela vaut pour tout modèle M et tout monde A dans M. Donc $\models\alpha$. L'assertion (PL) est donc satisfaite.

Comme le montrent les règles (I) à (IV), cette propriété repose bien sur la logique des propositions. Respectant les notations conventionnelles, nous la désignons par (PL) (de "*p*ropositional *l*ogic").

Jusqu'ici nous avons joué simultanément sur l'aspect syntaxique et sur les interprétations sémantiques des formules modales. Il est intéressant de noter qu'on peut éliminer toute interprétation ensembliste. Ainsi on peut introduire deux *règles d'inférence modale*:

- la *règle de nécessité* (RN) $\dfrac{\alpha}{\Box\alpha}$ (9.13)
- la *règle de la logique des propositions* (RLP)

(si $(\alpha_1\to(\alpha,\ \to\ldots\to(\alpha_n\to\beta))\ldots)$ est une tautologie modale, alors $\dfrac{\alpha_1\alpha_2\ldots\alpha_n}{\beta}$. (9.14)

Une *preuve modale de* φ, $\varphi\in\Omega(\Pi)$, est une suite de formules valides de $\Omega(\Pi):\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_p\equiv\varphi$ telle que, pour tout indice $i\in\{1,\ 2,\ \ldots p\}$, α_i soit ou bien l'une des formules (NE), (5), (déf. $\Diamond$), (K), (PL), ou bien une formule dérivée des α_k où $k<i$ selon l'une des règles d'inférence (RN) ou (RLP). La formule φ est alors un *théorème modal* et on note $\vdash\varphi$.

A titre d'exemple, démontrons que:

pour tout $\alpha\in\Omega(\Pi)$: $\quad\vdash\alpha\to(\Diamond\alpha)$,

on peut écrire successivement:

$\vdash\Box(\neg\alpha)\to(\neg\alpha)$ $\qquad$ (NE) appliqué à $(\neg\alpha)$

$\vdash(\Box(\neg\alpha)\to(\neg\alpha))\to(\alpha\to\neg(\Box(\neg\alpha)))$ $\qquad$ (PL)

$$\frac{\Box(\neg\alpha)\to(\neg\alpha)\quad(\Box(\neg\alpha)\to(\neg\alpha))\to(\alpha\to\neg(\Box(\neg\alpha)))}{\vdash\alpha\to\neg(\Box(\neg\alpha))}\quad (RLP) \tag{9.15}$$

$\vdash\neg(\Box(\neg\alpha))\leftrightarrow\Diamond\alpha$ $\qquad$ (déf. $\Diamond$) appliqué à α

$\vdash(\neg(\Box(\neg\alpha))\leftrightarrow\Diamond\alpha)\to(\neg(\Box(\neg\alpha))\to\Diamond\alpha)$ $\quad(PL)$

$$\frac{(\neg(\Box(\neg\alpha))\leftrightarrow\Diamond\alpha)\quad(\neg(\Box(\neg\alpha))\leftrightarrow\Diamond\alpha)\to(\neg(\Box(\neg\alpha))\to\Diamond\alpha)}{\vdash\neg(\Box(\neg\alpha))\to\Diamond\alpha}\qquad \begin{matrix}(RLP)\\(9.16)\end{matrix}$$

$\vdash(\alpha\to\neg(\Box(\neg\alpha)))\to((\neg(\Box(\neg\alpha))\to\Diamond\alpha)\to(\alpha\to\Diamond\alpha))$ $\quad(PL)\qquad(9.17)$

$\vdash\alpha\to\Diamond\alpha$ $\quad$ (RLP) appliqué à (9.15), (9.16) et (9.17)).

Ce théorème modal est connu sous la désignation scolastique: "*esse ad posse*", ce qui est est possible.

Nous n'avons donné aucune indication sur le choix des énoncés p_1, p_2, ... composant Π. On pourrait parfaitement partir d'un ensemble au plus dénombrable ***quelconque*** $\Pi=\{p_1, p_2, ...\}$, former l'ensemble $\Omega(\Pi)$ des formules modales sur Π selon les règles F_1), F_2), F_3), F_4), poser comme axiomes les formules (NE), (5), (déf. $\Diamond$), (K) et (PL) pour tous les $\alpha\in\Omega(\Pi)$ et enfin adopter la notion de preuve modale telle qu'elle découle des règles d'inférences (RN) et (RLP). Irving Lewis a appelé *système de logique modale (S5)* sur Π cette construction.

On peut prouver que le système ($S5$) que nous avons décrit initialement est *complet* en ce sens que toute formule modale valide α (testée sur les modèles de $\Omega(\Pi)$ est un théorème modal et réciproquement: autrement dit,

pour tout $\alpha\in\Omega(\Pi)$: $\quad\models\alpha\Leftrightarrow\vdash\alpha$

Le système ($S5$) constitue une *logique de la nécessité*. En changeant d'axiomes et de règles d'inférence, on peut construire d'autres systèmes logiques modaux. Certains de ces systèmes sont dits *déontiques*; ils fournissent une *logique du devoir*. Le symbole $\Box$ y est remplacé par O. Si α est une formule, (Oα) se lit "il est obligatoire que α" ou "α est obligatoire". Avec cette convention, $\neg(\mathrm{O}(\neg\alpha))$ peut se lire: "α est permis". Dans de tels systèmes, on peut poser des axiomes tels que:

$$((\mathrm{O}\alpha)\wedge(\mathrm{O}\beta))\to(\mathrm{O}(\alpha\wedge\beta))$$
$$(\mathrm{O}(\alpha\vee(\neg\alpha)))$$
$$\neg(\mathrm{O}(\alpha\wedge(\neg\alpha)))$$

et des règles d'inférence de la forme:

$$\frac{\alpha\to\beta}{\alpha\to\mathrm{O}\beta}$$

dont l'interprétation intuitive est évidente.

D'autres systèmes sont appelés *doxastiques* ou *logiques de l'opinion*. Le symbole $\Box$ est remplacé par C. Cα se lit: "on croit que α" ou "l'opinion est que α". Bien entendu les systèmes doxastiques ont leurs propres axiomes et leurs propres règles d'inférence. On peut aussi combiner les symboles $\Box$, O, C et introduire d'autres symboles. On peut former des logiques *épistémiques* (de la connaissance), *optatives* (du choix), *légales*, etc., presque à l'infini. Il est intéressant de noter que certains de ces systèmes possédent des propriétés de complétude ou de décidabilité.

Chapitre 10

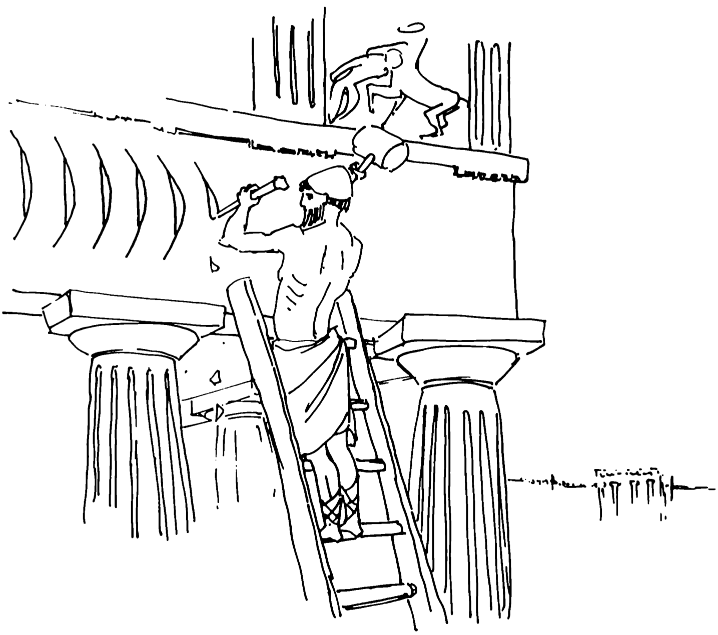
Epilogue

Nous voici parvenus au terme de cette incursion dans le domaine de la logique. Nous avons fait la part belle à la logique formelle, et particulièrement à celle du premier ordre. En procédant de la sorte, nous visions un double but.

D'une part, nous avons tenté de présenter quelques faits logiques non évidents. Le théorème de complétude de Gödel et quelques-unes des propositions qui gravitent autour de lui sont de ceux-là. Ils sont relativement faciles d'accès et pourtant ils débouchent sur des phénomènes qui excitent l'imagination et qui défient le "sens commun". A ceux qui voient dans la logique un tissu de banalités, nous espérons avoir donné matière à réflexion.

D'autre part, nous avons ébauché ici ou là quelques remarques touchant la langue courante et la logique ordinaire. La logique du premier ordre nous a servi en quelque sorte de référentiel. Par comparaison avec cette machinerie inflexible, les subtilités du discours naturel apparaissent plus clairement. Peut-être avons-nous ainsi fait entrevoir d'autres aspects de la logique.

Cette double visée nous a paru ménager une entrée possible dans le domaine si riche et si divers de la logique. D'où le titre de ce modeste ouvrage qui aurait atteint son but s'il incitait quelque lecteur à pousser plus loin ses réflexions et ses investigations.



Exercices

Chapitre 0

1. Mettre les argumentations suivantes sous forme de chaînes de syllogismes en faisant apparaître les hypothèses et les conclusions sous-entendues:

- Un losange est un parallélogramme. Mais certains losanges sont des carrés.
- Paul sera là dans cinq minutes; il a une bicyclette et il habite à moins d'un kilomètre d'ici.
- Voulez-vous m'acheter un billet de tombola?
  Merci, j'en ai déjà acheté un!

2. Etudier le paradoxe du barbier. Dans une forteresse isolée, occupée exclusivement par la totalité des hommes d'un régiment, un ordre a été affiché: "Après-demain vendredi, inspection générale du régiment. Tous les hommes seront rasés. Ceux qui ne se rasent pas eux-mêmes seront rasés par le barbier du régiment."

3. Etudier le passage suivant extrait de "Epiménide le menteur" de A. Koyré: "Car enfin, il semble clair qu'il y a toujours une chose que l'on ne peut pas mettre dans un sac, si grand soit-il, c'est le sac lui-même; en effet, le contenant doit toujours être plus grand que le contenu..."

Chapitre 1

4. On donne un langage du premier ordre L par:

$\mathrm{Cst}(L)=\{c, c'\}$, $\mathrm{Fct}(L)=\{f_2, f_3\}$, $\mathrm{Rel}(L)=\{R_2\}$.

Parmi les agrégats suivants, reconnaître ceux qui sont des termes et ceux qui sont des formules de L:

$x' \quad x'=c \quad f_2(x, x) \quad t_1$
$R_2(f_2(x, c), (x=x))$
$(f_3(c, x, R_2(c, x))=f_2(c, x)$
$((f_3(x, c', f_2(x, c'))=f_2(x, f_3(x, c', f_2(x, c'))))\leftrightarrow((R_2(x, f_2(x, c'))))$
$((\neg f_2(x, x))\vee(x=c) \qquad (\neg\forall x(x=f_2(x, c)))$
$f_2(f_3(f_2(f_3(x, f_2(x, x), c), c), f_2(x, x), c), c)$
$(\varphi\vee(\neg\varphi)) \qquad ((\forall x(f_2(x, x)=f_3(x, x, x)))\rightarrow(f_2=f_3))$
$(\forall x(\neg(c=c'))) \qquad (\forall x(\neg(x=x)))$.

5. Donner l'arbre de formation de chacune des formules suivantes:

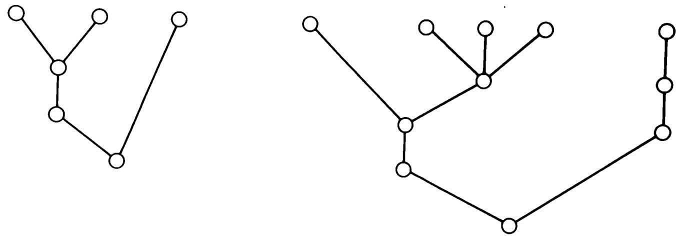
$(((x=c)\wedge(x'=c))\rightarrow(x=x'))$
$((\forall x(\forall x'(f_2(x, x)=f_2(c, c))))\leftrightarrow((x=c)\wedge(x'=c)))$
$(((\neg R_2(x, c))\vee(\neg R_2(c, x)))\rightarrow(\exists x(f_2(c, x)=f_2(x, c))))$
$(((\neg(f_2(x, c)=c))\wedge((x=c)\vee(c=x)))\rightarrow(\neg(f_2(c, c)=x)))$.

6. a) Définir la notion d'arbre de formation d'un terme d'un langage du premier ordre L.

b) Vérifier que les agrégats de symboles suivants sont des termes dans un langage du premier ordre approprié et donner leur arbre de formation.

$f_2(f_2(x, x), f_1(c)) \qquad x \qquad f_1(f_1(f_1(f_1(x))))$
$f_3(f_1(x), f_2(x, x), f_1(f_2(c, x)))$.

c) Former des termes admettant les arbres de formation suivants:



7. Donner l'ensemble des variables libres de chacune des formules suivantes:

- les deux premières formules de l'exercice 5
- $(\forall x((\exists x'(R_2(x, x') \to (x = x'))) \vee (x = c)))$
- $(((x = c) \vee (x = c')) \to (\forall x(c = c')))$
- $((\forall x(f_2(x, c) = x)) \vee (\exists x'((x = x') \wedge (\forall x(x = c)))))$.

8. Soit $A_1, A_2, \dots, A_p$, $p \in \mathbb{N}^*$, des agrégats de symboles, vides ou non. On dit que l'agrégat $A \equiv A_1 A_2 \dots A_p$ obtenu en juxtaposant dans l'ordre $A_1, A_2, \dots, A_p$ résulte de la *concaténation* de $A_1, A_2, \dots, A_p$. Si A résulte de la concaténation des agrégats non vides A_1 et A_2, A_1 est une section *commençante* propre de A et A_2 est une section *terminale* propre de A. A est une section commençante et terminale de lui-même.

Déterminer, parmi les agrégats suivants, ceux qui résultent de la concaténation de formules du premier ordre:

- $((x = c) \wedge (f_2(x, c) = f_2(c, x)))(\neg(c = c))(f_2(x, x) = f_1(x))$
- $((x = x') \wedge (y = c) \wedge (x' = c))(x = f_1(x))$
- $((\neg(x = c)) \wedge (x = x'))R_2(x, c)R_1(f_2(x, x))$
- $(x = x')((x' = x'') \wedge (x = x''))(x'' = c)((x' = c) \wedge (x'' = f_1(x)))$.

9. Considérons un langage M (non du premier ordre!) donné comme suit:
- symboles: a, b
- formules de M:
  - b est une formule de M

- Si F est une formule de M, Fb aussi
- Si F est une formule de M, aFa aussi
- Il n'y a pas d'autres formules de M que celles qui découlent des règles précédentes.

  Parmi les agrégats suivants, lesquels sont des formules de M:

  $bbbb \quad aaabaaba \quad ababa \quad aabbbababbb$

  $abaaba \quad \underbrace{aa...a}_{n}\underbrace{bb...b}_{m}\underbrace{aa...a}_{p} \quad \underbrace{aa...a}_{n}b\underbrace{aa...a}_{m}b\underbrace{aa...a}_{p}$?

10. Soit L un langage du premier ordre comportant un symbole de constante c. Soit α une formule de L. L'agrégat de symboles obtenu en remplaçant chaque occurrence de c dans α par le symbole de variable x est encore une formule de L.

Montrer qu'en général cette conclusion est fausse lorsqu'on remplace chaque occurrence de x par c.

11. La "notation polonaise" obéit aux règles suivantes:

- $\neg$ concerne la plus courte séquence de symboles qui le suit et qui constitue une formule, même règle pour $\forall x$ et $\exists x$, où x est un symbole de variable.
- $\wedge$ concerne la plus courte séquence de symboles qui le suit et qui résulte de la concaténation de deux formules; même règle pour $\vee$, $\rightarrow$ et $\leftrightarrow$.

Transcrire les formules du premier ordre suivantes dans la "notation polonaise":

- $((R_2(x, c) \wedge (\neg(x=c))) \rightarrow R_2(c, x))$
- $(f_2(f_2(x, c), f_2(c, x))=x)$
- $(((x=x') \wedge (x'=x'')) \wedge (x=x''))$
- $(\forall x(f_2(x, x)=c))$
- $((\forall x R_2(x, c)) \vee (\neg(\exists x R_2(x, c))))$
- $(((R_2(x, x') \vee R_2(x', x'')) \vee R_2(x, x'')) \rightarrow (R_2(x, x') \vee (R_2(x', x'') \vee R_2(x, x''))))$

Vérifier qu'on peut retrouver les formules initiales à partir des expressions polonaises obtenues.

12. Dans la notation polonaise, le terme dont l'expression ordinaire est $f_n(t_1, \ldots, t_n)$ s'écrit $f_n t_1 \ldots t_n$. Dans tout agrégat $A \equiv S_1 S_2 \ldots S_n$ ne comportant que des symboles de constantes, de variables et de fonctions, posons:

$z(S_k) := 1$ si S_k est un symbole de constante ou de variable;

$z(S_k) := 1-n$ si S_k est un symbole de fonction n-aire;

$z(S_1 S_2 \ldots S_m) := z(S_1) + z(S_2) + \ldots + z(S_m)$.

- Vérifier que si A résulte de la concaténation de $A_1, A_2, \ldots, A_p$, alors $z(A) = z(A_1) + z(A_2) + \ldots + z(A_p)$.
- Montrer que, pour tout terme t écrit dans la notation polonaise, $z(t) = 1$.
- Montrer que, dans la notation polonaise, toute section terminale d'un terme est une concaténation de termes; qu'aucune section commençante propre n'est une concaténation de termes.
- Soit un terme t écrit dans la notation polonaise et supposons que

$t \equiv f_n t_1 \ldots t_n \equiv f'_p t'_1 \ldots t'_p$, où f_n, f'_p sont des symboles de fonctions, $t_1, \ldots, t_n$, $t'_1, \ldots, t'_p$ des abréviations pour des termes. Montrer que:

$$f_n \equiv f'_p \quad ; \quad n = p \quad ; \quad t_1 \equiv t'_1, \ldots, t_n \equiv t'_n.$$

En déduire un théorème d'unique lisibilité pour les termes dans la notation polonaise.

13. En s'inspirant de l'exercice précédent, établir un théorème d'unique lisibilité des formules dans la notation polonaise.
Indication: on suggère de poser:

$$z(\neg) := 0$$
$$z(=) = z(\wedge) = z(\vee) = z(\rightarrow) = z(\leftrightarrow) = z(\forall) = z(\exists) := -1$$
$$z(R_n) := 1 - n.$$

14. Considérons un langage du premier ordre L donné par:

$$\mathrm{Cst}(L) = \{c\} \quad ; \quad \mathrm{Fct}(L) = \{f''\} \quad ; \quad \mathrm{Rel}(L) = \emptyset.$$

Le symbole f'' est mis pour f_2^0 et désigne une fonction binaire, numéro 0. Les symboles de variables sont notés x, x', x'', ... On peut donc écrire toute formule de L avec les quinze signes:

(*) $\quad \neg \quad \wedge \quad \vee \quad \rightarrow \quad \leftrightarrow \quad = \quad c \quad x \quad f \quad (\quad) \quad , \quad ' \quad \exists \quad \forall.$

Donner un *ordre lexicographique* sur For(L) en admettant que si $\alpha, \beta \in \mathrm{For}(L)$:

- α précède β si le nombre de signes de α est inférieur à celui des signes de β.
- α et β sont ordonnées selon l'ordre alphabétique donné par (*) lorsqu'elles ont le même nombre de signes.

Ecrire les dix premières formules de L selon cet ordre.

Chapitre 2

15. Effectuer les vérifications indiquées aux exemples 2.2.24 et 2.2.25.

16. On considère le langage L_2 donné par:

$$\mathrm{Cst}(L_2) = \{c\} \quad ; \quad \mathrm{Fct}(L_2) = \{f_2\} \quad ; \quad \mathrm{Rel}(L_2) = \{R_2\}.$$

Soit $E_1 = \{u, v, w\}$ un ensemble de trois éléments.
Dénombrer les L_2-structures de la forme (E_1, J), où J est une interprétation dans E_1.

17. Reprendre le langage L_2 de l'exercice précédent.
Soit $E_2 = \{0, 1, 2, 3, \ldots\}$. Soit J_2 l'interprétation dans E_2 donnée par:

$J_2(c) = 0$

$J_2(f_2)$: $\quad E_2 \times E_2 \rightarrow E_2$

$\qquad (a, b) \mapsto$ maximum de a et b

$J_2(R_2)$: $\quad \{(a, b) \in E_2 \times E_2 \mid a$ divise $b\}$.

Soit s_2 la spécialisation de J_2 donnée par:

$$s_2(x)=0,\ s_2(x')=1,\ s_2(x'')=2,\ \ldots$$

i) Déterminer les images par s_2 des termes suivants:
c ; $f_2(c, x')$; $f_2(f_2(x, x'), f_2(c, x))$;
$f_2(f_2(f_2(x''', x''), x'), x)$.

ii) Parmi les formules suivantes, quelles sont celles qui sont satisfaites par (E_2, J_2) pour s_2:
$(c=x)$; $(x''=f_2(c, x'))$; $R_2(x', f_2(x', x''))$;
$((\neg R_2(f_2(x'', c), x'')) \wedge (f_2(c, c)=x))$.
$(((x=x') \vee (c=x)) \rightarrow (f_2(x, x)=x'))$
$(\forall x R_2(x, x'))$; $(\exists x(f_2(x, x')=c))$
$(\exists x(\forall x'(R_2(x, x') \leftrightarrow R_2(x', x))))$.

18. Considérons le langage L_2 de l'exercice 16 (voir aussi exemples 2.2.3, 2.2.24 et 2.2.25) et, dans L_2, les énoncés:

$$\psi_3 \equiv (\forall x(\forall x'(R_2(x, x') \vee R_2(x', x))))$$
$$\theta \equiv ((\forall x(\forall x'(f_2(x, x')=f_2(x', x)))) \wedge (\forall x(\forall x'(\forall x''(R_2(x, x') \rightarrow R_2(f_2(x, x''), f_2(x', x''))))))).$$

Un modèle de $S=\{\varphi_1, \varphi_2, \varphi_3, \psi_1, \psi_2, \psi_3, \theta\}$, où $\varphi_1, \varphi_2, \varphi_3$ sont les énoncés de l'exemple 2.2.24, ψ_1 et ψ_2 les énoncés de l'exemple 2.2.25, est appelé *groupe commutatif ordonné*.

i) Montrer que (E_3, J_3) de l'exemple 2.2.24 n'est pas un groupe commutatif ordonné.

ii) Trouver un modèle de S.

19. Soit (E, J) une L-structure et s une spécialisation de (E, J). Soit $\varphi \in \mathrm{For}(L)$. Montrer que, si x et x' sont des symboles de variables:

$$(E, J) \models ((\forall x(\forall x'\varphi)) \leftrightarrow (\forall x'(\forall x\varphi)))[s]$$

20. Soit (E, J) une L-structure et s une spécialisation de (E, J). Soit α, β deux formules de L.

a) Montrer que $(E, J) \models (\alpha \vee (\neg\alpha))[s]$.

b) Montrer que, si $(E, J) \models (\alpha \rightarrow \beta)[s]$ *et* $(E, J) \models \alpha[s]$, alors $(E, J) \models \beta[s]$.

c) Montrer que $(E, J) \models ((\alpha \wedge (\neg\alpha)) \rightarrow \beta)[s]$.

21. Dans le plan de la géométrie élémentaire, on considère la propriété pour trois points d'être alignés (c'est-à-dire d'appartenir à une même droite). Trouver un langage du premier ordre L et des énoncés dans L permettant de décrire formellement cette situation.

22. Donner un langage du premier ordre L propre à décrire une communauté humaine (famille, tribu, etc.) où on distingue le sexe de chaque individu, les relations d'époux, de parents à enfants et éventuellement d'autres (ancienneté, etc.).

Décrire d'une manière détaillée des exemples de L-structures finies.

Trouver des énoncés dans L qui sont satisfaits naturellement dans toute L-structure donnée par une communauté à un moment fixé. Essayer de caractériser formellement la monogamie, la polygamie, le fait que x et y ont le droit de se marier, etc.

Chapitre 3

23. Dresser les tables de vérité des fonctions propositionnelles suivantes en fonction des valeurs de vérité des formes propositionnelles A, B, C:

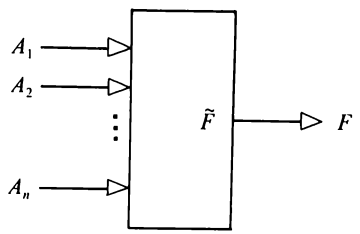
- $((((A\to B)\to A)\to A)\to B)$
- $(A\to((\neg A)\to A))$
- $((A\wedge(\neg B))\vee B)$
- $((A\wedge B)\to(B\wedge C)$

24. a) Dénombrer les fonctions n-aires à arguments et valeurs dans $\mathbb{F}_2=\{0, 1\}$.
b) Dresser les tables des fonctions unaires à arguments et valeurs dans $\mathbb{F}_2$. Pour chaque table, trouver une forme propositionnelle dépendant d'une formule première A et admettant cette table de valeurs.
c) Même question pour les fonctions binaires de $\mathbb{F}_2^2$ dans $\mathbb{F}_2$.
d) Choisir une fonction $f\colon \mathbb{F}_2^3\to\mathbb{F}_2$. Essayer de trouver une forme propositionnelle dépendant de trois formules premières A, B, C, correspondant à f.
e) Que peut-on dire de deux formes propositionnelles dépendant des mêmes formules premières et déterminant la même fonction à arguments et valeurs dans $\mathbb{F}_2$?
Comment peut-on en construire?

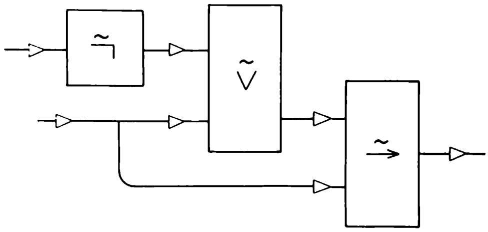
25. Soit E un ensemble non vide. A toute forme propositionnelle $F\in\Phi(E)$ comportant les éléments $A_1, A_2, \dots, A_n$ de E, on peut attacher une fonction n-aire, dite "de Boole":

$$\tilde{F}:(0, 1\}^n\to\{0, 1),$$

déterminée comme suit: soit $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$ un n-uple d'éléments de $\{0, 1\}$, $\tilde{F}(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$ est la valeur de $V(F)$ pour toute fonction de vérité V telle que $V(A_i)=\varepsilon_i$, $i=1, 2, \dots, n$. La fonction $\tilde{F}$ peut être schématisée par une "boîte noire":



Aux entrées marquées A_1, A_2, ... , A_n, on peut inscrire les valeurs ε_1, ε_2, ... , ε_n respectivement, et à la sortie, la valeur correspondante de $\tilde{F}$. On peut considérer des boîtes noires élémentaires relatives aux connecteurs $\neg$, $\wedge$, $\vee$, $\rightarrow$ et $\leftrightarrow$, notées respectivement $\tilde{\neg}$, $\tilde{\wedge}$, $\tilde{\vee}$, $\tilde{\rightarrow}$ et $\tilde{\leftrightarrow}$. On peut combiner ces boîtes conformément aux nombres de leurs entrées:



est un schéma donnant une décomposition de la boîte $\tilde{F}$ lorsque $F \equiv (((\neg A) \vee B) \rightarrow B)$ à l'aide de $\tilde{\neg}$, $\tilde{\vee}$ et $\tilde{\rightarrow}$.

- Donner des schémas relatifs à:
  $(((A \rightarrow B) \rightarrow (A \wedge B)) \rightarrow B)$
  $(((A \rightarrow (\neg B)) \vee (A \wedge C)) \rightarrow (A \vee C))$
- Montrer qu'on peut décomposer toute boîte noire en boîtes noires élémentaires $\tilde{\neg}$ et $\tilde{\wedge}$.
- Montrer qu'on ne peut pas faire l'économie de la boîte noire élémentaire $\tilde{\neg}$.

Note: Les schémas considérés peuvent être matérialisés par des montages électriques ou pneumatiques; on peut ainsi réaliser des machines à calcul propositionnel.

Chapitre 4

26. Montrer que dans toute L-structure (E, J)

$$(E, J) \models (\forall x (\forall x' (\forall x'' (\forall x''' (((x = x') \wedge ((x' = x'') \wedge (x'' = x'''))) \leftrightarrow (((x = x') \wedge (x' = x'')) \wedge (x'' = x''')))))).$$

27. Dans l'ensemble des droites du plan de la géométrie ordinaire, on considère la relation de parallélisme notée $\|$, exprimant que deux droites ont la même direction. On y introduit en outre la relation de perpendicularité notée $\perp$.

Introduire un langage du premier ordre L et des énoncés dans L permettant de décrire formellement cette situation. On notera $(x \| y)$ au lieu de $\|(x, y)$ et $(x \perp y)$ au lieu de $\perp(x, y)$. Montrer que dans cette interprétation, les formules obtenues en remplaçant le symbole $=$ par $\|$ dans les axiomes ơe l'égalité sont satisfaites. Peut-on en dire autant de $\perp$?

28. Dans l'ensemble $\mathbb{R}$ des nombres réels, considérons comme *indiscernables* deux nombres a et b tels que $|a-b| < 10^{-9}$. Nous noterons alors $a \approx b$.

Transcrire les axiomes de Leibniz en y substituant un symbole de relation binaire R_2 au symbole $=$. Montrer que $\mathbb{R}$ muni de la relation $\approx$ ne vérifie qu'une partie des axiomes ainsi obtenus.

A l'aide de R_2, écrire des axiomes dont $\mathbb{R}$ muni de la relation $\approx$ soit un modèle et qui ne soient pas satisfaits par $\mathbb{R}$ muni de l'égalité.

Chapitre 5

29. Au cours de la démonstration de la proposition 5.3.4, on a montré que l'axiome de Henkin $H_2(\varphi)$ n'est qu'une paraphrase de l'axiome $H_1(\neg\varphi)$. Découvrir et établir une parenté analogue entre les axiomes des quantificateurs d'un langage L (cf. déf. 5.3.0).

30. Appelons *pavage du plan* la donnée d'une famille dénombrable de régions polygonales dont les intérieurs sont d'un seul tenant, appelées *contrées*, telles que:

- tout point du plan appartienne à une contrée au moins;
- tout point intérieur à une contrée n'appartienne qu'à cette seule contrée.

Deux contrées sont dites *adjacentes* lorsqu'elles sont distinctes et qu'elles ont au moins un segment de droite en commun.

a) Décrire quelques pavages du plan. En montrer un, tel qu'il existe un point du plan appartenant à une infinité de contrées.

b) Soit $P = \{c_0, c_1, c_2, \ldots, c_p, \ldots\}$ un pavage du plan, c_i, $i = 1, 2, \ldots, p, \ldots$ étant les contrées de ce pavage. Trouver un langage du premier ordre L et des axiomes S dont P soit un modèle; on introduira un symbole de relation binaire R_2 traduisant formellement l'adjacence des contrées.

c) On dit qu'on peut *colorier le pavage P avec n couleurs* $T_1, T_2, \ldots, T_n$ lorsqu'on peut attribuer à chaque contrée une couleur unique prise dans $\{T_1, T_2, \ldots, T_n\}$, de manière que deux contrées adjacentes aient des couleurs différentes.

Considérons le langage L' obtenu en adjoignant à L:

- les symboles de constantes $c_0, c_1, c_2, \ldots, c_p, \ldots$
- n symboles de relations unaires $R_1^1, R_1^2, \ldots, R_1^n$.

Supposons qu'on ait réussi à colorier le pavage P avec n couleurs. Montrer que le pavage colorié P est un modèle d'un système S' d'énoncés sans quantificateurs dans L' traduisant:

i) les incidences des contrées de P
ii) le fait que chaque contrée a l'une des n couleurs
iii) le fait que les contrées adjacentes ont des couleurs différentes.

d) Montrer que si toute partie finie de P peut être coloriée avec n couleurs, il en est de même de P.

e) Montrer qu'on peut immédiatement étendre ce résultat à d'autres situations que les pavages du plan.

Note: Ce résultat joue un rôle dans le problème dit "des quatre couleurs".

Chapitre 6

31. Soit (L, S) un système formel et α, β, γ des énoncés de L. Etablir les règles d'inférence suivantes:

a) $S \cup \{\alpha, \beta\} \vdash \gamma \quad \Rightarrow S \cup \{\alpha \wedge \beta\} \vdash \gamma$
b) $(S \vdash \alpha \text{ et } S \vdash \beta) \quad \Rightarrow S \vdash (\alpha \wedge \beta)$
c) $(S \cup \{\alpha\} \vdash \gamma \text{ et } S \cup \{\beta\} \vdash \gamma) \quad \Rightarrow S \cup \{\alpha \vee \beta\} \vdash \gamma$
d) $(S \vdash \alpha \text{ ou } S \vdash \beta) \quad \Rightarrow S \vdash \alpha \vee \beta$
e) $S \cup \{\alpha\} \vdash \beta \quad \Rightarrow S \vdash (\neg \alpha) \vee \beta$
f) $S \vdash \alpha \vee \beta \quad \Rightarrow S \cup (\neg \alpha) \vdash \beta$
g) $(S \vdash (\alpha \vee \beta) \text{ et } S \cup \{\gamma\} \vdash \alpha) \Rightarrow S \cup \{\beta \rightarrow \gamma\} \vdash \alpha$
h) $S \cup \{\beta\} \vdash \alpha \quad \Rightarrow S \vdash (\beta \rightarrow \alpha)$.

Trouver celles d'entre elles qui admettent une réciproque.

32. Soit (L, S) une théorie du premier ordre. Soit d un symbole de constante n'apparaissant dans aucun énoncé de S. Soit φ une formule de L.
Montrer que, si $S \vdash \varphi$, alors:

$$S \vdash \forall x(\varphi_x^d)$$

où x est un symbole de variable n'apparaissant pas dans φ et où φ_x^d est la formule obtenue en remplaçant, dans φ, le symbole d par x (cf. exercice 10).

Interpréter le résultat obtenu.

33. On parle en mathématiques de "condition nécessaire", de "condition suffisante", de "condition nécessaire et suffisante".

Préciser le sens de ces expressions dans une théorie du premier ordre.

34. Une théorie (L, S) du premier ordre est dite *complète* si, pour tout énoncé α de L, on a soit $S \vdash \alpha$, soit $S \vdash (\neg \alpha)$ (cf. déf. 8.4.1).

Deux modèles (E, J) et (E', J') d'une théorie (L, S) du premier ordre sont dits *élémentairement équivalents* lorsque tout énoncé de L satisfait dans (E, J) l'est aussi dans (E', J'), et réciproquement.

Montrer que les conditions suivantes sont équivalentes:

- (L, S) est une théorie complète.
- Deux modèles quelconques de (L, S) sont élémentairement équivalents.
- L'ensemble des théorèmes de (L, S) coïncide avec l'ensemble des énoncés de L satisfaits dans un modèle de (L, S).

Donner un exemple de théorie complète et trouver quelques théorèmes non banals (i.e. qui ne soient pas des axiomes de la théorie).

35. Une théorie du premier ordre (L, S) est dite *axiomatisable de manière finie* – *AMF* – lorsque l'ensemble de ses théorèmes coïncide avec celui d'une théorie

(L, T) où T est un ensemble fini d'énoncés.

- Montrer que si (L, S) est AMF, on peut s'arranger pour que ses axiomes non-logiques se réduisent à un énoncé au plus.
- Montrer que si (L, S) est AMF, il existe une partie finie $S_0 \subset S$ telle que (L, S) et (L, S_0) aient les mêmes théorèmes.

36. Soit L un langage du premier ordre. Une formule $\varphi \in \mathrm{For}(L)$ est dite *logiquement valide* lorsque: $\emptyset \vdash \varphi$ (i.e. il existe une preuve de φ à partir de l'ensemble vide d'énoncés non-logiques de L). Deux formules α et β de L sont dites *logiquement équivalentes* si $\alpha \leftrightarrow \beta$ est logiquement valide. On note alors $\alpha \mathrel{\vDash\!\!\!\!\dashv} \beta$.

a) Montrer que les trois conditions suivantes sont équivalentes:

- $\alpha \mathrel{\vDash\!\!\!\!\dashv} \beta$
- pour toute L-structure (E, J) et toute spécialisation s de (E, J):
  $(E, J) \vDash \alpha[s] \Leftrightarrow (E, J) \vDash \beta[s]$
- pour toute L-structure (E, J) et toute spécialisation s de (E, J):
  $(E, J) \vDash (\alpha \leftrightarrow \beta)[s]$.

b) Donner quelques exemples de paires de formules logiquement équivalentes dans un langage du premier ordre qu'on choisira.

c) Montrer que si le symbole de variable y est substituable au symbole de variable x dans la formule φ de L:
$(\forall x \varphi) \mathrel{\vDash\!\!\!\!\dashv} (\forall y \varphi^x_y)$.

37. (suite de l'exercice 36)
Montrer que, quelles que soient $\alpha, \beta \in \mathrm{For}(L)$ et $x \in \mathrm{Var}$:

1) $\alpha \mathrel{\vDash\!\!\!\!\dashv} \beta \Leftrightarrow (\neg\alpha) \mathrel{\vDash\!\!\!\!\dashv} (\neg\beta)$
2) $\alpha \mathrel{\vDash\!\!\!\!\dashv} \beta \Leftrightarrow (\forall x\alpha) \mathrel{\vDash\!\!\!\!\dashv} (\forall x\beta)$
3) $(\neg(\forall x\alpha)) \mathrel{\vDash\!\!\!\!\dashv} (\exists x(\neg\alpha))$
4) $(\neg(\exists x\alpha)) \mathrel{\vDash\!\!\!\!\dashv} (\forall x(\neg\alpha))$
5) $(\forall x(\alpha \wedge \beta)) \mathrel{\vDash\!\!\!\!\dashv} ((\forall x\alpha) \wedge (\forall x\beta))$
6) $(\exists x(\alpha \vee \beta)) \mathrel{\vDash\!\!\!\!\dashv} ((\exists x\alpha) \vee (\exists x\beta))$

Si, en outre, $x \notin VL(\alpha)$

7) $(\alpha \to (\forall x\beta)) \mathrel{\vDash\!\!\!\!\dashv} (\forall x(\alpha \to \beta))$
8) $(\alpha \to (\exists x\beta)) \mathrel{\vDash\!\!\!\!\dashv} (\exists x(\alpha \to \beta))$
9) $(\alpha \wedge (\exists x\beta)) \mathrel{\vDash\!\!\!\!\dashv} (\exists x(\alpha \wedge \beta))$
10) $(\alpha \vee (\forall x\beta)) \mathrel{\vDash\!\!\!\!\dashv} (\forall x(\alpha \vee \beta))$
11) $((\forall x\beta) \to \alpha) \mathrel{\vDash\!\!\!\!\dashv} (\exists x(\beta \to \alpha))$
12) $((\exists x\beta) \to \alpha) \mathrel{\vDash\!\!\!\!\dashv} (\forall x(\beta \to \alpha))$.

38. (Suite des exercices 36 et 37)
Une formule de L est dite *prénexe* lorsqu'elle est de la forme:

$$(Q_1(Q_2(\dots \quad (Q_p\alpha)\dots))),$$

où α est une formule sans quantificateur et où Q_i $(i=1, 2, \ldots, p)$ est un agrégat du type $\forall x_i$ ou $\exists x_i$, x_i étant un symbole de variable.
Montrer que toute formule φ de L est logiquement équivalente à une formule prénexe.

Indication: procéder par récurrence sur le nombre de quantificateurs dans φ et utiliser les résultats des deux exercices précédents.
Donner des formules prénexes logiquement équivalentes aux formules suivantes:

$$(\exists x(R_2(x, y)) \wedge (\neg(\forall y R_2(y, x))))$$
$$(\forall x((f_1(x)=x) \wedge (\exists y R_2(x, y))))$$
$$(((\exists x R_2(x, y)) \vee (\exists y R_2(y, x))) \rightarrow (\forall x R_2(x, x))).$$

39. Soit (L, S) une théorie du premier ordre.

a) S est dit *libre* si, pour tout $\alpha \in S$, il est faux que $(S-\{\alpha\}) \vdash \alpha$:
Montrer que la condition nécessaire et suffisante pour que S soit libre est que toute partie finie de S soit libre.

b) Un ensemble S' d'énoncés de L est *équivalent* à S si, quels que soient $\alpha \in S$ et $\alpha' \in S'$,
$S \vdash \alpha'$ *et* $S' \vdash \alpha$.
Montrer que pour tout énoncé φ de L:
$S \vdash \varphi \Leftrightarrow S' \vdash \varphi$.

c) Montrer que, si S est fini, il existe dans S une partie S_0, libre et équivalente à S. Examiner le cas où S est dénombrable.

Chapitre 7

40. Existe-t-il des ensembles totalement ordonnés de cardinal infini arbitraire?

Chapitre 8

41. Montrer que dans (L_n, S_n), $\forall x \forall y\ x \cdot y = y \cdot x$ n'admet pas de preuve à partir des seuls axiomes A_1, A_2, A_3, A_4 et A_5.

Donner dans (L_n, S_n) une preuve de $\forall x \forall y\ x \cdot y = y \cdot x$

42. Donner une preuve de $\forall x(\neg(x+1=x))$ dans (L_n, S_n).

43. A partir du système formel (L_e, S_e) pour les ensembles, montrer que:

- quels que soient les ensembles x et y, la paire $\{x, y\}$ est bien déterminée;
- quels que soient les ensembles x et y, il existe exactement un ensemble réunion $x \cup y$;
- si le couple (x, y) égale le couple (x', y'), alors $x = x'$ et $y = y'$.

44. On considère les systèmes d'équations définies sur les numéraux:

1) $\begin{cases} f(x, 0)=1 \\ f(x, y+1)=f(x, y) \cdot x \end{cases}$

2) $\begin{cases} f(0)=0 \\ g(0)=0 \\ g(x+1)=f(x)+1 \\ f(x+1)=f(x) \cdot g(x) \end{cases}$

3) $\begin{cases} f(x, 0)=x \\ f(x, y) \cdot f(y, x)=0 \\ f(x+1, y+1)=f(x, y) \end{cases}$

4) $\begin{cases} f(x, 0)=x+1 \\ f(0, y+1)=y+1 \\ f(x+1, y+1)=f(x, f(x+1, y)) \end{cases}$

5) $\begin{cases} f(0, 0)=0 \\ f(x+1, y)=f(x, y)+1 \\ f(x, y+1)=f(y, y). \end{cases}$

- Dans chaque cas, déduire quelques valeurs de f, le cas échéant de f et de g.
- Montrer que 5) ne détermine pas une fonction.
- Essayer de reconnaître les fonctions récursives déterminées par 2) et 3).

45. On considère le groupe G présenté par

$< x, y | x^2, y^3, xyx^{-1}y^{-1} >$

a) Reconnaître l'élément de G donné par le mot $xyxyxyxyxyxy$
b) Donner une théorie du premier ordre caractérisant G. Montrer qu'elle est complète (cf. exercice 34).

46. Montrer que $< x, y | xyxy^{-1}x^{-1}y^{-1} >$ et $< x, y | x^2y^{-3} >$ sont des présentations de deux groupes isomorphes.

47. Illustrer par des exemples les observations de R. Thom sur le comportement sémantique des conjonctions "et" et "ou". Etudier la pseudo-conjonction "et/ou" qu'emploient certains auteurs.

48. Réfléchir sur le *paradoxe de K. Jaakko J. Hintikka*:

si faire Y est immoral
et si faire X sans faire Y est impossible.
Alors faire X est immoral.

Si faire Y est immoral et si faire X est impossible
alors faire X sans faire Y est impossible.
Donc faire X est immoral.

Par suite, toute action impossible est immorale.

49. Prendre le langage du premier ordre L_e de la théorie des ensembles; y adjoindre un symbole de relation binaire $\leqq$. Ecrire dans L_e une formule exprimant que $\leqq$ est un bon ordre sur un ensemble x.

50. Ecrire les axiomes des groupes sans torsion dans un langage approprié de $\mathbb{N}$-Logique. Employer des notions simplifiées: x, y, ... pour les éléments des groupes, n, n', ... pour les nombres naturels, xy pour le produit de x et y dans un groupe, x^n pour la n-ième puissance de x dans un groupe, etc.

Chapitre 9

51. Ecrire un système formel du deuxième ordre décrivant les nombres réels. Ne pas oublier l'axiome de la borne supérieure!

52. a) Montrer qu'en logique intuitionniste, pour toute formule α et β: $(\alpha \wedge (\neg \alpha)) \vdash \beta$.
Cette expression est parfois appelée *principe de contradiction.*

b) En revanche, la logique intuitionniste rejette le *principe du tiers exclu*: $\neg \alpha$ et $\neg \neg \alpha$ ne sont pas exclusifs l'un de l'autre. Montrer que cela équivaut à admettre qu'il est possible que $\alpha \vee (\neg \alpha)$ ne soit pas satisfait. Montrer que cela a pour conséquence de rejeter la validité logique de $(\forall x \varphi) \vee (\exists x (\neg \varphi))$, φ étant une formule.

53. Construire quelques tautologies modales.

54. Ce qui est nécessaire est-il possible?

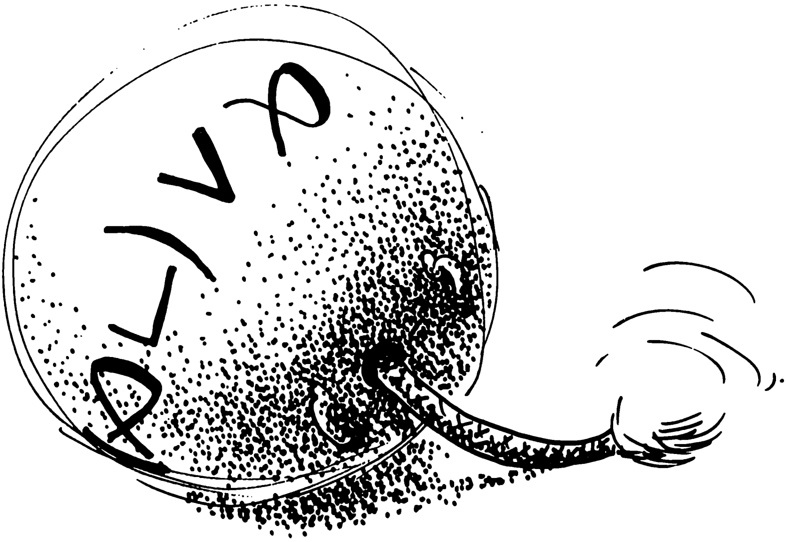
55. Trouver les formules valides du système modal S_5 dans la liste suivante

$\models \quad \Box\Box\alpha \rightarrow \alpha$

$\models \quad \Diamond\alpha \rightarrow \alpha$

$\models \quad (\Diamond(\alpha \rightarrow \beta)) \rightarrow (\Diamond\alpha \rightarrow \Diamond\beta)$

$\models \quad \Box\alpha \rightarrow \Box\Box\Box\alpha$



Index terminologique

Les références sont celles des pages

analyse non standard 154
application 32
– bijective 46
– injective 46
– surjective 46
arbre
– de composition 53
– de formation 21
argument d'une application 32
aspect syntaxique et sémantique 29
axiome
– du bon ordre 113
– du choix 113, 133
– de l'égalité 66
– de l'ensemble des parties 133
– de l'ensemble vide 132
– d'extensionnalité 132
– des groupes 81
– de Henkin 74
– de l'infini 132
– logique 90
– des paires 132
– des quantificateurs 74
– de régularité 133
– de la réunion 132
– de spécification 90

bijection 46

cardinal 111
– d'un langage du premier ordre 115
concaténation 184
connecteur 17
constantes 66
– de Henkin 73
composante première 53
correspondance biunivoque 46

dérivabilité de φ à partir de S 91

élément d'un ensemble 30
énoncé 25
ensemble 30, 131
– bien ordonné 33, 46
– dénombrable 46
– *s* disjoints 32
– fini 46
– héréditairement fini 162
– ordonné 44
– vide 31

extension 75
– de Henkin 73

fonction 32, 66
– binaire 32
– de Boole 188
– calculable 143
– *n*-aire 32
– numérale 145
– récursive (générale) 143
– unaire 32
– de vérité 54
forme propositionnelle 52
formule 19
– atomique 19
– de Leibniz 66
– logiquement équivalente 192
– logiquement valide 192
– modale valide 177
– première 52

graphe d'une application 32
groupe 43
– abélien libre 151
– commutatif ordonné 187
– libre 151
– avec torsion 82
– sans torsion 82, 157

hauteur d'une constante de Henkin 73
hypothèse du continu 168

induction
– complète 49, 123, 144
– transfinie 114
interprétation 35
intersection 32

langage
– du premier ordre 14, 17
– polytypique 160
lemme
– de rectitude 96
– de réduction à la logique des propositions 76
logique
– faible du second ordre 162, 164
– intuitionniste 172
– modale 175
– du premier ordre des prédicats 21

– des propositions 51
– du second ordre 165
– $\mathbb{N}$-logique 159
– ω-logique 161
lois de De Morgan 57, 58
longueur d'une preuve 96
LP-consistance 59
– finie 60
L-structure 35
– canonique 76

modèle 43
– élémentairement équivalent 191
– isomorphe 120
"*modus ponens*" 90
monde 176
– L-Σ-monde 176
mot 150

nombre de Gödel 143
notation polonaise 28, 185
n-uple 31
numéral 129

ordre 33
– bon 33
– total 33

pavage du plan 190
preuve 91
principe de contradiction 195
– de contraposition 58
– de double négation 58
– de non-contradiction 58
– du tiers exclu 58
produit cartésien 31
programme de Hilbert 155

quantificateur 17

récurrence 20, 49, 56, 123
règles
– de contraposition 92
– de généralisation 91
– d'inférence 90
– d'inférence modale 179
relation 33, 66
– *n*-aire 33
– unaire 33
restriction d'une application 32
réunion 31, 32

satisfaction par (E, J) d'une formule 38
schéma d'axiomes
– de l'induction complète 123
– de remplacement 133
section
– commençante 23, 184
– terminale 184
spécialisation 37, 160, 166
sous-ensemble 31
sous-modèle 128
– propre 128
substitution 70
symbole
– de constante 17
– de fonction 18
– d'un langage du premier ordre 17
– logique 17
– de ponctuation 17
– de relation 18
– de variable 17
– de variable libre 25
système formel 104
– pour l'arithmétique 122
– consistant 104
– pour les ensembles 131
– récursif 147
– de Zermelo-Fraenkel 131
système d'inférence 90
– de Hilbert 90

tautologie 56
– modale 176
terme 18, 160
– clos 71
théorème 104
– de Cantor 112
– de Cantor – Bernstein 112
– de compacité de la logique des propositions 60
– de compacité de la logique du premier ordre 80
– de complétude 100
– de déduction 107
– d'incomplétude 142, 146
– d'incomplétude généralisé 147
– de Löwenheim-Skolem 81
– de Löwenheim-Skolem, cas général 118
– de Löwenheim-Skolem-Tarski 118
– modal 179
– de la preuve par l'absurde 107
théorie 104
– complète 141, 191
– incomplète 141
thèse de Hilbert 153
torsion 82

union 31, 32

valeur d'une application 32
variable 66
– libre 25

Index des notations

Les références sont celles des pages

$\neg$ 17
$\wedge$ 17
$\vee$ 17
$=$ 17, 31
$\rightarrow$ 17
$\leftrightarrow$ 17
$\forall$ 17
$\exists$ 17
Var 17
x 17
Cst(L) 17
c 17
Fct(L) 18
f_n 18
Rel(L) 18
R_m 18
Ter(L) 18
For(L) 19
$P(T, p)$ 22
$\equiv$ 25
$VL(\varphi)$ 25
$\in$ 31
$\notin$ 31
$\subset$ 31
$\emptyset$ 31
$E \times F$ 31
E^n 31
$E \cup F$ 31
$\bigcup_n E_n$ 32
$E \cap F$ 32
$\bigcap_n E_n$ 32
$E - F$ 32
$f: E \rightarrow F$
$x \mapsto f(x)$ 32
$f(x)$ 32
$f|_A$ 32
Δ 33
$\Rightarrow$ 34
$\Leftrightarrow$ 34
(E, J) 35
J 35
$\tilde{c}$ 35
$\tilde{f}_n$ 35
$\tilde{R}_m$ 35
s 37
$t(s)$ 38
$s(\frac{x}{a})$ 38
$\models$ 38
For(n, L) 49
$P(L)$ 52
$\Phi(E)$ 52
V_s 54
V 54
Leib(L) 66
φ_t^x 70
$J(t)$ 72
$\tilde{t}$ 72
For$_1$(L) 72
$\varphi(x)$ 72
$\varphi(t)$ 72
$\varphi(x)[\frac{x}{a}]$ 72
$M(D)$ 73
c_φ 73
C_n 73
C 73
C^* 77
$L(C)$ 73
$H_1(\varphi)$ 74
$H_2(\varphi)$ 74
$Q_1(\varphi, t)$ 74
$Q_2(\varphi, t)$ 74
Hen(L) 74
$\vdash$ 91
$\frac{\alpha \; \beta}{\gamma}$ 91
(L, S) 104
$\#(E)$ 111
$\mathscr{P}(E)$ 112
(L_n, S_n) 124
(L_e, S_e) 134
$G(\varphi)$ 143
Consis(L_n, S_n) 145
Λ 159
γ 159
$\Omega^i_{p_i, q_i}$ 159
$\mathscr{P}F(E)$ 162
$\square$ 176
$\diamond$ 176
$\Omega(\Pi)$ 176
$\models \alpha$ 177
(NE) 177
(5) 177
(déf. $\diamond$) 178
(K) 178
(PL) 178
$\vdash \varphi$ 179
(RN) 179
(RLP) 179
$(S5)$ 180
$\alpha \boxminus \beta$ 192

Petite bibliographie

1. *Handbook of Mathematical Logic.* Edited by Jon Barwise. Studies in Logic and Foundations of Mathematics. Volume 90, North Holland Pub. (1977).
   Somme réunissant les contributions de trente-quatre auteurs. Le chapitre A 1, dû à Jon Barwise, a fourni le fil conducteur des paragraphes 1 à 6 du présent exposé. L'ouvrage comporte, en particulier, un chapitre sur l'analyse non standard, appliquée à l'étude des courbes et des surfaces par K.D. Stroyan, et un chapitre sur la logique intuitionniste par A.S. Troelstra.
   Abondante bibliographie.
2. E.W. BETH. *Les fondements logiques des mathématiques.* Gauthier-Villars, Paris-Louvain 1950.
   Le lecteur y trouve des développements intéressants sur les antinomies logiques, sur l'intuitionnisme ainsi que de précieuses indications sur la philosophie de la logique.
3. BRIAN F. CHELLAS. *Modal Logic, an introduction.* Cambridge Univ. Press, Cambridge 1980.
   D'un accès facile pour tout lecteur familier avec la matière des paragraphes 1, 2 et 3 du présent exposé.
4. PAUL J. COHEN. *Set Theory and the Continuum Hypothesis.* W.A. Benjamin, Inc., New York 1966.
   Texte désormais classique. Présente sous une forme particulièrement claire et concise quelques-uns des résultats les plus profonds de la logique du premier ordre et de la théorie des ensembles. Demande une lecture très attentive.
5. ANTON DIMITRIU. *History of Logic.* 4 volumes. Abacus Press, Tunbridge Wells, Kent 1977.
   Ouvrage très vaste sur la logique en général, depuis les origines connues jusqu'au milieu du XX^{e} siècle environ.
6. HERBERT B. ENDERTON. *A Mathematical Introduction to Logic.* Academic Press, New York 1970.
   Comporte une démonstration du théorème d'incomplétude de Gödel et une introduction à la logique du second ordre. Nombreux exercices.
7. PAUL R. HALMOS. *Introduction à la théorie des ensembles.* Gauthier-Villars, Paris 1967.
   Le titre original de cet ouvrage est "Naive Set-theory". Le qualificatif "naïf" a été abondamment réutilisé dans le présent exposé. Le texte de P. Halmos offre, dans une langue accessible à chacun, une présentation sérieuse de la "théorie des ensembles".
8. S.C. KLEENE. *Logique mathématique.* Collection U, Armand Colin, Paris 1971.
   Ouvrage très riche sur la logique du premier ordre et les fondements des mathématiques. Comporte de nombreuses indications sur l'histoire récente de la logique mathématique. Beaucoup d'exercices.

9. G. Kreisel et J.L. Krivine. *Logique mathématique.* Dunod, Paris 1967.
Exposé très dense de type mathématique. Exercices accompagnés d'indications sur leurs solutions.

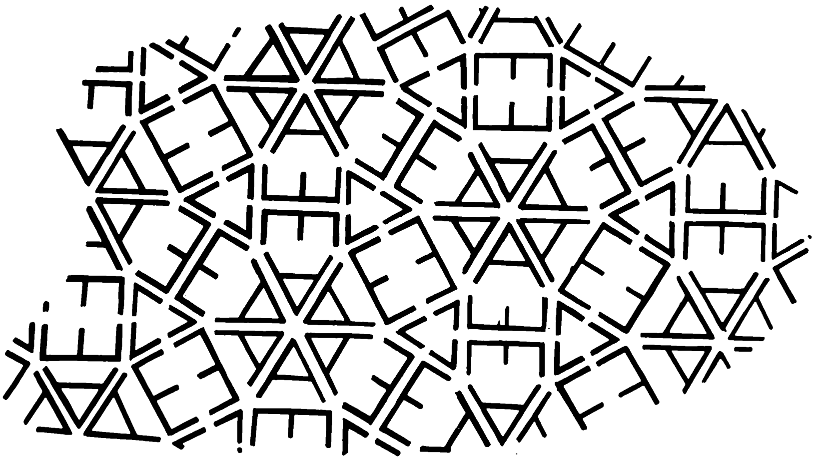
10. Jean-Louis Krivine. *Théorie axiomatique des ensembles.* Collection SUP. Presses univ. de France, Paris 1972.
Présentation du système d'axiomes de Zermelo – Fraenkel, dans le style de l'ouvrage précédent.

11. Richard Purtill. *Logic (Argument, refutation and proof).* Harper and Row. New York 1979.
L'ouvrage présente en particulier les rapports de la logique symbolique d'aujourd'hui avec la logique aristotélicienne, ainsi que le calcul des probabilités. Un chapitre est consacré aux logiques modales. Nombreux exemples et citations. Problèmes avec solutions.

12. Alain Robert. *L'analyse non standard.* Presses polytechniques romandes, Lausanne 1985.
L'aspect mathématique de la théorie est privilégié par rapport à son aspect purement logique.

13. Joseph R. Shoenfield. *Mathematical Logic.* Addison – Wesley Pub. Co. 1967.
Ouvrage très riche sur la logique du premier ordre, l'arithmétique et la théorie des ensembles. Une annexe est consacrée au "problème des mots". Nombreux problèmes.

14. Alfred Tarski. *Introduction à la logique.* Gauthier-Villars, Paris 1971.
Livre écrit à l'intention d'un large public. Il n'exige pas la maîtrise d'un appareil mathématique compliqué. Comporte des exercices et des suggestions d'ouvrages à lire.



Introduction à la logique

André Delessert

Destiné à un large public, ce livre, qui ne nécessite pas de connaissances avancées en mathématiques, est axé principalement sur la logique du premier ordre. L'intention générale est de proposer des faits de logique non banals, tels que le théorème de complétude de la logique de premier ordre et ses divers corollaires. Quelques relations avec la langue, la philosophie et les fondements des mathématiques sont abordées à la lumière des résultats démontrés.

André Delessert est né à Lausanne où il a obtenu sa licence ès sciences puis son doctorat. Nommé professeur extraordinaire puis ordinaire à la Faculté des sciences de l'Université de Lausanne, dont il a été le recteur, André Delessert a fait partie, en qualité de secrétaire ou de président, de diverses commissions nationales et internationales traitant de mathématiques et a publié de nombreux ouvrages dont, entre autres, ***Géométrie plane***, ***Introduction à la géométrie de l'espace***, ***Introduction à la trigonométrie*** ainsi que de nombreux articles concernant les mathématiques et leur enseignement

9 782880 741532

Presses polytechniques romandes