Centre de Recherches Sémiologiques

Travaux de logique

Nº 5 — Avril 1991

Denis Miéville

INTRODUCTION A LA THEORIE DES SYSTEMES FORMELS (DEUXIEME PARTIE)

EDITION REVUE ET CORRIGEE

CdRS

Université de Neuchâtel

Cet ouvrage constitue une réédition revue et corrigée d'un texte paru sous le même titre en 1987 (Travaux de logique, Nº 2).

Centre de Recherches Sémiologiques
Université de Neuchâtel
Espace Louis-Agassiz 1
CH-2000 Neuchâtel (Switzerland)

TABLE DES MATIERES

CHAPITRE 6 - LES FONCTIONS RECURSIVES

CHAPITRE 4 - LES SYSTEMES FORMELS DU PREMIER ORDRE

1. PREAMBULE

Il s'agit d'un vaste ensemble de systèmes formels qui d'une part, formalisent la logique des propositions et celle des prédicats et, d'autre part, permettent de formaliser différentes théories dont celle de l'arithmétique par exemple: la partie logique permettant en quelque sorte de calculer sur la théorie formalisée.

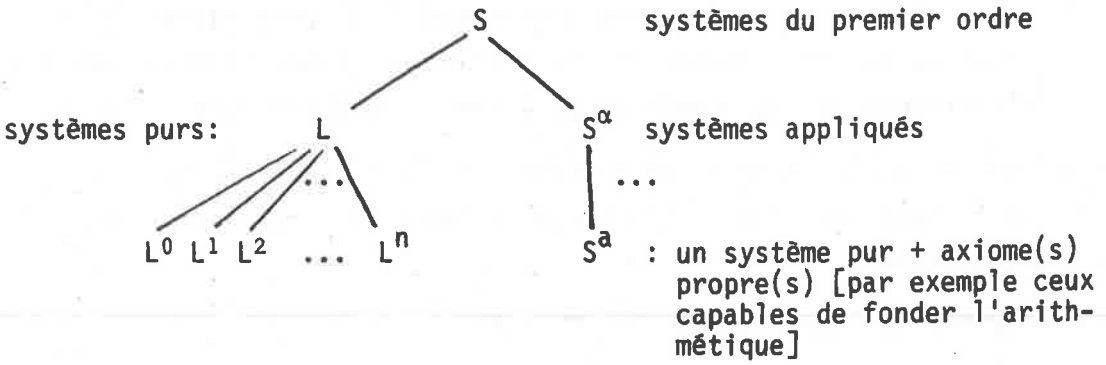
On désignera un système formel quelconque du premier ordre par le nom S. On opérera une distinction entre deux catégories de systèmes du premier ordre.

1. Il y a celle qui représente les systèmes logiques purs. Il s'agit d'un ensemble de systèmes conçus pour représenter par exemple:
- la logique des propositions: L^0;
- la logique des prédicats monadiques: L^1 (la logique des propriétés);
- la logique des prédicats binaires: L^2 (la logique des relations);

  ⋮
- la logique des prédicats n-aires: L^n.

On désignera un système quelconque de cette catégorie-là par le nom L.

2. Il y a la catégorie des systèmes du premier ordre qui constituent une expansion des systèmes logiques purs, expansion conçue de manière à représenter des théories appliquées. Ces systèmes, en plus des axiomes logiques, possèdent des axiomes extra-logiques caractérisant une théorie particulière. Ils possèdent ainsi des axiomes propres. On désignera un système quelconque de cette catégorie-là par le nom S^α.



Les systèmes du premier ordre contiennent donc L^0. Nous avons choisi de présenter ce système dans un chapitre séparé pour deux raisons:

1. Il nous semble raisonnable de présenter l'esprit et les concepts fondamentaux des systèmes formels à partir d'un système relativement simple.

2. La logique des propositions est d'une importance capitale, ce qui justifie d'en présenter séparément la formalisation.

R e m a r q u e. Les systèmes S sont du premier ordre parce qu'il est possible d'y représenter une quantification qui n'agit que sur des symboles qui seront interprétés comme des variables d'objet. Si, ce que nous ne ferons pas, la quantification agissait sur des variables de prédicat, le système serait du deuxième ordre et, du troisième ordre si elle agissait sur des variables de "prédicat de prédicat", etc.

2. LES QUATRE ENSEMBLES FONDAMENTAUX

2.1 L'alphabet $\mathscr{A}$

Il est constitué de l'union des ensembles suivants:

(1) Ensemble des constantes d'objet: $\{c_1, c_2, \ldots, c_n, \ldots\}$
Cet ensemble peut être vide: c'est souvent le cas pour la formalisation de la logique des prédicats. Il peut aussi ne contenir qu'un nombre fini d'éléments: pour formaliser l'arithmétique, un seul élément suffit.

(2) Ensemble des variables d'objet: $\{v_1, v_2, \ldots, v_n, \ldots\}$
Elles constituent toujours, quand elles existent, un ensemble infini (dénombrable).

(3) Des ensembles de symboles de prédicat: $\{p_1^d, p_2^d, \ldots, p_n^d, \ldots\}$
L'indice supérieur d est le degré du symbole. Il peut varier de 0 à k quelconque. Pour formaliser la logique des propositions, nous n'avons considéré que les symboles de prédicat de degré zéro.

(4) Des ensembles de symboles de foncteur: $\{f_1^d, f_2^d, \ldots, f_n^d, \ldots\}$
L'indice supérieur d est le degré du symbole. Il peut varier de 1 à k quelconque.

(5) L'ensemble des connecteurs: $\{\sim, \supset, \forall\}$

(6) L'ensemble des parenthèses: {(,)}

Remarque. Chaque ensemble est spécifié en fonction du rôle que ses éléments joueront dans la démarche interprétative.

Conventions: c, c_i, c_j désignent une constante quelconque

v, v_i, v_j désignent une variable quelconque

p^d, p_i^d, p_j^d désignent un symbole quelconque de prédicat de degré d

f^d, f_i^d, f_j^d désignent un symbole quelconque de foncteur de degré d

Questions :

1. L'ensemble $\mathscr{A}$ est-il dénombrable?
2. L'ensemble $\mathscr{A}$ est-il décidable?
3. Que peuvent représenter les symboles de foncteur dans une interprétation?

2.2 L'ensemble des ebf: $\mathscr{E}$

Nous allons procéder en trois temps et définir successivement:

I. L'ensemble des termes.

II. L'ensemble des formules atomiques.

III. L'ensemble des ebf lui-même.

I. L'ensemble des termes

(1) Une constante d'objet est un terme.

(2) Une variable d'objet est un terme.

(3) Si f^d est un foncteur de degré d et si $t_1, t_2, \ldots, t_d$ sont des termes (pas nécessairement distincts), $f^d t_1 t_2 \ldots t_d$ est un terme.

(4) Rien n'est un terme sinon par ce qui précède.

Questions:

4. Ecrire quelques termes.
5. Parmi les expressions suivantes, lesquelles sont des termes?

c_4, $f_2^1 v_3$, v_4, $f_2^3 v_1 v_1 v_1$, $f_3^2 v_1 v_1 v_1$, $f_1^1 f_1^1 f_1^1 f_1^1 c_1$, $f_1^3 c_3 f_1^2 c_2 f_1^1 c_1 c_1$, f_1^2

6. Quels sont les termes dans la logique des propositions, dans la logique des prédicats?

II. L'ensemble des formules atomiques

(1) Si p^d est un prédicat de degré d et si $t_1, t_2, \ldots, t_d$ sont des termes (pas nécessairement distincts), $p^d t_1 t_2 \ldots t_d$ est une formule atomique.

(2) Rien n'est une formule atomique sinon par ce qui précède.

Questions :

7. Ecrire quelques formules atomiques.
8. Parmi les expressions suivantes, lesquelles sont des formules atomiques?
$p_1^1 c_1$, $p_1^2 v_3 v_5$, c_3, $f_1^2 c_3 v_4$, p_1^0, $p_1^2 f_1^2 c_1 f_1^1 v_4 c_1$, $f_1^2 p_1^1 v_2 v_1$, $p_1^2 c_1 f_1^2 v_1 c_1$, $p_1^1 f_1^1 f_1^1 v_1$
9. Quelles sont les formules atomiques dans la logique des propositions, dans celle des prédicats?
10. En quoi se distinguent un terme et une formule atomique?

III. L'ensemble des expressions bien formées (ebf) : $\mathscr{E}$

(1) Une formule atomique est une ebf.

(2) Si A est une ebf, $\sim A$ est une ebf.

(3) Si A et B sont des ebf, $(A \supset B)$ est une ebf.

(4) Si A est une ebf et v une variable d'objet, $(\forall v)A$ est une ebf.

(5) Rien n'est une ebf sinon par ce qui précède.

Remarque. Nous conservons les conventions énoncées en page 37, 1ère partie (cf. remarques). De plus, nous poserons $(\exists v)A =_{df} \sim(\forall v)\sim A$.
Le signe $\forall$ est appelé le quantificateur universel et le signe $\exists$ le quantificateur existentiel ou particulier.

Questions :

11. Dans la clause (4) de la définition inductive de l'ensemble des ebf, l'expression A contient-elle v?
12. L'expression suivante est-elle une ebf?

$$(\forall v_1)p_1^1 v_2 \supset \sim(\exists v_2)p_1^1 v_1$$

13. Ecrire quelques ebf.
14. Ecrire sans abréviation: $\sim(\exists v)p_1^1 v \wedge (\exists v)\sim p_2^1 v$

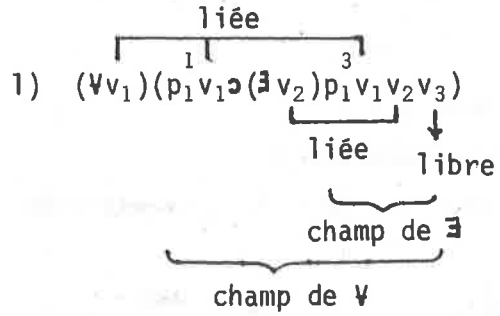
Il faut maintenant introduire deux notions.

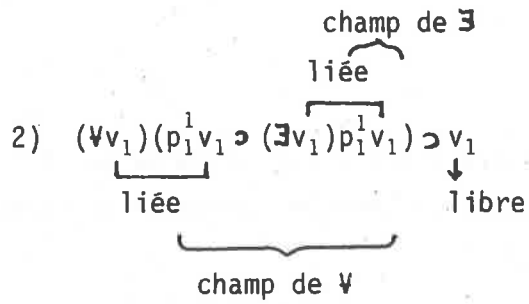
DEFINITION 19 - Soit les ebf $(\forall v)A$ et $(\exists v)A$. Les quantificateurs $\forall$ et $\exists$ sont dits au nom de la variable v. Chacun d'eux opère sur l'ebf A qui constitue le champ des quantificateurs.

-variables liées et variables libres-

Toute variable située dans le champ d'un quantificateur à son nom est dite liée. Sinon elle est libre.

Exemples





Q u e s t i o n s:

15. Quelles sont les variables libres dans :
    $(\forall v_1) p_1^2 v_1 v_2 \supset (\exists v_2) p_1^2 v_1 v_2$
    $(\forall v_1)(p_1^2 v_1 v_2 \supset (\exists v_2) p_1^2 v_1 v_2)$
16. Un terme peut-il contenir une variable? Si oui, peut-elle être liée dans ce terme? Et dans une ebf qui contient ce terme?
17. Une formule atomique peut-elle contenir une variable? Si oui, peut-elle être liée dans cette formule? Et dans une ebf qui contient cette formule?

Convention: Pour indiquer qu'une ebf A contient la variable v libre, nous écrirons A(v).

DEFINITION 20 - -libre pour v- Soit un terme t et une ebf A(v) -elle contient donc une variable v libre. On dit que le terme t est libre pour v dans A(v) si, mis à la place des occurrences libres de v dans A, aucune des éventuelles variables de t ne se trouve liée. Dit autrement, le terme t est libre pour v dans A(v) si, dans A(v/t) [l'expression obtenue après avoir substitué le terme t à chaque occurrence libre de v dans A(v)] les variables libres qui peuvent figurer dans le terme t restent libres.

Exemple : $A(v_1)$: $(\forall v_2)p_1^2 v_2 v_1 \supset p_1^2 v_2 v_1$

- le terme v_3 est libre pour v_1 dans $A(v_1)$
- le terme $f_1^2 v_4 v_3$ est libre pour v_1 dans $A(v_1)$
- le terme $f_1^1 v_2$ n'est pas libre pour v_1. En effet, sa variable v_2 se trouve liée dans
  $A(v_1/t)$: $(\forall v_2)p_1^2 v_2 f_1^1 v_2 \supset p_1^2 v_2 f_1^1 v_2$
  (v_2 liée)

Questions :

18. Soit le terme $f_1^2 v_1 c_1$. Trouver une ebf $A(v_4)$ telle que ce terme ne soit pas libre pour v_4 dans $A(v_4)$. Une fois $A(v_4)$ trouvée, chercher un terme f_1^2-- qui soit libre pour v_4 dans $A(v_4)$.
19. Un terme qui ne contient pas d'autres variables que v est-il libre pour v dans A(v)?
20. Un terme qui ne contient que des constantes est-il toujours libre pour v dans A(v)?

2.3 L'ensemble des axiomes: $\mathscr{P}$

Il s'agit d'un élargissement de l'ensemble des axiomes de L^0. Toute ebf de l'une des cinq formes suivantes est un axiome logique, et rien n'est un axiome logique sinon par l'une de ces formes:

(A1) $A \supset (B \supset A)$

(A2) $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$

(A3) $(\sim B \supset \sim A) \supset ((\sim B \supset A) \supset B)$

(A4) $(\forall v)A(v) \supset A(v/t)$ si t est libre pour v dans A(v)

(A5) $(\forall v)(B \supset A(v)) \supset (B \supset (\forall v)A(v))$ si B ne contient pas v libre.

Questions:

21. Donner un exemple d'axiome pour chacun des schémas A1-A5.
22. Les ebf suivantes sont-elles des axiomes?
    $(\forall v_1)(p_1^1 c_1 \supset p_1^2 v_1 c_1) \supset (p_1^1 c_1 \supset (\forall v_1) p_1^2 v_1 c_1)$
    $(\forall v_1)(\exists v_2) p_1^2 v_1 v_2 \supset (\exists v_2) p_1^2 v_2 v_2$
    $(\forall v_1)(\exists v_2) p_1^2 v_1 v_2 \supset (\exists v_2) p_1^2 v_1 v_2$

Remarque. Insistons encore sur la distinction entre systèmes du premier ordre purs (L) et les systèmes de premier ordre appliqués (S^α). Les premiers ne contiennent que des axiomes logiques. Ils formalisent l'appareil logique. Quant aux seconds, ils possèdent, en plus des axiomes logiques, des axiomes d'une autre nature. Il s'agit d'une catégorie d'axiomes qui mentionnent explicitement telles constantes, tels symboles de prédicat et tels symboles de foncteur. Ce sont les axiomes propres.

Par exemple, pour formaliser une structure d'ordre partiel, il faut offrir une base axiomatique qui, en plus des axiomes logiques, possède des axiomes propres, par exemple:

(A01) : $(\forall v) \sim p_1^2 v v$

(A02) : $(\forall v_i)(\forall v_j)(\forall v_k)((p_1^2 v_i v_j \wedge p_1^2 v_j v_k) \supset p_1^2 v_i v_k)$

Ces deux axiomes spécifient l'irréflexivité et la transitivité du prédicat p_1^2 choisi pour représenter une relation d'ordre partiel.

2.4 L'ensemble des règles: $\mathscr{R}$

Cet ensemble ne contient que deux éléments:

- la règle MP, le modus ponens (cf. p. 38, 1ère partie)
- la règle GEN, la généralisation. Elle s'énonce ainsi:

  Si A est une ebf, alors $(\forall v)$A est une conséquence immédiate de A.

  GEN: $A \rightarrow (\forall v)A$

Questions :

23. La règle du modus ponens s'applique-t-elle à $(\forall v_1)(p_1^0 \supset p_1^1 v_1)$ et p_1^0? Si non, peut-on transformer les expressions données de manière à ce que la règle MP s'y applique?
24. Mêmes questions pour $(\forall v_1) p_1^1 v_1 \supset p_1^0$ et $p_1^1 v_1$?
25. $(\forall v_1)(p_1^0 \supset (\exists v_1)\ p_1^2 v_1 v_1)$ est-elle une conséquence immédiate par GEN de l'ebf $p_1^0 \supset (\exists v_1)\ p_1^2 v_1 v_1$?

3. THEOREME ET CONCLUSIONS SYNTAXIQUES

Les théorèmes et conclusions syntaxiques d'un système S sont construits selon les démarches exposées au chapitre 2 [1ère partie, pp. 27-31]. Nous n'insisterons donc pas sur cet aspect, sinon pour souligner la distinction au niveau de l'appareil déductif entre le système L^0 et le système L qui formalise la logique pure des prédicats du premier ordre.

	Appareil déductif L^0	Appareil déductif L
Axiomes	(A1) (A2) (A3)	(A1) (A2) (A3) (A4) (A5)
Règles	MP	MP GEN

Q u e s t i o n s :

26. Etablir la preuve du théorème suivant: $\vdash(\forall v_1)p_1^1 v_1 \supset (\forall v_2)p_1^1 v_2$ [Utiliser notamment (A4) et (A5)].

27. A première vue, le résultat précédent peut paraître étrange. Que peut-on en conclure quant au 'statut' des variables liées?

28. Effectuer la déduction suivante: $(\forall v_1)((\forall v_3)p_1^2 v_3 v_2 \supset p_1^1 v_1), p_1^2 v_1 v_2 \vdash (\forall v_1)p_1^1 v_1$ [Utiliser notamment (A4) et (A5)].

4. LE "THEOREME" DE LA DEDUCTION POUR S

Nous allons établir le "théorème de la déduction" pour un système quelconque du premier ordre. Il s'agit d'un métathéorème analogue au métathéorème 3. Mais le système L^0 est une réalisation 'élémentaire' des systèmes du premier ordre et le "théorème de la déduction" n'offre aucune difficulté. Pour un système qui formalise le calcul des prédicats, il est nécessaire de prendre quelques précautions par rapport au jeu des variables. Une difficulté intervient donc. Elle correspond à l'interdiction -en déduc-

tion naturelle- de réitérer dans certaines conditions une variable libre. Les deux définitions que nous proposons contribuent à formuler un "théorème" qui évite toute confusion.

DEFINITION 21 - -dépendre de- Soit une déduction $B_1, B_2, \ldots, B_n$ à partir d'une classe d'hypothèses qui contient en particulier A.

Une ebf B_i <u>dépend de A</u> si

(1) B_i est A ou

(2) B_i résulte par la règle MP ou GEN d'ebf dont l'une au moins dépend de A.

<u>Exemples</u>:

1. Soit la déduction de $(\forall v)B$ à partir de la classe d'hypothèses Γ:

   $\Gamma = \{A, (\forall v)A \supset B\}$

   1. A $\in \Gamma$
   2. $(\forall v)A$ 1, GEN
   3. $(\forall v)A \supset B$ $\in \Gamma$
   4. B 3, 2, MP
   5. $(\forall v)B$ 4, GEN

   Si l'on abrège l'expression "dépend de E" par dép(E), on a la situation suivante:

   Expression de la ligne

   1. dép(A): c'est A
   2. dép(A): résulte par GEN de A qui dép(A)
   3. dép($(\forall v)A \supset B$): c'est $(\forall v)A \supset B$
   4. dép(A): résulte par MP d'une ebf qui dép(A) et dép($(\forall v)A \supset B$): résulte par MP d'une ebf qui dép($(\forall v)A \supset B$)
   5. dép(A) et dép($(\forall v)A \supset B$): résulte par GEN de B qui elle-même dép(A) et dép($(\forall v)A \supset B$).

2. Soit la déduction de $(\forall v_j)(\forall v_i)A(v_i, v_j)$ à partir de la classe d'hypothèses Γ: $\Gamma = \{(\forall v_j)A(v_i, v_j)\}$.

   1. $(\forall v_j)A(v_i, v_j) \supset A(v_i, v_j)$ (A4)
   2. $(\forall v_j)A(v_i, v_j)$ $\in \Gamma$; dép($(\forall v_j)A(v_i, v_j)$)
   3. $A(v_i, v_j)$ 1, 2, MP; " "
   4. $(\forall v_i)A(v_i, v_j)$ 3, GEN; " "
   5. $(\forall v_j)(\forall v_i)A(v_i, v_j)$ 4, GEN; " "

Q u e s t i o n s:

29. Un axiome dépend-il d'une quelconque hypothèse?
30. Considérer la déduction de la question 28 et déterminer les dépendances -si elles existent- pour les ebf de chacune des lignes.

DEFINITION 22 -tenir constant- Dans une déduction, une variable est <u>tenue constante</u> relativement à une hypothèse A si:

1) elle ne figure pas libre dans A ou
2) si, libre dans A, elle n'est pas liée par GEN dans une ebf qui dépend de A.

<u>Exemples</u>:

1. Dans la déduction 2 qui précède, la variable v_j est tenue constante relativement à l'hypothèse $(\forall v_j)A(v_i, v_j)$: v_j n'y figure pas libre. La variable v_i, par contre, n'est pas tenue constante; en effet, elle est liée par GEN [ligne 4] dans l'ebf $A(v_j, v_j)$ qui dépend de l'hypothèse.
2. Soit la déduction de $(\forall v_1)p_1^1v_1$ à partir de la classe d'hypothèses Γ :

$\Gamma = \{\underbrace{(\forall v_1)((\forall v_3)p_1^2v_3v_2 \supset p_1^1v_1)}_{P1}, \underbrace{p_1^2v_1v_2}_{P2}\}$

1.	$p_1^2v_1v_2$	$\in \Gamma$
2.	$(\forall v_1)p_1^2v_1v_2$	1, GEN
3.	$(\forall v_1)p_1^2v_1v_2 \supset p_1^2v_3v_2$	(A4), t: v_3
4.	$p_1^2v_3v_2$	3, 2, MP
5.	$(\forall v_3)p_1^2v_3v_2$	4, GEN
6.	$(\forall v_1)((\forall v_3)p_1^2v_3v_2 \supset p_1^1v_1) \supset ((\forall v_3)p_1^2v_3v_2 \supset (\forall v_1)p_1^1v_1)$	(A5)
7.	$(\forall v_1)((\forall v_3)p_1^2v_3v_2 \supset p_1^1v_1)$	$\in \Gamma$
8.	$(\forall v_3)p_1^2v_3v_2 \supset (\forall v_1)p_1^1v_1$	6, 7, MP
9.	$(\forall v_1)p_1^1v_1$	8, 5, MP

v_1 est tenue constante relativement à P1: elle y est liée.
v_2 est tenue constante relativement à P1: elle y est libre et le reste.
v_3 est tenue constante relativement à P1: elle y est liée.

v_1 n'est pas tenue constante relativement à P2: elle y est libre mais se fait lier par GEN relativement à l'ebf $p_1^2v_1v_2$ qui dépend de P2.
v_2 est tenue constante relativement à P2: elle y est libre et le reste.

Q u e s t i o n s :

31. Y a-t-il sens à définir la propriété "d'être tenue constante relativement à une hypothèse" pour une constante?
32. La notion de "dépendance" ou celle "d'être tenue constante" s'applique-t-elle à autre chose qu'à des hypothèses?
33. Effectuer la déduction suivante et déterminer quelles variables sont tenues constantes:
$A(v_i, v_j), (\forall v_k)A(v_i, v_j) \supset B(v_k) \vdash (\forall v_k)B(v_k)$

METATHEOREME 12 - le "théorème" de la déduction pour S
Dans S, si $\Gamma, A \vdash B$ et si les variables sont tenues constantes relativement à A alors $\Gamma \vdash A \supset B$.

Démonstration: Il s'agira d'une démonstration par induction sur le nombre k de lignes de la déduction supposée donnée: $\Gamma, A \vdash B$

Base de l'induction : $k = 1$

Dans une déduction ne comportant qu'une ligne aucune application des règles n'est possible. L'étude de ce cas est donc en tout point semblable à celle présentée pour la démonstration du métathéorème 3 [1ère partie, pp. 41-43].

Hypothèse d'induction :

Pour toute déduction $\Gamma, A \vdash B$ dont les variables sont tenues constantes relativement à A et qui compte au plus k lignes, on peut établir la déduction $\Gamma \vdash A \supset B$.

Pas d'induction :

Nous devons montrer que si la déduction $\Gamma, A \vdash B$ compte $k+1$ lignes et si les variables sont tenues constantes relativement à A, on peut établir une déduction $\Gamma \vdash A \supset B$. Considérons une déduction de $k+1$ lignes dont l'expression de la $k+1$ nième ligne est B. L'expression B peut se justifier de cinq manières différentes.

1. B est un axiome ou un théorème: $\vdash B$.
2. B appartient à Γ.
3. B est A.

4. B est une conséquence immédiate de deux ebf qui la précèdent par la règle MP.
5. B est une conséquence immédiate d'une ebf qui la précède par la règle GEN.

L'étude des quatre premiers cas est en tout point semblable à celle présentée pour la démonstration du métathéorème 3 [1ère partie, pp. 43-44]. Nous ne traiterons en conséquence que le cinquième cas: B est une conséquence immédiate d'une ebf qui la précède par la règle GEN.

Considérons donc la déduction $\Gamma, A \vdash B$ qui compte k+1 lignes.

1.		
2.		
:	:	
i	B_i	
:	:	
k+1	B	i, GEN .

L'expression B de la ligne k+1 résulte par GEN d'une ebf B_i qui la précède. B est soit de la forme $(\forall v)C$ où C ne contient pas v libre, soit de la forme $(\forall v)C(v)$ où C contient v libre.

B_i est donc de la forme C ou C(v). Cette distinction n'intervient cependant pas dans la démonstration. Nous utilisons donc uniquement C(v).

L'ebf B_i s'inscrit à la ligne i; cet indice est strictement plus petit que k+1. L'ebf B_i entre donc dans le champ de l'hypothèse d'induction et on obtient: $\Gamma \vdash A \supset C(v)$ B_i est C(v) et hyp. d'induction.
Poursuivons cette déduction:

n	$A \supset C(v)$	hyp. d'induction [conclusion déduite à partir de l'ensemble des hypothèses Γ]
n+1	$(\forall v)(A \supset C(v))$	n, GEN
n+2	$(\forall v)(A \supset C(v)) \supset (A \supset (\forall v)C(v))$	(A5), si A ne contient pas v libre
n+3	$A \supset (\forall v)C(v)$	n+2, n+1, MP
n+4	$A \supset B$	n+3, $(\forall v)C(v)$ est B

Donc, si A ne contient pas v libre [c'est-à-dire, si v a été tenue constante relativement à A], on obtient $\Gamma \vdash A \supset B$.

Q u e s t i o n s :

34. Comment savoir si A ne contient réellement pas v libre?

35. On donne la déduction: $\Gamma, A_1, A_2 \vdash B$. Que permet d'écrire le métathéorème 12 si A_1 et A_2 ne contiennent pas de variable? Et si A_1 contient v_1, A_2 contient v_2 et que seule v_2 est tenue constante?
36. Pour quelle raison n'avons-nous pas à nous soucier, dans l'étude des quatre premiers cas de la démonstration du pas d'induction, d'opérer avec des variables tenues constantes?

METATHEOREME 13 - Dans S, si $\Gamma \vdash A \supset B$, alors $\Gamma, A \vdash B$.

Démonstration: Sous les hypothèses de l'ensemble Γ, on a une déduction de $A \supset B$.
Ajoutons à cet ensemble d'hypothèses, l'hypothèse A. Sous cette condition, il est possible d'établir la déduction: $\Gamma, A \vdash B$.

1. $A \supset B$ se déduit de Γ (hypothèse du Mth. 13)
2. A est l'hypothèse ajoutée
3. B 1,2, MP

On obtient donc la conclusion B à partir de l'ensemble des hypothèses Γ et A : $\Gamma, A \vdash B$.

Q u e s t i o n :

37. Pourquoi n'a-t-on pas ici à prendre de précaution avec les variables?

5. LES REGLES DE LA DEDUCTION NATURELLE

Les règles de la déduction naturelle établies pour L^0 restent valables dans S. Il reste à vérifier que les règles pour le quantificateur universel sont disponibles dans S.

On avait:

1] Règle ∀e

$$n \left| \begin{array}{l} (\forall v)A(v) \\ \hline A(v/t) \end{array} \right. \quad \text{si t libre pour v dans } A(v)$$

La régle ∀e n'est qu'une autre façon d'écrire le schéma d'axiome (A4) avec sa restriction d'emploi.

2] Règle ∀i

```
n | v |
  |   |
m |   | A(v)
  | (∀v)A(v)
```

n-m, ∀i. A condition de ne pas réitérer une ebf qui contient v libre.

Dans la règle ∀i, le fait que la sous-déduction ne comporte pas d'hypothèse exprime que la règle GEN est de la forme:

si A(v) alors (∀v)A(v) et non pas

si B ⊢A(v) alors B⊢(∀v)A(v).

Enfin, l'interdiction de réitérer une ebf qui contient v libre, garantit que v est tenue constante et autorise l'utilisation du Mth. 12.

Q u e s t i o n :

38. Considérer la déduction $(\forall v_2)A(v_1, v_2) \vdash (\forall v_2)(\forall v_1)A(v_1, v_2)$ dans laquelle v_1 n'est pas tenue constante et vérifier qu'il n'est pas possible de démontrer -en déduction naturelle- l'expression $(\forall v_2)A(v_1, v_2) \supset (\forall v_2)(\forall v_1)A(v_1, v_2)$.

6. LA SEMANTIQUE DES SYSTEMES FORMELS DU PREMIER ORDRE

Il s'agit maintenant d'offrir le moyen de 'revêtir' les systèmes formels du premier ordre d'une dimension sémantique. Reconnaître une signification aux ebf nécessite donc d'interpréter tous les symboles qui les composent. Dans le système L^0 l'interprétation des symboles était aisée. Il suffisait d'établir une application entre les symboles de prédicat de degré zéro et l'ensemble des valeurs V: $V = \{\top, \bot\}$. Mais ici, la situation est autre puisque nous disposons d'autres symboles, soit:

EC : ensemble des constantes

EV : ensemble des variables

EP^n : ensemble des symboles de prédicat de degré n; $n \in \mathbb{N}$, $n>0$ [pour n = 0, nous avons déjà une interprétation].

EF^n : ensemble des symboles de foncteur de degré n; $n \in \mathbb{N}$, $n>0$.

Nous allons donc nous donner non seulement $V = \{\top, \bot\}$, mais également un ensemble Ω non vide d'objets quelconques. Mais si cela est suffisant pour offrir une interprétation aux symboles de constante et de variable, c'est encore insuffisant pour attribuer une signification aux

symboles de prédicat et de foncteur. Pour pallier cette difficulté nous allons procéder comme suit: à partir de l'ensemble Ω, nous définirons de manière extensionnelle d'une part les propriétés et les relations, et d'autre part, les foncteurs.

Définition 'en extension' d'une relation: un rappel

Définir une propriété, une relation binaire, une relation n-aire, c'est donner les éléments, les couples d'éléments, les n-uples qui possèdent la propriété ou ont entre eux la relation [cf. 1ère partie, pp. 83-84]. Attribuer une signification à un symbole de prédicat de degré $\underline{d}$, $p_i^{d>0}$, c'est donc lui faire correspondre un ensemble de d-uple.

Exemple:

Soit $\Omega = \{0, 1, 2, 3, 4, 5, 6, 7, \ldots, n, \ldots\}$
Attribution d'une signification à p_i^d où $d = 3$

1) En extension:

$p_i^3 \longmapsto R = \{<0,1,9>, <0,2,9>, <0,3,9>, <0,4,9>, <0,5,9>, <0,6,9>, <0,7,9>, <0,8,9>\}$

Cet ensemble R est contenu dans l'ensemble produit Ω^3; c'est donc une partie [un sous-ensemble] de Ω^3 :

$R \in \wp(\Omega^3)$

2) En compréhension:

p_i^3 : "être entre le plus grand et le plus petit"

Définition 'en extension' d'un opérateur: un rappel

Définir un opérateur à n-opérandes, c'est donner les couples d'arguments dont le premier consiste en un n-uple représentant les $\underline{n}$ opérandes, et dont le second argument représente le résultat de l'opération [cf. 1ère partie, pp. 84-85]. Attribuer une signification à un symbole de foncteur f_i^d de degré $\underline{d}$, c'est donc lui faire correspondre un ensemble de cette nature.

$$f_i^d = \{\ldots, \underbrace{<<-, -, \ldots, ->}_{\text{n-uple de } \underline{n} \text{ opérandes}} \overset{\text{résultat}}{\downarrow} ->, \ldots\}$$

Exemple:

Soit Ω: {0,1,2,3}

Attribution d'une signification à f_i^d où d = 2.

1) En extension:

$f_i^2 \longmapsto T$ = {<<0,0>, 0>, <<0,1>, 1>, <<0,2>, 2>, <<0,3>, 3>,
<<1,0>, 1>, <<1,1>, 2>, <<1,2>, 3>, <<1,3>, 0>,
<<2,0>, 2>, <<2,1>, 3>, <<2,2>, 0>, <<2,3>, 1>,
<<3,0>, 3>, <<3,1>, 0>, <<3,2>, 1>, <<3,3>, 2>}

Cet ensemble T est contenu dans l'ensemble produit $\Omega^2 \chi \Omega$, c'est donc une partie de $\Omega^2 \chi \Omega$: $T \in \wp(\Omega^2 \chi \Omega)$.

2) En compréhension:

f_i^2 : addition 'reste modulo 4'.

Conventions : Posons les notations suivantes:

EC : ensemble des constantes de S.
EV : ensemble des variables de S.
EP^0 : ensemble des symboles de prédicat de degré zéro de S.
$EP^{d>0}$: ensemble des symboles de prédicat de degré d de S, d>0 .
$EF^{d>0}$: ensemble des symboles de foncteur de degré d de S, d>0 .

DEFINITION 23 -interprétation- - Une interprétation de S est la donnée
1) de l'ensemble V = {⊤, ⊥}- le domaine de valeurs;
2) d'un ensemble non vide Ω d'objets - le domaine d'objets;
3) d'une application Ψ de chacune des espèces suivantes:
3.1 Ψ_C : EC $\longrightarrow$ Ω
3.2 Ψ_V : EV $\longrightarrow$ Ω
3.3 Ψ_{p^0} : EP^0 $\longrightarrow$ V
3.4 $\Psi_{p^{d>0}}$: EP^d $\longrightarrow \wp(\Omega^d)$ -organisation relationnelle
3.5 $\Psi_{F^{d>0}}$: EF^d $\longrightarrow \wp(\Omega^d \chi \Omega)$ -organisation fonctionnelle.

Questions :

39. Que peut-on dire des éléments de Ω ?
40. En quoi l'interprétation d'une variable diffère-t-elle de celle d'une constante?
41. De quelles façons une interprétation I1 peut-elle être différente d'une interprétation I2?

Après l'attribution d'une signification aux différents symboles du vocabulaire, il s'agit d'offrir également une valeur sémantique aux termes ainsi qu'aux ebf.

Un terme [cf. pp. 3-4] étant une construction bien formée sur la base de foncteurs, de constantes et de variables, c'est en considérant l'application relative à ces éléments-là que nous fournirons une application attribuant une valeur sémantique à chaque terme.

Soit ET, l'ensemble des termes. On définit l'application

$$\Psi_T : ET \longrightarrow \Omega$$

par les trois conditions suivantes:

1) $\Psi_T(c_i) = \Psi_C(c_i)$

2) $\Psi_T(v_i) = \Psi_V(v_i)$

3) $\Psi_T(f_i^d t_1 t_2 \ldots t_d)$ = l'élément de Ω qui dans l'image $\Psi_{Fd}(f_i^d)[\in \mathcal{P}(\Omega^d \times \Omega)]$ est en relation directe avec le d-uple : $\langle \Psi_T(t_1), \Psi_T(t_2), \ldots, \Psi_T(t_d) \rangle$ $[\in \Omega^d]$

Cette formulation apparemment confuse mérite d'être exemplifiée.

Exemple

Soit $\Omega = \mathbb{N}$, le terme $f_1^2 c_1 v_2$ et l'interprétation I:

$\Psi_C(c_1) = 1$

$\Psi_V(v_2) = 2$

$\Psi_{Fd}(f_1^2) = \{\langle\langle 0,0\rangle, 0\rangle, \langle\langle 0,1\rangle, 1\rangle, \langle\langle 0,2\rangle, 2\rangle, \ldots,$
$\langle\langle 1,0\rangle, 1\rangle, \langle\langle 1,1\rangle, 2\rangle, \langle\langle 1,2\rangle, 3\rangle, \ldots,$
$\langle\langle 2,0\rangle, 2\rangle, \langle\langle 2,1\rangle, 3\rangle, \langle\langle 2,2\rangle, 4\rangle, \ldots\}$

En compréhension : "addition dans $\mathbb{N}$".

Recherche de la valeur de $f_1^2 c_1 v_2$

1. Constitution du couple $\langle \Psi_T(c_1), \Psi_T(v_2) \rangle$

$\Psi_T(c_1) = \Psi_C(c_1) = 1$

$\Psi_T(v_2) = \Psi_V(v_2) = 2$

On obtient le couple $\langle 1, 2 \rangle$

2. Reconnaissance du couple <1,2> dans un des éléments de l'image de f_1^2 :

$$<<1,2>,\ 3>$$

3. Attribution au terme $f_1^2 c_1 v_2$ de la valeur de Ω qui est en relation directe avec le couple <1,2>: 3.

$$\Psi_T(f_1^2 c_1 v_2) = 3$$

Q u e s t i o n s :

42. Soit le terme $f_2^2 v_3 f_1^2 v_1 c_2$, l'ensemble $\Omega = \mathbb{N}$ et l'interprétation I:

$\Psi_C(c_2) = 2$; $\Psi_V(v_3) = 7$; $\Psi_V(v_1) = 3$

$\Psi F^d(f_1^2)$ = comme ci-dessus

$\Psi_F{}^d(f_2^2) = \{<<0,0>, 0>, <<0,1>, 0>, <<0,2>, 0>, \ldots,$
$<<1,0>, 0>, <<1,1>, 1>, <<1,2>, 2>, \ldots,$
$\vdots$
$<<7,1>, 7>, <<7,2>, 14>, \ldots, <<7,5>, 35>, \ldots\}$

En compréhension : "le produit dans $\mathbb{N}$"

Déterminer l'image de $f_2^2 v_3 f_1^2 v_1 c_2$.

43. Soit $\Omega = \{1,2,3\}$ et la formule atomique $p_1^2 c_1 v_3$. On a choisi une interprétation I dans laquelle

$\Psi_C(c_1) = 2$; $\Psi_V(v_3) = 1$; $\Psi_{pd}(p_1^2) = \{<1,2>, <1,3>, <2,3>\}$

Comment interpréter en compréhension l'image de p_1^2 ?

Pourquoi a-t-on $<1,2> \in \Psi_P{}^d(p_1^2)$?

A-t-on $<\Psi_C(c_1), \Psi_V(v_3)> \in \Psi_P{}^d(p_1^2)$?

DEFINITION 24 -évaluation- - Soit A une ebf de S et une interprétation I. On appelle <u>évaluation de A pour l'inteprétation I</u> la valeur de l'application $val : A \longrightarrow V$ telle que:

1. $val(p_i^0) = \top$ ssi $\Psi_{p0}(p_i^0) = \top$ dans I.
2. $val(p_i^d t_1 t_2 \ldots t_d) = \top$ ssi
$<\Psi_T(t_1), \Psi_T(t_2), \ldots, \Psi_T(t_d)> \in \Psi_{pd}(p_i^d)$ dans I.
3. $val(\sim A) = \top$ ssi val(A) est différente de $\top$ dans I.
4. $val(A \supset B) = \top$ ssi val(A) est différente de $\top$ dans I ou val(B) = $\top$ dans I.

5. $val((\forall v_i)A) = \top$ ssi $val(A) = \top$ dans I, quelle que soit l'image de la variable v_i.

6. $val(A) = \perp$ ssi val(A) est différente de $\top$ dans I.

Q u e s t i o n s :

44. Dans la définition 23 [cf. p. 16], nous attribuions par l'application Ψ_V un élément de Ω à chaque élément de l'ensemble des variables EV. Cette application ne différait en aucune manière de l'application Ψ_C, laissant ainsi entendre que le statut de variable et de constante n'est, en fait, pas distinct. Dans la clause 5 de la définition 24, il est spécifié: "quelle que soit l'image de la variable v_i". A l'aide de cette spécification quelle est l'idée qui est réintroduite relativement aux éléments de EV?

45. Soit l'ensemble Ω: $\Omega = \{1, 2, 3\}$, et l'interprétation I ainsi donnée:

$\Psi_C(c_1) = 2$; $\Psi_C(c_2) = 1$; $\Psi_V(v_1) = 1$

$\Psi_{Pd}(p_1^2) = \{<1,2>, <1,3>, <2,3>\}$

$\Psi_{Pd}(p_2^2) = \{<1,1>, <2,2>, <3,3>\}$.

Pour cette interprétation, quelle est l'évaluation de :

1) $p_1^2c_1v_1$ 2) $p_1^2v_1c_1$ 3) $p_2^2c_1v_1$ 4) $p_2^2v_1v_1$

5) $(\forall v_1)p_2^2v_1v_1$ 6) $(\forall v_1)p_2^2v_1c_2$?

DEFINITION 25 -logiquement valide sur Ω- Une ebf A de S est <u>logiquement valide sur un domaine particulier Ω</u> ssi $val(A) = \top$ pour toute interprétation sur Ω

DEFINITION 26 -logiquement valide- Une ebf A de S est <u>logiquement valide</u> ssi elle est logiquement valide sur tout domaine Ω, ce que nous écrirons ainsi: $\models A$

<u>R e m a r q u e</u> On voit que la validité logique [déf. 26] est plus forte que la validité logique sur Ω [déf. 25].

Q u e s t i o n s :

46. Peut-il arriver qu'une ebf soit logiquement valide sur un certain domaine et pas sur un autre?

47. Est-il possible qu'une ebf soit logiquement valide sans être logiquement valide sur un certain domaine Ω?

Exemple

Soit l'ebf A =df $\sim(\forall v)\sim p^1v \supset (\forall v)p^1v$ et le domaine Ω à un seul élément: $\Omega = \{1\}$.

Il n'existe qu'une seule manière d'interpréter la variable v: $\Psi(v) = 1$.

Mais il existe deux possibilités pour interpréter le prédicat de degré 1.

En effet, attribuer une signification à p^1, c'est lui faire correspondre un élément R appartenant à l'ensemble des parties de Ω:

$$R \in \wp(\Omega)$$

Si l'ensemble $\Omega = \{1\}$, alors $\wp(\Omega) = \{\emptyset , \{1\}\}$, ou autrement écrit: $\wp(\Omega) = \{\emptyset, \Omega\}$. Il y a donc deux interprétations possibles pour p^1:

$\Psi_{pd}(p^1)$ < $\emptyset$: Interprétation I'

Ω : Interprétation I"

Comme nous voulons examiner la validité de A sur Ω , il suffit dès lors d'étudier les deux interprétations possibles :

	I'	I"	EXPLICATIONS	
$\Psi_V(v)$	1	1		
$\Psi_{pd}(p^1)$	$\emptyset$	Ω	I'	I"
1. val(p^1v)	$\perp$	$\top$	. $\perp$ car $1 \notin \emptyset$	. $\top$ car $1 \in \Omega$
2. val($(\forall v)p^1v$)	$\perp$	$\top$	. Quelle que soit la valeur de v il n'y a qu'une seule possibilité pour $\Psi_V(v)$	
3. val($\sim p^1v$)	$\top$	$\perp$	. $\top$ car 1.+ déf. 24	. $\perp$ car 1.+ déf. 24
4. val($(\forall v)\sim p^1v$)	$\top$	$\perp$	. cf. explication ligne 2	
5. val($\sim(\forall v)\sim p^1v$)	$\perp$	$\top$	. $\perp$ car 4. + déf. 24	. $\top$ car 4. +déf. 24
6. val(A)	$\top$	$\top$	. $\top$ car 5., 2. +déf. 24	. $\top$ car 5.,2. +déf. 24

L'ebf A est donc logiquement valide sur Ω.

Q u e s t i o n s :

48. Considérer l'expression A de l'exemple précédent et le domaine Ω : $\Omega = \{1, 2\}$.
    - Combien y a-t-il d'interprétations différentes pour v?
    - Former l'ensemble des parties de Ω : $\wp(\Omega)$ puis établir toutes les interprétations possibles pour p^1.
    - L'ebf A est-elle valide sur Ω?

- Considérer une ebf possédant un prédicat de degré 2; par exemple: $B = \sim(\forall v)p^2vv$.
  Décrire la démarche à effectuer pour déterminer si l'ebf B est logiquement valide sur Ω.

49. Une tautologie sous-tend l'idée d'une analyse finie de la combinatoire des valeurs de vérité. L'exemple ci-dessus met en évidence qu'une telle combinatoire finie est effectivement réalisée. Il est tentant d'assimiler le terme de "tautologie" à celui de "logiquement valide". Mais cette combinatoire finie est-elle toujours réalisée?

7. QUELQUES METATHEOREMES

Il est nécessaire de s'assurer que dans L, tout théorème est logiquement valide. Pour le démontrer, nous procéderons en deux étapes: nous établirons tout d'abord que les règles GEN et MP conservent la propriété "d'être logiquement valide", puis nous montrerons que tout axiome est logiquement valide.

7.1 Où il est question des règles d'inférence

La règle du modus ponens conserve la validité logique:
Si A et $A \supset B$ sont logiquement valides, alors B est logiquement valide.

Ce résultat a été démontré dans le cadre de l'étude du système L° [1ère partie, pp. 58-9]. Occupons-nous donc de la règle GEN. Proposons tout d'abord une définition.

DEFINITION 27 -fermeture- Soit $A(v_1, v_2, \ldots, v_k)$ une ebf dont les seules variables libres sont $v_1, v_2, \ldots, v_k$. La fermeture de cette ebf est: $(\forall v_k)\ldots(\forall v_2)(\forall v_1)A(v_1, v_2, \ldots, v_k)$. Il s'agit d'une ebf dans laquelle toutes les variables sont liées. On la dira fermée.

Q u e s t i o n s :

50. L'ordre dans lequel les quantificateurs sont introduits afin de fermer une ebf a-t-il de l'importance?
51. Quelle est la fermeture de $p^1_1v_1 \supset (\exists v_3)p^2_1v_3v_2$?
52. L'ebf $A(v_1, v_4, v_3)$ a-t-elle une fermeture?
53. De quelle manière peut-on modifier l'énoncé du métathéorème 12 [p. 11] si l'ebf A est fermée?

METATHEOREME 14 - Une ebf et sa fermeture sont logiquement valides ensemble.

Démonstration: il est nécessaire d'établir que:

1) Si A est valide, alors $(\forall v)A$ l'est aussi:
   Si $\models A$ alors $\models (\forall v)A$, (v désigne une variable quelconque); et
2) Si $(\forall v)A$ est valide, alors A l'est aussi:
   Si $\models (\forall v)A$ alors $\models A$, (v désigne une variable quelconque).

Raisonnons ainsi:

1) Admettons par hypothèse que A est logiquement valide: $\models A$. Quelle que soit l'interprétation I, on a donc $val(A) = \top$. L'application Ψ_V peut donc attribuer n'importe quelle image à la variable v, l'expression A conserve la valeur $\top$. Dit autrement, $val(A) = \top$ quelle que soit l'image de la variable v et quelle que soit l'interprétation I. La définition 24, clause 5, permet de conclure que $(\forall v)A$ est également valide: $\models (\forall v)A$.
2) Admettons par hypothèse que $(\forall v)A$ est logiquement valide: $\models (\forall v)A$. Dans ce cas, le raisonnement est de la même nature que le précédent; nous ne le formulerons donc pas.

Remarque: Le métathéorème 14 montre davantage que simplement la conservation de la propriété "d'être logiquement valide" à travers la règle GEN. Il établit également que la règle d'élimination du quantificateur universel conserve aussi cette propriété.

7.2 Où il est question des axiomes

Les trois premiers schémas d'axiome de L possèdent la même forme que ceux de L^0. Dans ce dernier système, nous avions montré que les axiomes étaient logiquement valides en exposant un raisonnement qui se fondait sur l'unique présence de la valeur $\top$ dans une table de vérité -une tautologie. Il n'est pas possible de procéder de la même manière dans un système qui autorise une substitution à partir d'un ensemble d'ebf qui possède notamment des formes quantifiées. Nous effectuerons un détour en raisonnant ainsi:

> Quel que soit le schéma d'axiome A1-A3 considéré, nous obtenons un axiome en substituant aux métavariables, des ebf de L. L'évaluation de chaque ebf -avec ou sans variables, avec ou sans quantificateurs- conduit soit à la valeur $\top$, soit à la valeur $\bot$. Il est donc possible

d'envisager à nouveau une combinatoire des valeurs de vérité d'un axiome et de déterminer que sa table de vérité résultante possède une qualité de l'ordre de la tautologie: à savoir, ne contenant que la valeur $\top$.

Nous pouvons poursuivre notre raisonnement et établir que tout schéma de tautologie de L^0 auquel est substituée, à chacune de ses métavariables, une ebf de L, possède également cette qualité de l'ordre de la tautologie.

DEFINITION 28 -instance de tautologie- - On appelle instance de tautologie dans L, le résultat de la substitution d'ebf de L dans un schéma de tautologie de L^0.

METATHEOREME 15 - Les schémas d'axiome A1-A3 fournissent des instances de tautologie dans L.

METATHEOREME 16 - Les schémas d'axiome A1-A3 sont logiquement valides.

METATHEOREME 17 - Le schéma d'axiome A4 est logiquement valide:
$\models (\forall v)A(v) \supset A(v/t)$ si t est libre pour v dans A(v).

Démonstration: Donnons-nous une interprétation I quelconque. Deux cas peuvent se présenter:

1) $val((\forall v)A(v)) = \top$
2) $val((\forall v)A(v)) = \bot$

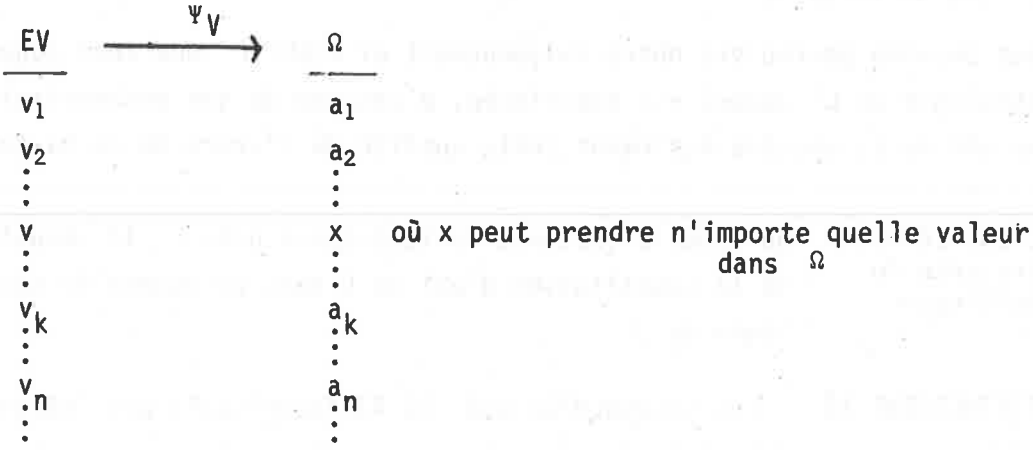
Etude du cas 1):
La clause 5 de la définition 24 stipule que $val((\forall v)A(v)) = \top$ ssi $val(A(v)) = \top$ quelle que soit l'image que ψ_V a attribuée à v. Donc en particulier si cette image est $\psi_T(t)$, ce qui signifie que $val(A(t)) = \top$.
Le schéma d'axiome A4 a la forme d'une conditionnelle dont le conséquent possède la valeur $\top$. Le raisonnement est tenu pour une interprétation quelconque [rien n'a été spécifié à son sujet], le schéma d'axiome A4 est donc, dans ce cas, logiquement valide.

Q u e s t i o n:

54. Par quel raisonnement s'assure-t-on que le schéma A4 est logiquement valide dans le deuxième cas?

R e m a r q u e: Le raisonnement très simple ci-dessus dissimule la raison pour laquelle A4 stipule que t doit être libre pour v dans A(v). Voici ce qu'il cache.

Poser que val((¥v)A(v)) = ⊤ revient à dire que val(A(v)) = ⊤ pour une application Ψ_V de la forme:



Supposons que dans l'expression (¥v)A(v)⊃A(v/t), le terme t ne soit pas libre pour v dans A(v). C'est dire que le terme t contient une variable v_k libre. Relativement à l'application Ψ_V, v_k possède une image, a_k par exemple. C'est également dire que v_k est liée dans l'expression A. Il faudrait donc que Ψ_V attribue à v_k non pas l'image a_k, qui donne une seule valeur dans Ω, mais n'importe quelle valeur dans Ω, ce qui n'est pas garanti.

Considérons l'exemple suivant:

$$A(v) =df \sim(\forall v_k)\sim p_1^2 v v_k$$

p_1^2 : "être différent" $\Omega = \mathbb{N}$

Le terme t est v_k et $\Psi_V(v_k) = a_k$.

Interprétons l'expression (¥v)A(v): "Pour tout nombre naturel x, il existe un nombre y tel que x est différent de y". Ce qui est vrai et donc val((¥v)A(v)) = ⊤. Ceci revient à dire que val(A(v)) = ⊤ également pour l'image de la variable v_k attribuée par Ψ_V: $\Psi_V(v_k) = a_k$.

Mais, $\sim(\forall v_k)\sim(p_1^2 v_k v_k)$ est fausse. En effet, il n'existe aucun nombre différent de lui-même.

METATHEOREME 18 - Le schéma d'axiome A5 est logiquement valide.

Démonstration: Raisonnons par l'absurde.
Supposons que (¥v)(B⊃A(v))⊃(B⊃(¥v)A(v)) ne soit pas valide. Il existe donc une interprétation I telle que:
val((¥v)(B⊃A(v))) = ⊤ et val(B⊃(¥v)A(v)) = ⊥
(* et **)

* $(\forall v)(B \supset A(v))$ est donc vraie quelle que soit l'image de v, et par la clause 5 de la déf. 24:

⊠ $val(B \supset A(v)) = \top$

** La fausseté de l'expression $B \supset (\forall v)A(v)$ conduit à :

⊠⊠ $val(B) = \top$ et $val((\forall v)A(v)) = \bot$

Ceci revient à admettre l'existence d'une image de v pour laquelle:

⊠⊠⊠ $val(A(v)) = \bot$

L'hypothèse restrictive du schéma d'axiome A5 stipule que B ne contient pas v libre, donc peu importe l'image que l'interprétation attribue à v et l'on a toujours $val(B) = \top$.

En considérant ⊠ et ⊠⊠ on obtient : $val(A(v)) = \top$

ce qui contredit ⊠⊠⊠

METATHEOREME 19 - Tout théorème de L est logiquement valide:

Si $\vdash_L A$ alors $\models_L A$

Démonstration: Les schémas d'axiome A1-A3 fournissent des instances de tautologie dans L et sont donc logiquement valides[Mth. 16, p. 23].

Les schémas d'axiome A4 et A5 sont logiquement valides [Mth. 17, 18, pp. 23-24].

Les règles MP et GEN préservent la propriété "d'être logiquement valide" [Mth. 14, p. 22].

Q u e s t i o n :

55. Sous quelle condition relative au terme t, l'expression suivante est-elle logiquement valide? $\models p_1^1 t \supset (\exists v) p_1^1 v$

METATHEOREME 20 - L'expression $(\forall v_i)A(v_i) \equiv (\forall v_k)A(v_k)$ est un théorème si les deux conditions suivantes sont remplies:

1) v_k est libre pour v_i dans $A(v_i)$
2) v_k ne figure pas libre dans $A(v_i)$

Q u e s t i o n s :

56. L'expression suivante satisfait-elle aux deux conditions du Mth. 20?
$(\forall v_1)(p_1^1 v_1 \supset (\forall v_3) p_1^2 v_2 v_3) \equiv (\forall v_4)(p_1^1 v_4 \supset (\forall v_3) p_1^2 v_2 v_3)$

57. Pourrait-on utiliser v_2 à la place de v_4? et v_3? et v_5?

58. La variable v_i est-elle libre pour v_k dans $A(v_k)$?

59. $A(v_k)$ contient-il v_i libre ?

Démonstration du métathéorème 20

1. $(\forall v_i)A(v_i) \supset A(v_k)$	A4, et condition 1
2. $(\forall v_k)((\forall v_i)A(v_i) \supset A(v_k))$	1, GEN
3. $(\forall v_i)A(v_i) \supset (\forall v_k)A(v_k)$	2, A5 et condition 2
4. $(\forall v_k)A(v_k) \supset A(v_i)$	A4, et question 58
5. $(\forall v_i)((\forall v_k)A(v_k) \supset A(v_i))$	4, GEN
6. $(\forall v_k)A(v_k) \supset (\forall v_i)A(v_i)$	5, A5, et question 59
7. $(\forall v_i)A(v_i) \equiv (\forall v_k)A(v_k)$	3, 6, déf. "$\equiv$"

Questions :

60. Relativement au nom des variables liées, que nous autorise ce métathéorème?

61. Comment satisfaire sans peine les conditions 1) et 2) du Mth. 20?

62. Une ebf fermée "dit"-elle quelque chose sur les variables qu'elle contient?

8. NON-CONTRADICTION ET CONSISTANCE DES SYSTEMES DU PREMIER ORDRE

Il est nécessaire de s'assurer que les systèmes du premier ordre purs sont non contradictoires. Pour le montrer il nous faut passer par une modification des ebf de L. Cette modification consiste à transformer toutes les ebf de L en des ebf qui se caractérisent par le fait qu'elles appartiennent au sous-langage L^0 de L. Il s'agit en quelque sorte d'une projection interne qui réduit l'écriture des expressions quantifiées à celle d'expressions qui, en plus des foncteurs logiques, ne contiennent que des prédicats de degré zéro.

Soit A une ebf quelconque de L. Nous appellerons formule propositionnelle associée (fpa) à A l'expression propositionnelle B obtenue en supprimant tous les termes de A et les quantificateurs de A, et en remplaçant chaque symbole de prédicat de degré $\underline{d}$, $\underline{d}>0$, par un symbole de prédicat de degré zéro. Il y a bien sûr quelques précautions à prendre, mais celles-ci sont triviales.

Précautions

- Remplacer chaque occurrence d'un prédicat de degré $\underline{d}$: $\underline{d}>0$, par un même prédicat de degré zéro.
- Associer aux prédicats différents d'indice ou de degré ($\underline{d}>0$) des prédicats de degré zéro différents.
- Choisir pour les prédicats de degré zéro liés à la fpa à une ebf A des indices autres que l'indice d'un prédicat de degré zéro appartenant déjà à A.

Exemples:	ebf de L	fpa
1)	$(\forall v_1)(p_1^1 v_1 \supset p_2^1 v_1) \wedge p_1^1 v_1$	$(p_3^0 \supset p_4^0) \wedge p_3^0$
2)	$(\forall v_1) p_1^2 v_1 c_1 \supset p_1^1 c_1$	$p_1^0 \supset p_2^0$
3)	$(\forall v_1)(p_1^3 c_1 v_1 c_1 \supset p_6^0)$	$p_5^0 \supset p_6^0$

Questions :

63. Une ebf logiquement valide dans L peut-elle posséder une fpa qui est une tautologie?
64. Quelle est la fpa de A?
    $A =_{df} (\forall v_1)(p_1^0 \supset p_1^2 v_1 c_1) \supset (p_1^0 \supset (\forall v_1) p_1^2 v_1 c_1)$

Avant d'exposer la démonstration de la non-contradiction du système L, il nous faut justifier le bien-fondé de la réduction de toute ebf de L en une fpa. Pour ce faire, considérons le système L ainsi qu'un domaine d'objets ne possédant qu'un et un seul élément: $\Omega = \{*\}$. Dans ce contexte, quelle que soit l'interprétation proposée, la situation est la suivante:

- Toute constante de L a pour image l'élément $*$.
- Toute variable de L a pour image l'élément $*$.
- Tout symbole de prédicat de degré zéro a pour image un élément du domaine des valeurs: soit $\top$, soit $\bot$.
- Tout symbole de prédicat de degré $\underline{d}$, $\underline{d}>0$, a pour image un élément de l'organisation relationnelle: $\mathcal{P}(\Omega^d)$; construisons cette organisation:
  1. $\Omega = \{*\}$ $\mathcal{P}(\Omega) = \{\Omega, \emptyset\}$
  2. $\Omega^2 = \{<*, *>\}$ $\mathcal{P}(\Omega^2) = \{\{<*, *>\}, \emptyset\}$
  3. $\Omega^d = \{\underbrace{<*, *,..., *>}_{\underline{d} \text{ fois}}\}$ $\mathcal{P}(\Omega^d) = \{\{\underbrace{< *, *,..., *>}_{\underline{d} \text{ fois}}\}, \emptyset\}$

  Il n'existe pas d'autres possibilités. Ainsi, dans une procédure interprétative liée à un domaine d'objets ne possédant qu'un unique élément, tout prédicat est lié au principe du double choix.
- Tout symbole de foncteur de degré $\underline{n}$, $\underline{n}>0$ a pour image un élément de l'organisation fonctionnelle $\mathcal{P}(\Omega^n \times \Omega)$ dont les arguments sont composés avec l'unique élément de Ω; il s'agit donc de : $\{<<*, *,..., *>, *>\}$.

Il s'ensuit que:

I. Le quantificateur ne joue plus aucun rôle. Une formule quantifiée ne "dit" rien de plus que ce que "dit" le champ de son quantificateur. Le quantificateur est donc -dans ce cas- inutile. Nous le supprimerons donc.

II. D'autre part, il n'existe pour toute formule atomique $p_i^d\ t_1 \ldots t_d$ que deux -et seulement deux- évaluations possibles. Elle ne peut donc prendre qu'une fois la valeur $\top$, et qu'une fois la valeur $\bot$.
L'image d'un p_i^d quelconque est soit $\emptyset$, soit $\{\underbrace{<*, *,..., *>}_{\underline{d} \text{ fois}}\}$

L'évaluation de la formule atomique à laquelle il est associé ne considère donc que ces deux possibilités:

$$val(p_i^d t_1 \ldots t_d) = \begin{cases} \top \text{ si } <\Psi_T(t_1),\ldots,\Psi_T(t_d)> \in \Psi_p(p_i^d). \text{ Càd dans le cas où } \Psi_p(p_i^d) = \underbrace{\{<*, *,..., *>\}}_{\underline{d} \text{ fois}} \\ \bot \text{ si } <\Psi_T(t_1),\ldots,\Psi_T(t_d)> \notin \Psi_p(p_i^d). \text{ Et dans ce cas, } \Psi_p(p_i^d) = \emptyset \end{cases}$$

Une formule atomique se comporte donc comme un prédicat de degré zéro.

Voyons cela plus concrètement sur un exemple.

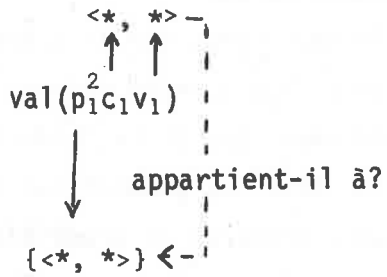
Soit A =df $p_1^2 c_1 v_1$ et $\Omega = \{*\}$ et étudions les 2 interprétations possibles.

I'.

$\Psi_C(c_1) \rightarrow *$

$\Psi_C(v_1) \rightarrow *$

$\Psi_p(p_1^2) \rightarrow \{<*, *>\}$



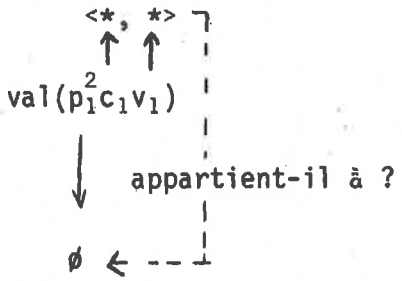
oui! donc $val(p_1^2 c_1 v_1) = T$

I".

$\Psi_C(c_1) \rightarrow *$

$\Psi_C(v_1) \rightarrow *$

$\Psi_p(p_1^2) \rightarrow \emptyset$



non! donc $val(p_1^2 c_1 v_1) = \perp$

Contre-exemple

Soit A =df $p_1^2 c_1 v_1$ et $\Omega' = \{*, \square\}$

En fonction des termes c_1 et v_1, il y a déjà quatre interprétations possibles.

	I_1	I_2	I_3	I_4
$\Psi_C(c_1) \rightarrow$	*	*	□	□
$\Psi_V(v_1) \rightarrow$	*	□	*	□

Et pour considérer le jeu des interprétations possibles pour p_1^2, il est nécessaire de construire $\mathcal{P}(\Omega'^2)$.

Q u e s t i o n :

65. Construire l'ensemble des parties de Ω'^2: $\mathcal{P}(\Omega'^2)$

Chacun des éléments de $\mathcal{P}(\Omega'^2)$ (question 65) est une image possible pour le prédicat p_1^2. Il possède donc 16 interprétations possibles.

Dans ce cas, l'ebf $p_1^2 c_1 v_1$ possède 4X16 = 64 interprétations possibles. Elle ne se comporte donc pas, dans le processus interprétatif, comme un prédicat de degré zéro.

Ce qui précède justifie la transformation proposée.

METATHEOREME 21 - Le système formel L est non contradictoire.

Démonstration. La fpa de chacun des axiomes conçus sur les schémas d'axiome A1-A3 est logiquement valide. [Mth. 16]

La fpa d'un axiome conçu sur le schéma d'axiome A4 est logiquement valide.

Si A est une fpa, A⊃A est un théorème et donc logiquement valide.

La fpa d'un axiome conçu sur le schéma d'axiome A5 est logiquement valide.

Si A et B sont des fpa, (A⊃B)⊃(A⊃B) est un théorème et donc logiquement valide.

Le modus ponens préserve la propriété d'être logiquement valide pour les fpa. [Mth. 5]

La règle GEN préserve la propriété d'être logiquement valide pour les fpa. En effet la fpa à A et à (∀v)A est la même. La règle GEN se réduit à une règle de répétition.

Il suit de ce qui précède que tout théorème de L possède une fpa qui est logiquement valide.

Posons l'hypothèse absurde suivante: Dans L, on a à la fois A est un théorème et ∿A est un théorème. Chacune de leur fpa B et ∿B est donc logiquement valide: $\models B$ et $\models \sim B$. Ce résultat met en évidence que le fragment L^0 de L est contradictoire, ce qu'il n'est pas [Mth.9]. On ne peut donc avoir à la fois $\vdash A$ et $\vdash \sim A$. L est donc non contradictoire.

METATHEOREME 22 - Le système L est consistant.

Démonstration. Pour le montrer, il suffit d'exhiber une ebf de L qui ne soit pas un théorème. Mais nous savons que le fragment L^0 de L est consistant. Il en résulte que L l'est aussi.

Q u e s t i o n s

66. L^0 est décidable [Mth. 11]. En résulte-t-il que L est décidable?

67. Démontrer que ni $(\forall v)p_1^1 v$, ni $\sim(\forall v)p_1^1 v$ n'est un théorème de L.

METATHEOREME 23 - Le système L n'est pas catégorique [cf. déf. 17].

Démonstration. cf. question 67 et déf. 17

Variante - L^0 n'est pas catégorique, [cf. question 26, I] il en résulte que L ne l'est pas.

DEFINITION 29 -syntaxiquement complet- - Un système formel est syntaxiquement complet ssi aucun schéma d'ebf non prouvable dans le système ne peut lui être adjoint comme schéma d'axiome sans le rendre contradictoire. [Comparer avec déf. 16].

Nous montrerons que le système L n'est pas syntaxiquement complet alors que son fragment L^0 l'est. A cette fin, posons préalablement trois définitions et proposons un résultat: le métathéorème 24.

DEFINITIONS 30.1 -modèle- - Une interprétation I est un modèle pour une ebf A d'un système S si et seulement si val(A) = $\top$ relativement à I.

30.2 - Une interprétation I est un modèle pour un ensemble Γ d'ebf d'un système S si et seulement si toute $A_i \in \Gamma$ est telle que val(A_i) = $\top$ relativement à I.

30.3 - Un système du premier ordre possède un modèle si et seulement si l'ensemble de ses théorèmes en possède un. [Comparer avec déf. 8].

METATHEOREME 24 - Tout système du premier ordre qui admet un modèle est non contradictoire.

Démonstration. Soit S un système formel du premier ordre qui possède un modèle I.
Supposons [hypothèse absurde] que S soit contradictoire.

Il existe donc une ebf A telle que $\vdash_S A$ et $\vdash_S \sim A$. L'ensemble des théorèmes de S ayant un modèle, il en résulte qu'il existe une interprétation I telle que $val_I(A) = \top$ et $val_I(\sim A) = \top$. Mais, quelle que soit l'interprétation, $val(\sim A) = \top$ ssi $val(A) = \bot$. Ceci est également valable pour l'interprétation I. Il n'est donc pas possible d'obtenir simultanément $val_I(\sim A) = \top$ et $val_I(A) = \top$. L'hypothèse absurde était bien absurde et le système S est non contradictoire.

COROLLAIRE Un système formel contradictoire n'admet pas de modèle.

Q u e s t i o n :

68. Comment justifier ce corollaire?

Le métathéorème 24 est très puissant. En effet, soit S un système appliqué du premier ordre. On sait que sa "partie purement logique", c'est-à-dire L, est non contradictoire [Mth. 21]. Il suffira donc de trouver un seul modèle pour ses axiomes propres pour savoir que S est non contradictoire.

METATHEOREME 25 - Le système L n'est pas syntaxiquement complet.

Démonstration: Considérons le schéma d'ebf $A \supset (\forall v)p^1v$ où A est une expression fermée quelconque. Ce schéma n'est pas prouvable dans L.
En effet, supposons qu'il le soit: $\vdash A \supset (\forall v)p^1v$. Il s'ensuit que $\models A \supset (\forall v)p^1v$ [Mth. 19]. Cela signifie que $val(A \supset (\forall v)p^1v) = \top$ pour toute interprétation. Il est donc nécessaire que $val((\forall v)p^1v)$ conserve la valeur $\top$ quelle que soit l'interprétation, mais ceci n'est pas le cas [question 67]. Ce schéma peut être adjoint aux schémas d'axiome de L sans le rendre pour autant contradictoire.
En effet, soit I, une interprétation dont le domaine d'objets Ω est l'ensemble de tous les termes ne possédant aucune variable. Attribuons à p^1 une image qui soit l'ensemble de tous les termes ne possédant aucune variable, donc Ω lui-même [en compréhension: "possède la propriété d'être un terme ne possédant aucune variable"].
Dans cette interprétation, $val(p^1v) = \top$ quelle que soit l'image de la variable v. Donc $val((\forall v)p^1v) = \top$ relative-

ment à l'interprétation I. Et davantage encore, $val(A \supset (\forall v)p^1v) = \top$ relativement à l'interprétation I.
Considérons le système L* conçu sur le système L auquel on adjoint comme nouveau schéma d'axiome, le schéma $A \supset (\forall v)p^1v$.

$$L^* : L + \underbrace{A \supset (\forall v)p^1v}_{\text{schéma d'axiome}}$$

Les schémas d'axiome A1-A5 sont logiquement valides.
Le modus ponens conserve la validité logique quelle que soit l'interprétation, donc également pour I.
La règle GEN conserve la validité logique quelle que soit l'interprétation, donc également pour I.
Le schéma d'axiome $A \supset (\forall v)p^1v$ a la valeur $\top$ relativement à I.
Il résulte que l'ensemble des théorèmes de L* est un ensemble dont tous les éléments ont la valeur $\top$ relativement à I.
I est donc un modèle pour L* [déf. 30.3]. Et possédant un modèle, L* est donc non contradictoire [Mth. 24].
Il est donc possible d'adjoindre à L comme schéma d'axiome, un schéma d'ebf non prouvable dans L, sans rendre pour autant le système contradictoire.
Le système L n'est pas syntaxiquement complet.

METATHEOREME 26 - Le fragment L^0 de L est syntaxiquement complet.

Démonstration: Soit A, un quelconque schéma d'ebf non prouvable dans L^0, et soit $B_1, B_2, \ldots, B_n$ ses n composants schématiquement distincts. Le schéma A ne peut pas être un schéma de tautologie [contraposée du Mth. 10]. Il existe donc une inteprétation I pour laquelle $val(A) = \bot$. Considérons le système L^{0*} dans lequel le schéma A est un schéma d'axiome (ce n'est pas le cas dans L^0). Dans ce système toute expression résultant de A par substitution d'ebf aux B_i est un axiome. Considérons une telle transformation. Soit C l'axiome résultant du schéma d'axiome A par la substitution suivante:
$B_i/p^0 \supset p^0$ si $val(B_i) = \top$ relativement à I.
$B_i/\sim(p^0 \supset p^0)$ si $val(B_i) = \bot$ relativement à I.
L'ebf C est un théorème (axiome) de L^{0*}. Mais quelle que soit l'interprétation considérée [$val(p^0) = \top$ ou $val(p^0) = \bot$],

val(C) = $\bot$. Il en résulte [déf. 24, clause 3] que val(~C) = $\top$ quelle que soit l'interprétation: $\models$~C. Il s'ensuit que ~C est un théorème: $\vdash$~C [Mth. 10].
Ainsi dans L^0*, on a $\vdash$C et $\vdash$~C. L^0* est donc contradictoire.
Le schéma A était un schéma d'ebf non prouvable quelconque dans L^0. L^0 est donc syntaxiquement complet.

9. LA COMPLETUDE SEMANTIQUE DU SYSTEME L

Il s'agit maintenant de montrer que les ebf logiquement valides de L sont précisément les théorèmes de L. Cette démonstration nécessite un long détour. Nous devons en effet établir certains résultats qui dépassent "en puissance" l'étude du système L. Notre exposé se déroulera donc en quatre temps.

1. Où il sera question de l'extension d'un système formel et de la propriété d'"être dénombrable".
2. Où il sera montré que pour tout système S non contradictoire, il existe une extension non contradictoire et catégorique relativement à la fermeture.
3. Où il sera établi que tout système formel S non contradictoire possède un modèle dénombrable.
4. Où la complétude sera enfin démontrée.

Si nous insistons tant sur ce cheminement, c'est pour que l'on n'oublie pas la finalité de l'exposé.

9.1 Extension et "dénombrabilité"

DEFINITION 31 -extension- - Un système S* est une extension d'un système S ssi
1/ S* a mêmes symboles et mêmes règles que S.
2/ Tout théorème de S est un théorème de S*, et pas inversement.

Q u e s t i o n s :

69. Le système L est-il une extension du système L^0?
70. Une extension offre quel type de liberté?
Autrement dit, que faut-il ajouter à un système formel S pour obtenir une extension?
71. Peut-on obtenir une extension non contradictoire de L^0? et de L?

LEMME I - Si ~A est une ebf fermée de S telle que $\not\vdash_S \sim A$, alors l'extension S* de S obtenue en adjoignant A aux axiomes de S est non contradictoire.

Démonstration: Supposons S* contradictoire [hyp. absurde]. Il existe alors une ebf B de S* telle que:

(*) $\vdash_{S^*} B$ et $\vdash_{S^*} \sim B$.

Cette contradiction résulte de la présence de A comme axiome de S*. En effet, on a $\vdash_S (B \supset (\sim B \supset \sim A))$ donc on a également [déf. 31]

(**) $\vdash_{S^*} (B \supset (\sim B \supset \sim A))$.

Il résulte de (*) et (**) par deux applications de la règle MP que $\vdash_{S^*} \sim A$. D'autre part, l'expression ~A est prouvable dans S* parce que A est un axiome de ce système.

Il est donc possible de déduire ~A dans S à partir de l'ensemble d'hypothèses Γ : $\Gamma = \{A\}$.

$$A \vdash_S \sim A$$

L'expression A étant fermée, on peut utiliser le "théorème" de la déduction et obtenir

(+) $\vdash_S A \supset \sim A$

Mais $(A \supset \sim A) \supset \sim A$ est un schéma de théorème de S:

(++) $\vdash_S (A \supset \sim A) \supset \sim A$.

Il résulte que (+) et (++) par application de la règle MP que $\vdash_S \sim A$.

Ce résultat contredit l'hypothèse du Lemme I (~A n'est pas prouvable dans S: $\not\vdash_S \sim A$).

Ainsi l'extension S* de S obtenue en adjoignant A aux axiomes de S est non contradictoire.

Q u e s t i o n :

72. A-t-on restreint -et en quoi- la portée du Lemme I en supposant A fermée?

LEMME II - L'ensemble des ebf d'un système formel est dénombrable (on dit aussi énumérable).

R e m a r q u e s :

1. Nous exposerons ce résultat en nous basant sur l'existence des symboles de L. L'esprit de la démonstration est le même pour un quelconque système formel appliqué.

2. Il est nécessaire de se convaincre de l'existence d'une infinité de nombres premiers. Nous démontrerons ce résultat.
3. Il est nécessaire d'accepter le résultat arithmétique suivant:

> Tout nombre entier est le produit des puissances des nombres premiers qui le divisent; cette décomposition est unique à l'ordre près. (On parle de factorisation en produit de nombres premiers).

Conventions: soit q un nombre naturel;

$q^1 = q$; $q^0 = 1$ (q puissance 1, q puissance 0)

Rappel: Un nombre premier est un entier naturel qui possède exactement deux diviseurs: lui-même et 1.

La table des nombres premiers a été prolongée en 1979 jusqu'au cent millionième nombre premier qui est 2 038 074 743. [Dictionnaire des mathématiques. A. Bouvier et M. George, PUF, 1979].

THEOREME DE L'INFINITE DES NOMBRES PREMIERS -

Il existe une infinité de nombres premiers. Nous donnons la preuve d'Euclide [Eléments, IX. 20], elle est élégante et facile à comprendre.

Démonstration: Hyp. absurde: il existe un plus grand nombre premier, soit p_m ce nombre.

Nous allons montrer qu'il en existe un plus grand.

1. Construisons le nombre q formé en additionnant 1 au produit de tous les nombres premiers jusqu'à p_m. $q = (p_1 \cdot p_2 \cdot \ldots \cdot p_m)+1$
2. Le nombre q est plus grand que p_m.
3. Quel que soit le nombre premier p_i (ou quel que soit le produit de nombres premiers $p_1 \cdot p_2 \cdot \ldots \cdot p_i$) pris comme diviseur, le quotient consistera en un produit de nombres premiers, et il restera toujours le reste 1. Le nombre q ne peut donc pas être factorisé en un produit de nombres premiers.
4. Mais le nombre q est ou non un nombre premier.

4.1 Si le nombre q est un nombre premier, il existe donc un nombre premier plus grand que p_m [cf. 2].

4.2 Si le nombre q n'est pas un nombre premier, il peut être factorisé en produit de nombres premiers. Ce qui n'est pas le cas [cf. 3].

5. Il existe donc un nombre premier plus grand que p_m.

La numérotation de Gödel

La démonstration du Lemme 2 passe par l'établissement de la numérotation de Gödel. L'idée est la suivante: assigner des entiers de manière systématique à tout assemblage fini de symboles, si long soit-il, qui forme les ebf de L.

> On peut créditer Leibniz d'une anticipation de l'idée de représenter les expressions d'un langage par des nombres entiers.
> (Dieudonné, 1978).

Première démarche - Attribution d'un nombre de Gödel à chaque symbole de l'alphabet de L [le nombre de Gödel d'un symbole est appelé un g-nombre].
Il s'agit d'une application g qui à chaque symbole de l'alphabet de L attribue un nombre univoquement déterminé:

$$g : \{\text{symboles de L}\} \longrightarrow \mathbb{N}$$

$g: (\ \longmapsto\ 3$
$g:)\ \longmapsto\ 5$
$g: \sim\ \longmapsto\ 7$
$g: \supset\ \longmapsto\ 9$
$g: \forall\ \longmapsto\ 11$
$g: c_i\ \longmapsto\ 5+8.i \qquad i>0$
$g: v_i\ \longmapsto\ 7+8.i \qquad i>0$
$g: p_i^n\ \longmapsto\ 9+8.(2^n.3^i) \qquad n\geq 0 \quad \text{et} \quad i>0$
$g: f_i^n\ \longmapsto\ 11+8.(2^n.3^i) \qquad n> 0 \quad \text{et} \quad i>0$

Cette application n'est pas la seule possible. Toutes les applications envisageables doivent posséder la même propriété, à savoir: ne pas attribuer à deux symboles de l'alphabet une même image.

Exemples:

$g(c_1) = 5+8.1 = 13$; 13 est le g-nombre de c_1
$g(p_3^2) = 9+8.(2^2.3^3) = 873$; 873 est le g-nombre de p_3^2

Q u e s t i o n s :

73. Calculer les g-nombres de c_2 et de f_2^2.
74. Le nombre 72 est-il le g-nombre d'un symbole de l'alphabet de L? et 81? Si oui, duquel?

Deuxième démarche - Attribution d'un nombre de Gödel à chaque ebf de L.
Toute ebf se présente comme une concaténation de symboles s_i de l'alphabet de L.

Soit A : $s_1 \ s_2 \ s_3 \ \text{---} \ s_k$

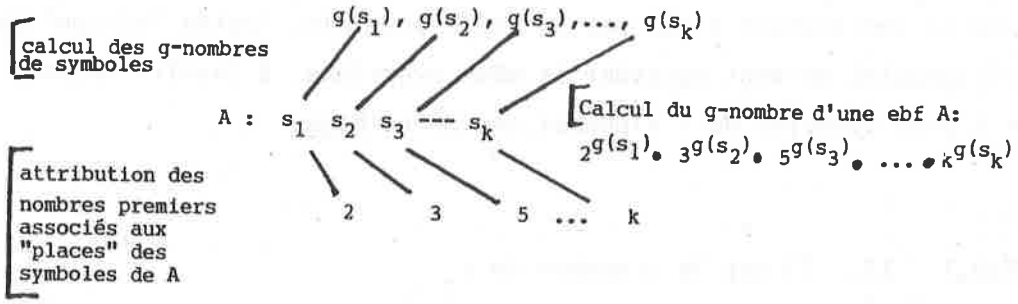
I. Chaque symbole possède une "place" bien déterminée dans une ebf.
A la première place, nous attribuons le premier nombre premier, à la deuxième place, nous attribuons le deuxième nombre premier,..., à la k-ième place nous attribuons le k-ième nombre premier.

première place:	$\longmapsto$	2	premier nombre premier
deuxième place:	$\longmapsto$	3	deuxième nombre premier
⋮		⋮	⋮
k-ième place	$\longmapsto$	k	le k-ième nombre premier

II. Indépendamment de la place des symboles, chaque symbole possède un nombre de Gödel univoquement déterminé.

$s_1 \longmapsto g(s_1)$
$s_2 \longmapsto g(s_2)$
⋮
$s_k \longmapsto g(s_k)$

A l'aide de ces deux informations (I et II), il est possible de déterminer le nombre de Gödel d'une expression. Cette démarche s'effectue ainsi.



Le g-nombre d'une expression A possédant k symboles est le produit des k premiers nombres premiers, chacun étant élevé à la puissance du g-nombre du symbole associé à sa place.

Exemples

1) $A =_{df} (\forall v_1)p_1^1 v_1$

$$g(A) = 2^{g(()}\cdot 3^{g(\forall)}\cdot 5^{g(v_1)}\cdot 7^{g())}\cdot 11^{g(p_1^1)}\cdot 13^{g(v_1)}$$

$$= 2^3\cdot 3^{11}\cdot 5^{(7+8)}\cdot 7^5\cdot 11^{(9+8(2\cdot 3))}\cdot 13^{(7+8)}$$

$$= n \in \mathbb{N}$$

2) $75000 = 2^3 \cdot 3^1 \cdot 5^5$

3 est le g-nombre de (

1 n'est pas un g-nombre

5 est le g-nombre de)

75000 n'est pas un g-nombre associé à une ebf de L .

3) $2^7 \cdot 3^{13}\cdot 5^3$

7 est le g-nombre de ~

13 est le g-nombre de c_1

3 est le g-nombre de (

$2^7\cdot 3^{13}\cdot 5^3$ est un g-nombre, mais pas d'une ebf de L.

Q u e s t i o n s :

75. Calculer le nombre de Gödel de $p_1^0 \supset p_1^0$
76. Calculer le nombre de Gödel de $p_1^1 v_1 \supset p_1^2 c_1 c_2$
77. 2^{81} est-il le nombre de Gödel d'une ebf?
78. Quelle distinction de nature y a-t-il entre le g-nombre 81 et le g-nombre 2^{81} ?

L'unicité, à l'ordre près, d'une factorisation en produit de nombres premiers et l'existence d'une infinité de nombres premiers garantissent que toute ebf possède un et un seul g-nombre, et que ce g-nombre n'est attribué qu'à cette ebf.

Tout g-nombre d'une expression étant un entier naturel, il est possible d'ordonner l'ensemble des g-nombres des ebf. Au premier g-nombre attri-

buons le premier nombre naturel 1; au deuxième, le deuxième nombre naturel 2; ...; au k-ième, le k-ième nombre naturel. Agissant ainsi nous établissons une correspondance bi-univoque entre les g-nombres des ebf et $\mathbb{N}$. L'ensemble des ebf de L est donc dénombrable.

9.2 Extension - non-contradiction - catégoricité

DEFINITION 32 - -catégoricité relativement à la fermeture- Un système du premier ordre est catégorique relativement à la fermeture ssi pour chacune de ses ebf fermées A, on a soit $\vdash A$, soit $\vdash \sim A$.

METATHEOREME 27 - Si S est un système du premier ordre non contradictoire il existe une extension S* de S qui est non contradictoire et catégorique relativement à la fermeture.

Démonstration: Considérons l'énumération des ebf fermées de S. Elle est possible [Lemme II, p. 35].

$$\langle A_1, A_2, \ldots, A_n, A_{n+1}, \ldots \rangle$$

Construisons une suite de systèmes formels

$$\langle S^0, S^1, S^2, \ldots, S^n, S^{n+1}, \ldots \rangle$$

conçus de la manière suivante:

1. $S^0 = S$

2.1 $S^{n+1} = S^n$ si $\vdash_{S^n} \sim A_{n+1}$

2.2 $S^{n+1} = S^n + A_{n+1}$ si $\nvdash_{S^n} \sim A_{n+1}$.

Dans le cas 2.2, le système S^{n+1} est une extension de S^n, extension réalisée en ajoutant A_{n+1} aux axiomes de S^n.

Supposons [ce qui est totalement arbitraire] que l'énumération des ebf fermées de S commence comme suit:

$A_1 = p_1^0$, $A_2 = p_1^0 \wedge \sim p_1^0$, $A_3 = p_1^1 c_1, \ldots$

1. On a : $S^0 = S$ clause 1) puis, comme $\sim p_1^0$ n'est pas un théorème de S^0 : $\nvdash_{S^0} \sim p_1^0$,
2. on obtient : $S^1 = S^0 + p_1^0$ clause 2.2). Ensuite, $\sim(p_1^0 \wedge \sim p_1^0)$ est un théorème de S^0, il est donc -par définition d'une extension- également théorème de l'extension S^1: $\vdash_{S^1} \sim(p_1^0 \wedge \sim p_1^0)$.
3. Il en résulte: $S^2 = S^1$ clause 2.1). Si l'on montre que la négation de la troisième ebf fermée n'est pas un théorème de S^2, on aura alors

4. $S^3 = S^2 + p_1^1 c_1$ clause 2.2) etc.

Considérant la suite des systèmes formels $<S^0, S^1, S^2, \ldots, S^n, \ldots>$ formons un nouveau système formel S*. Ce système est obtenu à partir de S en ajoutant tous les axiomes qui ont engendré les S^i. Sous ces conditions:

a] S* est une extension de S. En effet, S* a mêmes symboles et mêmes règles que S et tout théorème de S est un théorème de S*.

b] S* est non contradictoire.

Démonstration: par induction sur l'indice i des S^i.

Base : i = 0

S^0 est S et S est supposé non contradictoire.

Hypothèse d'induction: S^i est non contradictoire.

Pas d'induction: Montrons que le système suivant S^{i+1} est aussi non contradictoire. Il y a deux cas à étudier:

1] $\sim A_{i+1}$ est un théorème de S^i. Il en résulte que $S^{i+1} = S^i$. S^i est non contradictoire [hyp. d'induction] donc S^{i+1} est non contradictoire.

2] $\sim A_{i+1}$ n'est pas un théorème de S^i. Dans ce cas $S^{i+1} = S^i + A_{i+1}$. S^{i+1} est non contradictoire [Lemme I].

c] S* est catégorique relativement à la fermeture.

Démonstration: Soit B une ebf fermée quelconque de S*. Elle est nécessairement dans la liste $<A_1, A_2, \ldots, A_n, \ldots>$.
Admettons qu'il s'agisse de A_{k+1}. Deux situations sont possibles:
ou bien $\sim A_{k+1}$ est un théorème dans S^k

ou bien il ne l'est pas et A_{k+1} est un théorème (axiome de S^{k+1}).

Etant donné que S* contient toutes les ebf rajoutées comme axiomes, on a bien
soit $\vdash_{S^*} A_{k+1}$, soit $\vdash_{S^*} \sim A_{k+1}$

DEFINITION 33 -théorie axiomatique- - Une théorie dans laquelle l'ensemble des axiomes est décidable est appelée une théorie axiomatique.

Le système L est une théorie axiomatique.

Remarques:

- La preuve du métathéorème 27 ne permet pas de construire effectivement S*. Il se peut en effet que l'on ne puisse pas décider si une ebf $\sim A_{k+1}$ est ou n'est pas un théorème de S^k. Le système S* peut ne pas être une théorie axiomatique.
- Le métathéorème 27 est connu dans la littérature comme le lemme de Lindenbaum. "Selon un théorème bien connu, dû à A.Lindenbaum, tout un ensemble de propositions [non contradictoire] d'une théorie déductive quelconque peut être étendu pour former un système à la fois [catégorique relativement à la fermeture] et [non contradictoire]." [TARSKI, 1974, II, p. 123].

  Dans le premier tome Tarski démontre ce théorème [th. 56] et ajoute le commentaire suivant:

  > "...bien que tous les systèmes [non contradictoires] que l'on connaisse soient [non catégoriques relativement à la fermeture], le théorème 56 offre, au moins une possibilité théorique, d'étendre ces systèmes pour qu'ils deviennent à la fois [catégoriques relativement à la fermeture] et [non contradictoires]. La question se pose alors de savoir comment cette extension peut être construite pour être "effective", aussi naturelle que possible, et en même temps s'accorder avec tel ou tel point de vue philosophique". [1974, I, p. 102; première publication 1930].

- Nous avons modifié la terminologie utilisée par Tarski afin de ne pas introduire de confusion. En effet, les termes tels que "complétude", "consistance" n'ont pas chez Tarski la même acception que celle que nous leur avons attribuée. Ajoutons que cette malheureuse divergence terminologique est très générale.

9.3 Non-contradiction - modèle - "dénombrabilité"

METATHEOREME 28 - Tout système du premier ordre S qui est non contradictoire possède un modèle et ce modèle est dénombrable.

Démonstration:

I. Construction d'un système non contradictoire S^0 à partir de S.

II. "Construction" d'une extension non contradictoire S^∞ de S^0 puis d'une extension S* de S^∞, non contradictoire et catégorique relativement à la fermeture.

III. Construction d'un modèle I de S*, modèle dénombrable.

IV. Démonstration que le modèle dénombrable I de S* est également un modèle de S.

I.1 Construction d'un système S^0 à partir de S. Soit $a_1, a_2, \ldots, a_n, \ldots$ une liste dénombrable de constantes d'objet toutes différentes des c_i de S. Posons alors:

$$S^0 = S + \{a_1, a_2, \ldots, a_n, \ldots\}$$

Q u e s t i o n s:

79. S^0 est-il une extension de S?

80. S^0 a-t-il d'autres schémas d'axiome que S? d'autres axiomes?

I.2 S^0 est non contradictoire.

Démonstration: Supposons S^0 contradictoire [hyp. absurde]. Il existe donc une ebf A telle que $\vdash_{S^0} A \wedge \sim A$. Cela signifie que dans S^0, on a une preuve de $A \wedge \sim A$. A partir de cette preuve, opérons la transformation suivante: chaque fois qu'on rencontre une constante a_i, on la remplace par une v_j qui ne figure nulle part dans la preuve. On obtient donc ainsi une preuve dans S d'une expression $A' \wedge \sim A'$. S serait donc contradictoire, ce qui est incompatible avec l'hypothèse du métathéorème 28. S^0 est donc non contradictoire.

II.1 Construction d'une extension non contradictoire S^∞ de S^0. Enumérons les ebf de S^0 qui ne possèdent qu'une seule variable libre [le lemme II, p. 35 rend ceci possible]:

a] $A_1(v_{i_1}), A_2(v_{i_2}), \ldots, A_k(v_{i_k}), \ldots$

Donnons-nous une liste de constantes propres à S^0.

b] $a_{j_1}, a_{j_2}, \ldots, a_{j_k}, \ldots$

Soit alors l'ebf suivante:

c] $s_k =_{df} \sim(\forall v_{i_k}) A_k(v_{i_k}) \supset \sim A_k(a_{j_k})$ où a_{j_k} est la première constante de notre liste qui n'apparaît pas dans A_k.

Construisons maintenant une suite de systèmes S^n ainsi:

$S^n = S^0 + S^1 + S^2 + \ldots + S_n$ [le système S^0 auquel on ajoute les n premiers s_k considérés comme axiomes].

Concevons alors le système S^∞ de la manière suivante:

$$S^\infty = S^0 + \underline{\text{tous}} \text{ les } s_i.$$

Q u e s t i o n s :

81. Quels sont les axiomes de S^2?
82. S^∞ est-il une extension de S? de S^2?
83. Pourquoi peut-on garantir qu'une preuve dans S^∞ est toujours dans un S^n où n est fini?

Démontrons que cette extension S^∞ est non contradictoire.

Démonstration: par induction sur l'indice n des S^n.

Base : n = 0

S^0 est non contradictoire [I.2].

Hypothèse d'induction: S^n est non contradictoire.

Pas d'induction: Prouvons que $S^{n+1} = S^n + s_{n+1}$ est non contradictoire.

Raisonnons par l'absurde.

Si S^{n+1} est contradictoire [hyp. absurde] il existe une ebf A telle que $\vdash_{S^{n+1}} A \wedge \sim A$.

Mais S^{n+1} contient les théorèmes de S^0 qui, à son tour, contient les théorèmes de S; on a donc $\vdash_{S^{n+1}} (A \wedge \sim A) \supset B$, et ceci quelle que soit l'ebf B, et par la règle MP on obtient: $\vdash_{S^{n+1}} B$, quelle que soit B.

Donc en particulier: $\vdash_{S^{n+1}} \sim s_{n+1}$.

La construction de S^{n+1} à partir de S^n est telle que $\sim s_{n+1}$ est déductible de s_{n+1} dans S^n: $s_{n+1} \vdash_{S^n} \sim s_{n+1}$.

L'expression s_{n+1} étant fermée [cf. construction], on peut utiliser le "théorème" de la déduction et obtenir:

1] $\vdash_{S^n} s_{n+1} \supset \sim s_{n+1}$

Mais on a aussi dans S donc dans S^0 et dans S^n le théorème suivant: $\vdash_{S^n} (C \supset \sim C) \supset \sim C$ quelle que soit C, et en particulier:

2] $\vdash_{S^n} (s_{n+1} \supset \sim s_{n+1}) \supset \sim s_{n+1}$.

On obtient donc : $\vdash_{S^n} \sim s_{n+1}$ 1], 2], MP

c'est-à-dire: $\vdash_{S^n} \sim[\sim(\forall v_{i_{n+1}}) A_{n+1}(v_{i_{n+1}}) \supset \sim A_{n+1}(a_{j_{n+1}})]$

ce qui peut se transformer en:

(*) $\vdash_{S^n} \sim(\forall v_{i_{n+1}}) A_{n+1}(v_{i_{n+1}}) \wedge A_{n+1}(a_{j_{n+1}})$

Q u e s t i o n:

84. Comment justifier cette transformation?

La règle Ae offre la possibilité d'obtenir, partant de (*) les deux théorèmes suivants:

(**) $\vdash_{S^n} \sim(\forall v_{i_{n+1}})\ A_{n+1}(v_{i_{n+1}})$

et

$\vdash_{S^n} A_{n+1}(a_{j_{n+1}})$

Dans la preuve de cette dernière expression, remplaçons chaque mention de $a_{j_{n+1}}$ par une variable v qui ne figure nulle part dans la preuve. On a donc une preuve dans S^n dont la dernière ligne est $A_{n+1}(v)$.

Soit: $\vdash_{S^n} A_{n+1}(v)$ et par GEN :

(***) $\vdash_{S^n} (\forall v)A_{n+1}(v)$

Q u e s t i o n s :

85. $v_{i_{n+1}}$ est-elle libre pour v dans A_{n+1} ?

86. A(v) contient-elle $v_{i_{n+1}}$ libre ?

Le métathéorème 20 permet de changer dans (***) la variable liée v et d'écrire:

$\vdash_{S^n} (\forall v_{i_{n+1}})A_{n+1}\ (v_{i_{n+1}})$

ce qui est contradictoire avec (**). Ce résultat va à l'encontre de l'hypothèse d'induction. S^∞ est donc non contradictoire.

II.2 Construction d'une extension S* de S^∞ , non contradictoire et catégorique relativement à la fermeture.

S^∞ étant un système non contradictoire, il admet donc une extension S* non contradictoire et catégorique relativement à la fermeture [Mth. 27]

III. Construction d'un modèle I de S*, modèle dénombrable.

Dans un premier temps, nous établirons une interprétation dénombrable, puis nous montrerons qu'une telle interprétation est un modèle du système S*.

III.1 Construction d'une interprétation I.

L'interprétation doit fournir un domaine d'objets Ω dénombrable, le domaine des valeurs V et les applications Ψ [cf. déf. 23].

DEFINITION 34 -terme fermé- - Un terme fermé est un terme qui ne contient aucune variable.

Choix de Ω : l'ensemble des termes fermés de S^0. Il s'agit bien d'un ensemble dénombrable (pourquoi?)

Choix de V : comme toujours $\{\top, \bot\}$. Et les applications Ψ:

1] Si b est une constante (donc un c_i ou un a_j) alors $\Psi_C(b) = b$. L'image d'une constante est cette constante elle-même.

2] L'image de $f_i^n t_1 \ldots t_n$ où $t_1, t_2, \ldots, t_n$ sont des termes fermés de S^0, est le terme fermé $f_i^n t_1 \ldots t_n$ lui-même.

3] L'interprétation I assigne la valeur $\top$ à p_i^0 ssi $\vdash_{S^*} p_i^0$.

4] L'interprétation I assigne la valeur $\top$ à $p_i^n t_1 \ldots t_n$ où $t_1, t_2, \ldots, t_n$ sont des termes fermés de S^0 ssi $\vdash_{S^*} p_i^n t_1 \ldots t_n$.

Q u e s t i o n s :

87. L'ensemble des termes fermés de S* et celui de S^0 sont-ils égaux?
88. Pour quelle raison, dans le cas 2 par exemple, négligeons-nous de passer par les applications $\Psi_T(t_i)$?
89. Dans quelle condition aura-t-on $val(p_i^0) = \bot$? et $val(p_i^n t_1 \ldots t_n) = \bot$?

R e m a r q u e:

Il peut paraître surprenant que nous ayons omis de traiter des variables et donc des termes non fermés. En voici la raison. L'image d'une variable v_i par l'application Ψ_V serait un terme fermé de S^0. Mais ce terme fermé en tant qu'objet dans le domaine Ω est aussi un terme fermé dans le système S* et il sera de toute façon interprété. Ainsi, le choix du domaine des objets Ω permet de réduire les applications aux seuls termes fermés de S*, c'est-à-dire à ses constantes.

III.2 I est un modèle dénombrable de S*.

Revenons à l'interprétation I et montrons qu'elle est bien un modèle de S*. Il suffira d'établir que, quelle que soit l'ebf fermée A,

$\vdash_{S^*} A$ ssi $val_I(A) = \top$ [cf. déf. 30.3].

Q u e s t i o n :

90. Pour quelle raison avons-nous à ne considérer que les ebf fermées de S*?

Démonstration de III.2: Elle se fait par induction sur le nombre n des connecteurs de A.

Base: n = 0

Dans ce cas, deux possibilités seulement sont présentes:

- A est un symbole de prédicat de degré zéro p_i^0

ou - A est de la forme $p_i^d t_1 \ldots t_d$ où les t_i sont des termes fermés.

Dans l'un et l'autre cas: $val_I(A) = \top$ ssi $\vdash_{S^*} A$ [clauses 3) et 4) des applications Ψ, p. 46].

Hypothèse d'induction: L'interprétation I est un modèle pour toute ebf fermée qui contient au plus n connecteurs.

Pas d'induction : Montrons que l'interprétation I est un modèle pour toute ebf fermée A possédant n+1 connecteurs.

Trois cas sont à considérer:

1] A est ~B

2] A est B ⊃ C

3] A est $(\forall v_i)B$

Cas 1] : A est ~B et B est fermée puisque A l'est.

(→) 1.1 $val_I(A) = \top$ donc $val_I(B) = \bot$ et par hypothèse d'induction $\nvdash_{S^*} B$.
Comme S* est catégorique relativement à la fermeture, et que B est une ebf fermée $\vdash_{S^*}$ ~B.
Et ~B est A, donc $\vdash_{S^*} A$.

(←) 1.2 $\vdash_{S^*} A$. Il faut donc prouver que $val_I(A) = \top$.
Nous allons établir la contraposée :

si $val_I(A) \neq \top$ alors $\nvdash_{S^*} A$

On a : $val_I(A) \neq \top$ implique $val_I(A) = \bot$ et donc $val_I(B) = \top$

Par hypothèse d'induction on obtient $\vdash_{S^*} B$.
S* est non contradictoire, donc $\not\vdash_{S^*} \sim B$.
Et $\sim B$ est A, donc $\not\vdash_{S^*} A$.

Cas 2] : A est $B \supset C$
Les ebf B et C sont fermées puisque A l'est.

($\rightarrow$) 2.1 $val_I(A) = val_I(B \supset C) = \top$, montrons alors que $\vdash_{S^*} A$.
Passons par la contraposée et supposons que A n'est pas un théorème de S* : $\not\vdash_{S^*} A$.
S* étant catégorique relativement à la fermeture, on a $\vdash_{S^*} \sim A$
et donc $\vdash_{S^*} \sim(B \supset C)$ ou encore $\vdash_{S^*} B \wedge \sim C$
Ce qui nous permet d'établir: $\vdash_{S^*} B$ (1) ; $\vdash_{S^*} \sim C$ (2)

(1) Par l'hypothèse d'induction nous obtenons $val_I(B) = \top$ (*)

(2) S* étant non contradictoire, il s'ensuit de $\vdash_{S^*} \sim C$
que C n'est pas un théorème de S*: $\not\vdash_{S^*} C$
et une fois encore par hypothèse d'induction $val_I(C) = \bot$ (**)
Par (*) et (**), $val_I(B \supset C) = val_I(A) = \bot$.
Ainsi, si $\not\vdash_{S^*} A$ alors $val_I(A) = \bot$
DONC, si $val_I(A) = \top$ alors $\vdash_{S^*} A$.

($\leftarrow$) 2.2 Supposons que A (qui est $B \supset C$) soit un théorème: $\vdash_{S^*} A$ ou $\vdash_{S^*} B \supset C$, montrons alors que $val_I(A) = \top$.
Etablissons la contraposée. Posons $val_I(A) = \bot$ et montrons que $\not\vdash_{S^*} A$.
$val_I(A) = val_I(B \supset C) = \bot$ implique que $val_I(B) = \top$ et $val_I(C) = \bot$
Par hypothèse d'induction on obtient:
$\vdash_{S^*} B$ (*) et $\not\vdash_{S^*} C$
S* est catégorique relativement à la fermeture, il s'ensuit donc que $\vdash_{S^*} \sim C$ (**)

Par (*) et (**), on obtient
$\vdash_{S^*} B \wedge \sim C$ et donc $\vdash_{S^*} \sim(B \supset C)$

S* est non contradictoire, donc $\not\vdash_{S^*} (B \supset C)$ et $\not\vdash_{S^*} A$.

Ainsi, si $val_I(A) = \bot$ alors $\not\vdash_{S^*} A$.

DONC si $\vdash_{S^*} A$ alors $val_I(A) = \top$.

Cas 3]: A est $(\forall v_i)B$ où A est une ebf fermée.

Deux situations sont possibles.

3.1 B ne contient pas v_i libre. B est donc fermée.

($\rightarrow$) a) $val_I((\forall v_i)B) = \top$

Une ebf et sa fermeture sont logiquement valides ensemble [Mth. 14], donc on a aussi $val_I(B) = \top$ et par hypothèse d'induction $\vdash_{S^*} B$.
Dès lors, en utilisant la régle GEN, on obtient

$$\vdash_{S^*} (\forall v_i)B \qquad \text{donc} \qquad \vdash_{S^*} A.$$

($\leftarrow$) b) $\vdash_{S^*} A$ donc $\vdash_{S^*} (\forall v_i)B$.

Il existe donc une preuve de $(\forall v_i)B$ dans S*. Poursuivons cette preuve en y ajoutant la ligne qui contient l'ebf B [justification: présence préalable de $(\forall v_i)B$ et $\forall e$].
B est donc aussi un théorème dans S* : $\vdash_{S^*} B$
et par hypothèse d'induction $val_I(B) = \top$.
Une fois encore le Mth. 14 nous permet d'écrire $val_I((\forall v_i)B) = \top$.

3.2 B contient v_i libre, $B(v_i)$. A étant une ebf fermée, B ne contient que la variable v_i libre. B est donc une des ebf de notre liste [p. 43]
Admettons qu'il s'agit de l'ebf $A_k(v_{i_k})$ $[v_i = v_{i_k}]$.

($\rightarrow$) a) $val_I(A) = val_I((\forall v_{i_k})A_k(v_{i_k})) = \top$.

Raisonnons par l'absurde et posons $\not\vdash_{S^*} A$.
S* est catégorique relativement à la fermeture, donc

$$\vdash_{S^*} \sim A \qquad \text{et} \qquad \vdash_{S^*} \sim(\forall v_{i_k})A_k(v_{i_k}) \qquad (*)$$

Mais S* est une extension de S^∞. On a donc que l'axiome s_k est un théorème de S^∞ et donc de S*. C'est-à-dire :

$$\vdash_{S^*} \sim(\forall v_{i_k})A_k(v_{i_k}) \supset \sim A_k(a_{j_k}) \qquad (**)$$

Par (*), (**) et MP, on obtient :

$$\vdash_{S^*} \sim A_k(a_{j_k}) \qquad (\square)$$

Etant donné que $val_I(A) = val_I((\forall v_{i_k})A_k(v_{i_k})) = \top$ on a en particulier $val_I((A_k(a_{j_k})) = \top$. $A_k(a_{j_k})$ est fermée, donc par hypothèse d'induction, il vient

$$\vdash_{S^*} A_k(a_{j_k}) \qquad (\square\square)$$

Les théorèmes ($\square$) et ($\square\square$) feraient que S* serait contradictoire, ce qu'il n'est pas.

Ainsi l'hypothèse absurde $\not\vdash_{S^*} A$ est fausse.

DONC si $val_I(A) = val_I((\forall v_i)B) = \top$ alors $\vdash_{S^*} A$.

($\leftarrow$) b) $\vdash_{S^*} A$ donc $\vdash_{S^*} (\forall v_i)B(v_i)$ (*)

Considérons le schéma d'axiome A4:

$(\forall v_i)B(v_i) \supset B(t)$ si t est libre pour v_i dans $B(v_i)$ (**)

Quel que soit le terme <u>fermé</u> t de S* choisi il est toujours libre pour v_i dans $B(v_i)$. Il s'ensuit que

$$\vdash_{S^*} B(t) \qquad (*), (**), MP$$

Par hypothèse d'induction, B(t) étant une ebf fermée, $val_I(B(t)) = \top$ pour tout terme fermé de S*. Le terme fermé t étant quelconque, et le choix du domaine des objets Ω permettant de réduire les applications de I aux seuls termes fermés de S*, il s'ensuit que

$$val_I((\forall v_i)B(v_i)) = \top \quad \text{et donc} \quad val_I(A) = \top.$$

Ainsi, si $\vdash_{S^*} A$ alors $val_I(A) = \top$.

L'étude des cas 1], 2] et 3] établit que l'interprétation I est bien un modèle de S* et en raison même du choix du domaine Ω , ce domaine est dénombrable.

IV. Où le métathéorème 28 est enfin démontré, puis utilisé.

<u>Démonstration</u> :

1. I est un modèle dénombrable de S* [III.1 et III.2].
2. S* est une extension de S^∞ qui est lui-même une extension de S^0. I est donc également un modèle dénombrable de S^0.
3. Par construction, tous les théorèmes de S sont des théorèmes de S^0. L'interprétation I est donc aussi un modèle dénombrable de S.
4. S étant un système du premier ordre non contradictoire quelconque, nous avons donc prouvé que:

Tout système du premier ordre S qui est non contradictoire possède un modèle dénombrable.

Q u e s t i o n:

91. Le système L admet-il un modèle dénombrable?

METATHEOREME 29 - Tout système du premier ordre qui admet un modèle admet un modèle dénombrable.
[Théorème dit de Löwenheim-Skolem].

Démonstration: 1. Tout système du premier ordre qui admet un modèle est non contradictoire [Mth. 24].

2. Tout système du premier ordre qui est non contradictoire possède un modèle dénombrable [Mth.28].

R e m a r q u e s

- Le contenu du métathéorème 29 apparaît paradoxal si l'on songe qu'il est possible de formaliser la théorie des nombres réels [c'est un ensemble non dénombrable] dans un système du premier ordre.
- Le métathéorème 29 est très généreusement attribué à Löwenheim-Skolem. Le lecteur curieux qui voudrait retourner aux sources doit s'attendre à quelques surprises. Empruntons à Heijenoort [1971] la traduction anglaise de ces deux résultats:

Theorem 2 - If the domain is at least denumerably infinite, it is no longer the case that a first order fleeing equation is satisfied for arbitrary values of the relative coefficient.
[Heijenoort, 1971, p. 235, trad. Löwenheim, 1915.]

fleeing equation: il s'agit d'une formule qui n'est pas valide, mais qui est cependant n valide pour tout n, $n \in \mathbb{N}$.

first order equation: il s'agit d'une ebf du calcul des prédicats avec identité.

Theorem 2 - Every proposition in normal form either is a contradiction or is already satisfiable in a finite or denumerably infinite domain.
[Heijenoort, 1971, p. 256, trad. Skolem 1919].

contradiction: il s'agit d'une proposition qui n'est pas satisfaisable.
Dire d'une proposition A qu'elle n'est pas satisfaisable signifie que ~A est valide.

La forme normale d'une expression A est la transformée qui consiste en une expression organisée ainsi:

$(\exists x)(\exists y)\ldots(\exists z)(\forall m)(\forall n)\ldots(\forall r)B(x\ldots r)$, l'expression B ne contenant que des variables libres.

- L'essentiel de la démonstration du métathéorème 28 est dû à Henkin. Il s'agit d'une partie de sa thèse de doctorat soutenue en 1947 et publiée en 1949.
- Relativement à la démonstration du métathéorème 28, citons le commentaire suivant:

> *This proof skirts the edge of vicious circularity without quite falling into it. We want to prove that if a formula of [S*] is a theorem then it is true for a certain interpretation; and we then define the interpretation in question as one in which an atomic formula of [S*] is true iff it is a theorem of [S*]. For an atomic formula to be true, on this interpretation, is just for it to be a theorem of [S*]: this is what we mean by "true" (for atomic formulas) for the interpretation in question. [S*] is in fact interpreted in terms of itself. This will probably strike the reader as something of a cheat, especially if he was expecting a more interesting model.*
> [Hunter, 1973, pp. 184-185].

- Un résumé schématique de la démonstration du métathéorème 28 est proposé [p. 53].

9.4 La complétude sémantique de L

METATHEOREME 30 - Le calcul des prédicats [système L] est complet en ce sens que $\models_L A$ alors $\vdash_L A$.

Démonstration: Raisonnons par l'absurde.

Soit une ebf A logiquement valide, telle que $\not\vdash_L A$.

Etudions l'extension L' de L ainsi formée:

$$L' = L + \sim A \quad (\sim A \text{ est axiome}).$$

Le lemme I [p. 35] permet de dire que L' est non contradictoire. Et par le métathéorème 28 nous savons que L' possède un modèle I.

Etant donné que ~A est un axiome de L',

$$val_I(\sim A) = \top \quad \text{et } val_I(A) = \bot \qquad (*)$$

Mais A est logiquement valide, $\vdash A$, donc $val(A) = \top$ (**) dans toutes les interprétations, donc également dans I.

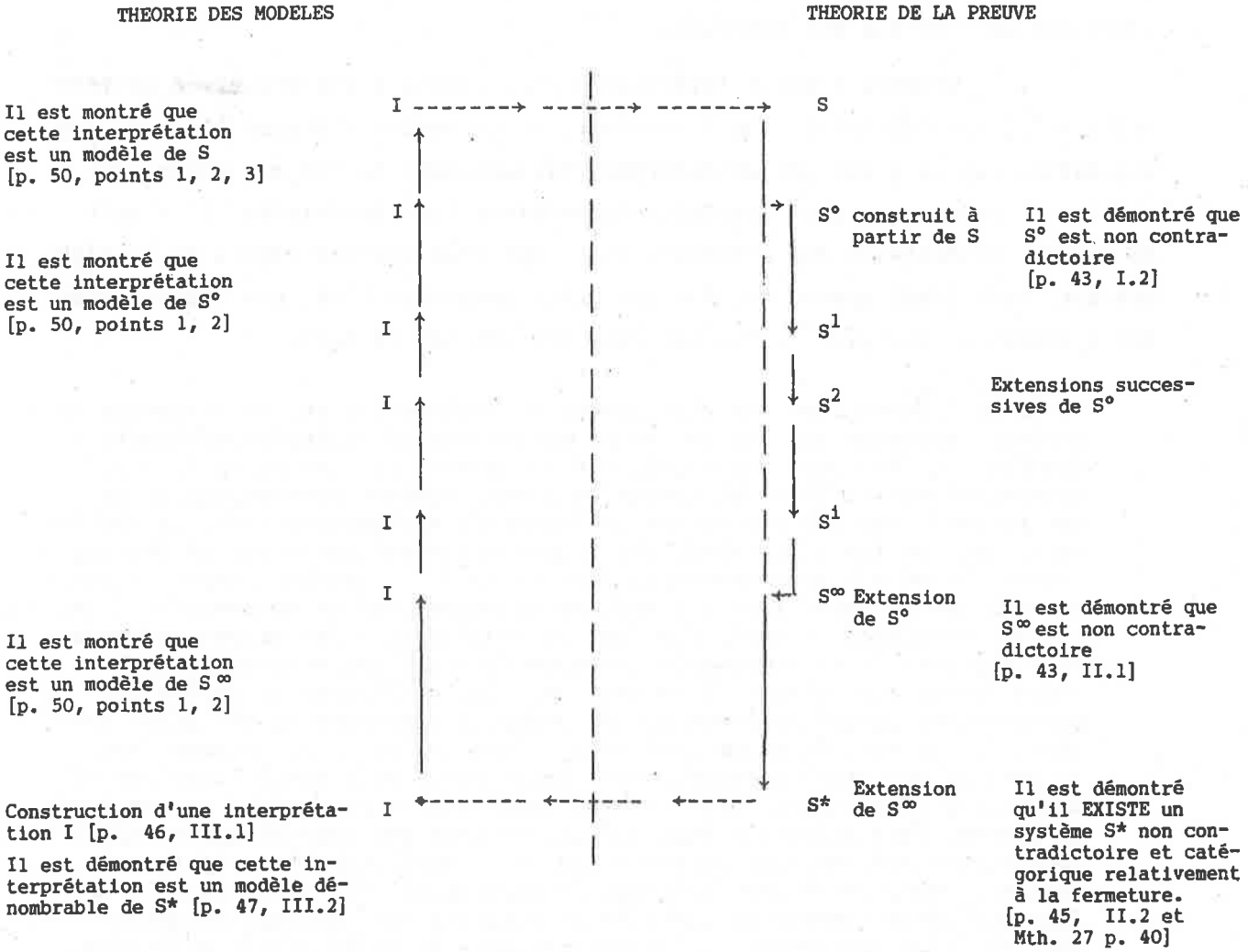
L'hypothèse absurde entraîne une contradiction: (*) et (**).

Toute ebf logiquement valide de L est donc un théorème dans ce système.

Remarque

Les deux démonstrations les plus marquantes relativement au métathéorème 30 sont dues à Gödel et Henkin. En 1930, dans sa thèse de doctorat Gödel démontre que toute ebf valide du calcul des prédicats est un théorème. Il s'agit de la première démonstration de ce résultat. La démarche qu'il propose est quelque peu différente de celle que nous avons suivie. Nous nous sommes largement inspirés de la démonstration de Henkin [1949].

RESUME SCHEMATIQUE DU METATHEOREME 28



10. LA DECIDABILITE

L'enjeu de la décidabilité est important. Pensons au dernier théorème de Fermat: l'équation $x^n+y^n = z^n$ ne possède pas de solution entière pour $n > 2$. Bien que Fermat ait affirmé avoir une preuve de cette proposition, personne depuis lors (≈1637) n'a réussi à démontrer cette proposition, ni sa négation. Envisageons un autre problème: considérons le nombre π dans sa représentation décimale 3, 14159265..., et posons-nous la question suivante: est-il possible de démontrer qu'il existe dans la suite décimale une première position k à partir de laquelle on trouve la suite de chiffres suivante: 2111110111112? Que répondre? L'intérêt de disposer d'un système offrant la garantie qu'il est toujours possible de déterminer si une expression est ou n'est pas un théorème est manifeste.

Leibniz s'était intéressé à l'existence d'une procédure universelle effective susceptible de déterminer, en un nombre d'étapes fini, si une expression est ou n'est pas un théorème. Hilbert dans la fin des années 20 réalise notamment que deux systèmes élémentaires sont décidables. Il s'agit du système élémentaire des prédicats ainsi que d'un système réduit de l'arithmétique. Mais Gödel montre en 1931 que cette propriété n'est pas acquise pour des systèmes un peu plus riches que ceux traités par Hilbert.

> *It is well known that the development of mathematics in the direction of greater precision has led to the formalization of extensive mathematical domains, in the sense that proofs can be carried out according to a few mechanical rules. The most extensive formal systems constructed up to the present time are the system of Principia Mathematica (PM), on the one hand, and, on the other hand, the Zermelo-Fraenkel axiom system for set theory (which has been developed further by J. v. Neumann). Both of these systems are so broad that all methods of proof used in mathematics today can be formalized in them, i.e. can be reduced to a few axioms and rules of inference. It is reasonable therefore to make the conjecture that these axioms and rules of inference are also sufficient to decide all mathematical questions which can be formally expressed in the given systems. ... it will be shown that this is not the case, but rather that, in both of the cited systems, there exist relatively simple problems of the theory of ordinary whole numbers which cannot be decided on the basis of axioms. This situation does not depend upon the special nature of the constructed systems, but rather holds for a very wide class of formal systems, among which are included, in particular, all those which arise from the given systems by addition of finitely many axioms, assuming that no false sentences ... become provable by means of the additional axioms.*
> [K. GÖDEL, in The Undecidable. Davis (ed.), New York, Raven Press, 1967, 5-6].

Ce résultat, comme du reste d'autres limitations mises en évidence depuis, est riche d'enseignements:

- par lui, nous savons une des limitations des systèmes formels "riches";
- par lui, nous réalisons que les démarches démonstratives nécessaires à établir les propriétés d'un système formel dépassent en richesse ce qui est autorisé dans le système formel;
- enfin, on peut le penser, l'état de la question relative au calculable (le décidable se ramènera au calculable) montre aujourd'hui des limites qu'un jour peut-être l'esprit saura dépasser.

> *...le "théorème d'incomplétude de Gödel", semble nous dire, non seulement que la mathématique n'est pas encore logique pure, mais aussi qu'il lui faut renoncer à jamais à l'espoir d'être entièrement maîtresse du sujet qu'elle se donne sitôt que l'esprit se le donne infini, cet infini aurait-il la simplicité la plus grande, celle justement de la suite des entiers.*
> *Or, rien n'oblige de penser qu'à cet égard la genèse intellectuelle humaine soit tout à fait achevée et indépassable. Après tout, qui sait si nous ne pouvons pas nous apprendre à penser mieux la multiplicativité du nombre, cet aspect de son être sur lequel notre épistémologie génétique ne semble pas avoir tout dit? Qui sait si cet effort de meilleure pensée n'aura pas finalement des répercussions jusque sur le cadre logique trop simple dans lequel, inconsidérément, notre spontanéité croit devoir couler l'énergie vive de l'intelligence mathématicienne?*
> *Seulement, sur un point de cette sorte, l'épistémologie génétique a à se faire non seulement étude génétique de la pensée mathématique à travers les stades avant tout prémathématiques de la pensée humaine. Il lui faut désormais se poursuivre en étude génétique de la pensée mathématique à travers des stades eux-mêmes déjà mathématiques de la pensée. Qui sait? ce travail se faisant, il lui faudra peut-être oser poursuivre plus avant le vecteur génétique de l'intellect et, de récit qui élucide, se transmuter, au bon moment, en décision consubstantielle à la clarté, créer.*
> [D. DUBARLE: in Logique et connaissance scientifique, La Pléiade, 1967, pp. 354-355].

10.1 Décidabilité de L^1

Soit L^1, le calcul des prédicats dans lequel on supprime:

1] tous les symboles de prédicat de degré >1

2] tous les symboles de foncteurs.

Il représente le calcul des propriétés (les prédicats monadiques), par opposition à la logique des relations.

Le système L est non contradictoire (Mth. 21), consistant (Mth.22) et sémantiquement complet (Mth. 30); le système L^1 possède donc également ces propriétés puisqu'il n'est qu'une partie de L.

Nous allons montrer que de plus L^1 est décidable et, pour cela, établir deux lemmes.

LEMME I - Si A est une ebf fermée de L^1 et si I est une interprétation sur un domaine Ω de k éléments, on peut construire une interprétation I' sur un domaine Ω' de (k+1) éléments telle que

$val_{I'}(A) = \top$ ssi $val_I(A) = \top$

ou

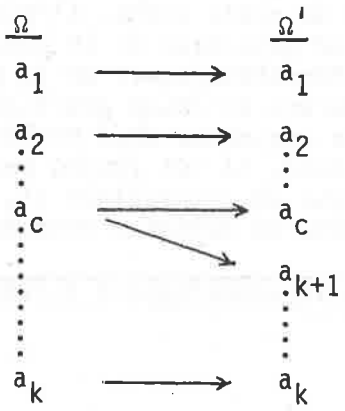
$val_I(A) = \bot$ ssi $val_{I'}(A) = \bot$

Démonstration: Considérons une ebf A fermée contenant m symboles de prédicats différents de degré 1. Soit p_i^1 l'un quelconque d'entre eux. D'autre part, considérons une interprétation I sur le domaine d'objets Ω de k éléments: $\Omega = \{a_1, a_2, \ldots, a_k\}$

Nous voulons construire une interprétation I' sur le domaine d'objets Ω' de k+1 éléments:

$\Omega' = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$

Etablissons tout d'abord la correspondance suivante:



Questions :

92. La correspondance ci-dessus est-elle une application?
93. Soit l'ensemble Ω contenant les dix premiers nombres entiers, et $\Omega' = \Omega \cup \{12\}$. Ecrire la correspondance ci-dessus en posant $a_c = 8$.
94. Soit le prédicat p_1^1 défini en compréhension ainsi: "être un nombre premier". Déterminer le sous-ensemble γ de l'ensemble Ω ci-dessus qui satisfait en extension la propriété. Il s'agit du résultat de l'application $\Psi(p_1^1)$ sur Ω: $\Psi(p_1^1) = \gamma$. Ecrire également le résultat de l'application $\Psi'(p_1^1)$ sur Ω' : $\Psi'(p_1^1) = \gamma'$, qui satisfait la propriété.
95. Mêmes questions pour le prédicat p_2^1 défini en compréhension ainsi: "être un nombre pair".
96. Si l'on compare les sous-ensembles γ et γ' de la question 94, et ceux de la question 95, qu'observe-t-on?

Construction de l'interprétation I'

Cette construction s'établit notamment sur l'appartenance ou la non-appartenance de l'élément a_c (l'élément de Ω qui est en correspondance avec l'élément a_{k+1} de Ω') à l'image de p_i^1 par l'application Ψ.

1] $\Psi'(c_i) = \Psi(c_i)$

2] $\Psi'(p_i^0) = \Psi(p_i^0)$

3] Posons $\Psi(p_i^1) = \gamma$

Si $a_c \notin \gamma$ alors : $\Psi'(p_i^1) = \Psi(p_i^1) = \gamma$

Si $a_c \in \gamma$ alors : $\Psi'(p_i^1) = \gamma \cup \{a_{k+1}\}$

La démonstration de "$val_{I'}(A) = \top$ ssi $val_I(A) = \top$" se fait par induction sur le nombre n des connecteurs de A.

Base : n = 0

Deux cas sont possibles :

a. A est p_i^0 ou

b. A est $p_i^1 c_j$

a. Démonstration immédiate: clause 2] de la construction de I'

b. (←--) Supposons que $val_I(p_i^1 c_j) = \top$

Cela signifie que $\Psi(c_j) \in \Psi(p_i^1)$

ou autrement dit que $\Psi(c_j) \in \gamma$.

Mais $\gamma \subseteq \gamma'$, et que γ soit ou non un sous-ensemble propre de γ', $\Psi'(c_j) \in \gamma'$, clause 1]; dit autrement, $\Psi'(c_j) \in \Psi'(p_i^1)$, donc $val_{I'}(p_i^1 c_j) = \top$

(--→) Supposons maintenant que $val_{I'}(p_i^1 c_j) = \top$, et montrons que $val_I(p_i^1 c_j) = \top$. Procédons par contraposition.

Soit donc $val_I(p_i^1\ c_j) = \bot$. Cela entraîne que $\Psi(c_j) \notin \gamma$ et donc que $\Psi'(c_j) \notin \gamma'$.

DONC $val_{I'}(p_i^1 c_j) = \bot$.

Questions :

97. Est-il nécessaire de passer par la contraposée?

98. De cette démonstration émane un parfum de sophisme. Bien que γ' contienne

avec certitude γ, ne se pourrait-il pas qu'il contienne également a_{k+1}? En ce cas si $\Psi'(c_j) = a_c$, $\Psi'(c_j)$ pourrait être dans γ' et notre raisonnement n'en serait pas un. Cette remarque n'est pas fondée. Pourquoi?

Hypothèse d'induction :

Si A est une ebf fermée de L^1 contenant au plus n connecteurs, et si I est une interprétation sur un domaine Ω de k éléments, on peut construire une interprétation I' sur un domaine Ω' de (k+1) éléments telle que

$$val_{I'}(A) = \top \quad \text{ssi} \quad val_I(A) = \top$$

Pas d'induction :

Démontrons le lemme pour une ebf fermée A possédant n+1 connecteurs. Trois cas sont à considérer.

a] A est ~B

1. (←--) $val_I(A) = \top$ donc $val_I(B) = \perp$ [et B est fermée.]
   Par hypothèse d'induction:
   $val_{I'}(B) = \perp$ et donc
   $val_{I'}(\sim B) = val_{I'}(A) = \top$

2. (--→) même procédure.

b] A est B ⊃ C

1. (←--) $val_I(A) = \top$. Il s'ensuit que:
   soit $val_I(B) = \perp$ soit $val_I(C) = \top$
   [Les ebf B et C sont fermées.]
   Par hypothèse d'induction:
   $val_{I'}(B) = \perp$ et $val_{I'}(A) = \top$
   $val_{I'}(C) = \top$ et $val_{I'}(A) = \top$

2. (--→) même procédure

c] A est (∀v)B

1. (←--) $val_I(A) = \top$ donc $val_I((\forall v)B) = \top$
   Il s'ensuit que quelle que soit l'image de v dans Ω, $val_I(B) = \top$

Si B est fermée, alors il s'ensuit par hypothèse d'induction, que $val_{I'}(B) = \top$, quelle que soit l'image de v dans Ω'.

DONC $val_{I'}(A) = \top$

Si B possède la variable v libre, procédons comme suit:
Par hypothèse, quelle que soit l'image de v, l'ebf a pour valeur $\top$.
Associons donc à v un quelconque des objets. Exhibons la constante c_m qui par l'application Ψ est associée justement à cet objet.
Formons l'expression $B(c_m)$ à partir de B(v) dans laquelle nous substituons c_m à v.

$val_I(B(v)) = \top$ donc $val_I(B(c_m)) = \top$

L'expression $B(c_m)$ possède un connecteur de moins que A et est fermée; par hypothèse d'induction on obtient que $val_{I'}(B(c_m)) = \top$.
Opérons à partir de $B(c_m)$ la substitution inverse, c_m/v. Nous avons alors $val_{I'}(B(v)) = \top$ et ceci quelle que soit la valeur de la variable v
DONC $val_{I'}(A) = \top$

2. (--→) même procédure.

Q u e s t i o n :

99. Dans le lemme I aurions-nous pu nous dispenser de la condition: "si A est une ebf fermée" ?

LEMME II - Si A est une ebf fermée de L^1 et si A contient m symboles de prédicats différents de degré 1, et si de plus on a une interprétation I sur un domaine fini quelconque on peut construire une interprétation I' sur un domaine qui a au plus 2^m éléments et telle que

$val_{I'}(A) = \top$ ssi $val_I(A) = \top$

ou $val_I(A) = \bot$ ssi $val_{I'}(A) = \bot$

Q u e s t i o n s :

100. Soit $\Omega = \{1, 2, \ldots, 10\}$. Attribuons en compréhension une propriété à chaque prédicat de degré 1 suivant:

p_1^1 = "être un nombre premier"

p_2^1 = "être un nombre pair"

p_3^1 = "être multiple de 3"

Ecrire les sous-ensembles γ_1, γ_2 et γ_3 de Ω qui correspondent extensionnellement aux propriétés ci-dessus.

101. Faire une partition de l'ensemble Ω ci-dessus en classes d'équivalence; c'est-à-dire construire les classes des éléments de Ω qui appartiennent
- à la fois à γ_1, γ_2 et γ_3
- à la fois à γ_1, γ_2 mais pas à γ_3
- à γ_1 mais pas à γ_2 ni à γ_3
  :
- ni à γ_1, ni à γ_2 et ni γ_3.

Combien y a-t-il de possibilités?

102. Effectuer la même démarche en attribuant aux prédicats p_2^1 et p_3^1 les mêmes propriétés que ci-dessus et au prédicat p_1^1 la propriété : "être plus petit que 8".

Construction de l'interprétation I'.

Cette construction se fait comme suit:

Le domaine d'objets Ω' associé à l'interprétation I' est l'ensemble des classes d'équivalence construites à partir de Ω et déterminées par les m prédicats différents de A. Il y a au plus 2^m classes d'équivalence différentes.

Soit $\Omega = \{a_1, a_2, \ldots, a_k\}$;

Construction des applications Ψ' :

1. Si $\Psi(c_i) = a_j$, alors $\Psi'(c_i)$ est la classe d'équivalence de Ω' qui contient a_j.
2. $\Psi'(p_i^0) = \Psi(p_i^0)$
3. Si $\Psi(p_i^1) = \gamma$, alors $\Psi'(p_i^1)$ est l'ensemble des classes d'équivalence de Ω' qui contient les éléments de γ.

Q u e s t i o n :

103. Relativement à la question 100, si $\Psi(p_1^1) = \{2, 3, 5, 7,\}$, quelle est $\Psi'(p_1^1)$?

La démonstration du lemme II se déroule de la même manière que celle du lemme I hormis la base de l'induction. Nous ne traiterons donc que de ce cas.

Base : n = 0

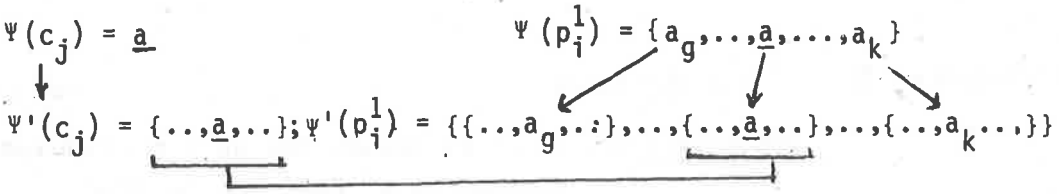
1] A est p_i^0 . trivial, cf. construction.

2] A est $p_i^1 c_j$

1. (←--) $val_I(p_i^1 c_j) = \top$

il s'ensuit par définition que $\Psi(c_j) \in \Psi(p_i^1)$.
Ainsi, si $\Psi(c_j) = \underline{a}$ et $\Psi(p_i^1) = \{a_g, \ldots \underline{a}, \ldots, a_k\}$

alors $\Psi'(c_j)$ est la classe d'équivalence qui contient $\underline{a}$ et $\Psi'(p_i^1)$ est l'ensemble des classes d'équivalence de Ω' qui contient les éléments de $\Psi(p_i^1)$. De plus, l'unique prédicat p_i^1 détermine sur Ω au plus 2^n classes d'équivalence.



DONC $\Psi'(c_j) \in \Psi'(p_i^1)$ et $val_{I'}(p_i^1 c_j) = \top$

2. (--→) $val_{I'}(p_i^1 c_j) = \top$. Il faut montrer que $val_I(p_i^1 c_j) = \top$

Procédons par contraposition et posons :
$val_I(p_i^1 c_j) = \bot$, il s'ensuit que $\Psi(c_j) \notin \Psi(p_i^1)$.

Ainsi, si $\Psi(c_j) = \underline{a}$, alors $\Psi(p_i^1)$ ne contient pas $\underline{a}$. Dès lors,

$\Psi'(c_j)$ qui est la classe d'équivalence qui contient $\underline{a}$ ne se trouve pas parmi les classes d'équivalence qui composent $\Psi'(p_i^1)$.

DONC $\Psi'(c_j) \notin \Psi'(p_i^1)$ et $val_{I'}(p_i^1 c_j) = \bot$

DEFINITION 35 - Une ebf A de L est n-valide ssi elle est valide pour toute interprétation sur un domaine fini Ω de n éléments, $n \in \mathbb{N}$
-n-valide-

METATHEOREME 31 - Dans L^1, toute ebf A fermée qui contient m symboles différents de prédicat de degré un est logiquement valide ssi elle est 2^m-valide
ou A n'est pas 2^m-valide ssi A n'est pas logiquement valide.

Démonstration: (--→) Si A est logiquement valide, elle est valide sur tout domaine et on sait construire

un domaine possédant 2^m éléments.

(←--) Procédons par contraposition et montrons que si A n'est pas logiquement valide alors elle n'est pas 2^m-valide.
Si $\not\models_{L1} A$ alors il existe une interprétation I telle que $val_I(A) = \perp$. Donc par le lemme II on peut trouver une interprétation I' sur un domaine à 2^m éléments au plus telle que $val_{I'}(A) = \perp$

En appliquant aussi souvent que nécessaire le lemme I, on arrivera à une interprétation qui a exactement 2^m éléments.

METATHEOREME 32 - L^1 est décidable.

Démonstration: Il n'est besoin que de s'occuper des ebf fermées de L^1 [Mth. 14, Ve, GEN].
Soit A une ebf fermée quelconque contenant m prédicats de degré 1 différents. Pour décider si A est ou n'est pas un théorème on procède par un calcul de sa validité sur un domaine fini de 2^m éléments. Il s'agit donc de calculer si A est ou n'est pas 2^m-valide.
En effet:
Les métathéorèmes 19 et 30 garantissent que:

$\vdash A$ ssi $\models A$

ou $\not\vdash A$ ssi $\not\models A$

et le métathéorème 31 que:

$\models A$ ssi A est 2^m-valide

ou A n'est pas 2^m-valide ssi $\not\models A$.

Nous possédons ainsi une procédure effective de calcul.

10.2 Indécidabilité des systèmes arithmétiques

Il est nécessaire pour démontrer l'indécidabilité du calcul des prédicats de degré n, $n \geq 2$ de prouver un résultat plus "fort". Il s'agit en effet d'établir préalablement l'indécidabilité de l'arithmétique. C'est la raison pour laquelle nous abordons ce problème maintenant.

Précisons tout d'abord les conditions minimales qu'il faut réunir pour construire un système formel capable de représenter de manière acceptable l'arithmétique, système que nous appellerons un système arithmétique minimal: un SAM. Afin de formaliser l'arithmétique en un SAM, S^a, il semble raisonnable d'exiger que:

1. Le système S^a soit un système du premier ordre.
2. Il soit possible d'interpréter certains au moins de ses termes comme des nombres naturels.
3. Certains des théorèmes de S^a correspondent à des lois arithmétiques.
4. Le système S^a soit non contradictoire.
5. Chaque ensemble décidable de nombres naturels soit représentable dans S^a. De manière intuitive, il s'agit d'établir une correspondance bi-univoque entre les éléments d'un tel ensemble et les ebf du système formel dont la variable libre, quand elle représente un terme interprétable comme un nombre naturel, est un théorème de S^a. Nous préciserons bien sûr cette notion.

Formaliser l'arithmétique consistera donc à construire un système formel appliqué dont certains termes pourront être interprétés comme des nombres naturels. Il s'ensuit qu'il est indispensable de distinguer de manière typographique les nombres naturels des termes qui seront interprétés comme tels. De manière à reconnaître immédiatement qu'un terme de S^a est lié aux nombres naturels, nous utiliserons la convention suivante:

> Si n est un nombre naturel, nous noterons $\underline{n}$ le terme qui lui est associé par l'interprétation. Nous appellerons ce terme un numéral (un numéral, des numéraux). Le terme $\underline{n}$ est donc un objet formel du système.

Questions :

104. Si t est un terme de S^a, quelle est $\Psi_T(t)$?
105. Ecrire le numéral qui a comme image 0? celui qui a comme image 4? celui qui a comme image 3+5? celui qui a comme image n.m?
106. Si le système S^a ne possédait pas les symboles $\underline{+}$ et $\underline{.}$ (qui correspondent respectivement à + et à .), avec quel type de symboles aurions-nous pu les écrire?

DEFINITION 36 - -fonction caractéristique- Soit A(v) une ebf de S^a qui contient la variable libre v. On appelle fonction caractéristique associée à A(v), la fonction f(n) définie ainsi :

$$\begin{cases} f(n) = 0 & \text{si} \quad \vdash_{Sa} A(\underline{n}) \\ f(n) = 1 & \text{sinon} \end{cases}$$

Remarque

Si S^a est décidable, la fonction caractéristique d'une ebf de la forme A(v) est calculable, ce qui signifie que quel que soit le nombre n, on saura si f(n) = 0 ou si f(n) = 1.

DEFINITION 37 - Soit E un ensemble de nombres naturels. On dit que E est -représentable- représentable dans S^a, s'il existe une ebf de S^a, de la forme A(v) et telle que, quel que soit le nombre n, $n \in E$:
$n \in E$ ssi $\vdash_{Sa} A(\underline{n})$

Question:

107. Soit un système S^a et le domaine d'objets $\Omega = \mathbb{N}$
Soit le prédicat de degré $2\,p_1^2$ qui dans l'interprétation est associé en compréhension à la relation "être égal à". Acceptons que dans ce S^a l'expression suivante est un théorème : $\vdash_{Sa} p_1^2 v\ v$.
Peut-on affirmer que l'ensemble E des nombres premiers est représentable dans S^a parce que quel que soit le nombre $n \in E$, $\vdash_{Sa} p_1^2 \underline{n}\ \underline{n}$?
Si cela n'est pas le cas comment pourrait-on imaginer construire une ebf de telle manière qu'elle remplisse ce rôle de 'représentativité'?

METATHEOREME 33 - Tout SAM est indécidable

Démonstration: I. Enumération des fonctions caractéristiques.
Grâce à la numérotation de Gödel (lemme II, p. 35) il est possible d'énumérer les ebf de S^a qui contiennent une variable libre:
$A_0(-), A_1(-), \ldots, A_n(-), \ldots$
Pour chacune d'entre elles, on peut lui associer sa fonction caractéristique. En établissant une correspondance entre l'ensemble ordonné des ebf qui contiennent une variable libre et leur fonction caractéristique associée, on obtient bien un ensemble ordonné de fonctions caractéristiques:
$f_0(-), f_1(-), \ldots, f_n(-), \ldots$ (*)

II. Construction d'une fonction.
Construisons la fonction h(n) suivante :
$\begin{cases} h(n) = 1 & \text{si } f_n(n) = 0 \\ h(n) = 0 & \text{sinon.} \end{cases}$

Q u e s t i o n :

108. Quelle est la valeur de la fonction h pour n = 0, 1, 2, 3, si $f_0(0) = 0$; $f_1(1) = 1$; $f_2(2) = 0$; $f_3(3) = 0$?

Sachant que $f_8(5) = 1$ quelle est la valeur de h(8)?

$h(7) = 0$, quelle est la valeur de $f_7(7)$?

La fonction h est-elle calculable?

III. Lemme. La fonction h(-) n'est pas dans l'énumération (*) des fonctions caractéristiques.
Raisonnons par l'absurde et supposons que la fonction h(-) appartient à l'énumération (*). Cette fonction h(-) est donc un des $f_i(-)$. Supposons qu'elle est $f_k(-)$. Il s'ensuit alors que:
$h(k) = 1$, donc $f_k(k) = 1$, si $f_k(k) = 0$
ET $h(k) = 0$, donc $f_k(k) = 0$, si $f_k(k) = 1$
Nous obtiendrons ainsi un résultat quelque peu surprenant : $f_k(k) = 1$ ssi $f_k(k) = 0$.

Q u e s t i o n:

109. De quelle ebf, la fonction h(-) est-elle fonction caractéristique sous l'hypothèse absurde? Et que pourrait-on dire de cette ebf?

IV. Construction d'un ensemble de nombres.
En utilisant la fonction h(-) construisons l'ensemble de nombres naturels E suivant:
$n \in E$ ssi $h(n) = 0$

V. Montrons enfin que S^a n'est pas décidable.
Hypothèse absurde: S^a est décidable.
Il s'ensuit que l'ensemble E construit en IV, est un ensemble décidable. En effet, quel que soit le numéral $\underline{n}$, on peut savoir si $\vdash_{S^a} A_i(\underline{n})$, donc $f_i(n)$ est calculable pour tout i et pour tout n. Ceci entraîne que la fonction h(-) est calculable, et par conséquent, que l'ensemble E est décidable.

Q u e s t i o n:

110. Que faut-il faire pour savoir si $18 \in E$?

MAIS l'ensemble E n'est pas représentable dans S^a. En effet, s'il l'était, il existerait une ebf A(v) (déf. 37, p. 64) telle que:
$n \in E$ ssi $\vdash_S^a A(\underline{n})$
MAIS, $n \in E$ ssi $h(n) = 0$, c'est-à-dire, ssi $\vdash_S^a A(\underline{n})$
Il s'ensuit d'une telle situation que la fonction h(-) serait une fonction caractéristique de A(v) et qu'elle serait dans l'énumération (*), ce qui, comme nous venons de le montrer, n'est pas le cas.
Nous pouvons donc conclure:
Si S^a est décidable, S^a n'est pas un système arithmétique minimal; la condition (5) n'est pas remplie
OU par contraposition:
Si S^a est un système arithmétique minimal, alors S^a n'est pas décidable.

Remarque

Ce qui précède ne fait que fournir la démarche de pensée du théorème de Gödel. Il reste à prouver qu'il existe des systèmes arithmétiques minimaux. Pour cela, il faudra construire un tel SAM; nous nous y emploierons. Puis il faudra montrer que le système construit satisfait aux conditions d'un SAM [chap.5]

La démonstration de la non-contradiction est loin d'être triviale; elle exige une présentation particulière des systèmes formels. Gentzen offre cette démonstration en 1935/36. Il utilise pour cela un système de règles qui appartiennent à la déduction naturelle ainsi que le principe d'induction transfinie, principe qui n'appartient ni à la logique des prédicats du premier ordre ni à la théorie élémentaire des nombres.

Quant à la représentativité, elle exige de définir de façon opératoire l'idée naïve qu'une fonction est calculable. Pour ce faire, nous présenterons la notion de fonction récursive.

Question :

111. Pourrions-nous déduire sans autre l'indécidabilité de L^n de celle de S^a ?

10.3 Indécidabilité de la logique des prédicats de degré n, L^n [n>1]

Esquisse d'une démonstration

En 1950, R.M. Robinson a construit un système arithmétique minimal S^r, dit "arithmétique de Robinson". Il a montré que S^r était indécidable, comme d'ailleurs chacune de ses extensions. Ce système jouit de propriétés que ne possède pas le système S^a que nous construirons.

Le système S^r possède un nombre fini d'axiomes: $A_1, A_2, \ldots, A_n$. D'autre part, en remplaçant partout les symboles de foncteurs par des symboles de prédicats convenablement construits, les axiomes de S^r deviennent des ebf fermées de L^n, à savoir:

$$A_1^*, A_2^*, \ldots, A_n^*$$

Soit B, un théorème de S^r: $\vdash_{S^r} B$. B est donc issu entre autres choses des axiomes A_i de S^r. En opérant la transformation des foncteurs en prédicats sur l'expression B, on obtiendra l'ebf B* de L^n. Et l'on pourra déduire, dans L^n, B* des hypothèses $A_1^*, A_2^*, \ldots, A_n^*$.

Posons $A^* = A_1^* \wedge A_2^* \wedge \ldots \wedge A_n^*$

On peut démontrer alors que

$$A^* \vdash_{L^n} B^* \quad \text{ssi} \quad \vdash_{S^r} B$$

A* est une ebf fermée de L^n. On peut donc appliquer le "théorème de la déduction". Il s'ensuit donc que

$$\vdash_{L^n} A^* \supset B^* \quad \text{ssi} \quad \vdash_{S^r} B$$

MAIS S^r est indécidable, il existe donc au moins une ebf fermée C dont on ne pourra pas décider si elle est ou non un théorème, et donc, on ne pourra pas décider si l'expression $A^* \supset C^*$ est un théorème ou non de L^n. L^n est donc indécidable.

CHAPITRE 5 - UN SYSTEME ARITHMETIQUE MINIMAL: S^a

1. PREAMBULE

A la fin du chapitre précédent, nous avons présenté sommairement les propriétés essentielles qu'il faut réunir pour construire un système formel capable de représenter l'arithmétique. Nous exposons maintenant les éléments qui entrent dans la composition d'un tel système. Mais avant de présenter cette construction, proposons deux commentaires.

L'histoire récente de la théorie des systèmes formels s'inscrit profondément dans l'héritage hilbertien qui cherche à éliminer toute intuition des fondements mathématiques. L'arithmétique élémentaire -la théorie des nombres entiers naturels- n'est qu'une partie de l'ensemble des théories mathématiques. Son étude se justifie cependant dans la mesure où elle sert de fondement à la construction de systèmes plus complexes. En effet, grâce à elle, il est possible d'accéder aux théories des nombres rationnels, réels et complexes, ainsi que d'aborder l'analyse. Cette nature première de l'arithmétique élémentaire justifie l'étude de sa construction formelle. Nous nous emploierons donc à développer un système du premier ordre appliqué qui permettra de représenter cette théorie, c'est-à-dire, à même de rendre compte des opérations et des relations qui règlent la structure dont le domaine des objets est l'ensemble des entiers naturels. Ensuite, il s'agira de vérifier que la structure abstraite développée est alors adéquate pour interpréter l'arithmétique. Dans cette perspective, nous aurons également à nous préoccuper de l'existence d'autres modèles possibles que celui simplement arithmétique.

A la fin du XIXe siècle, la mathématique classique avait déjà été réduite à la théorie des nombres entiers naturels. Il restait cependant à l'axiomatiser. Cette expression est à comprendre dans l'esprit de ce temps: une représentation symbolique intuitive et une organisation des idées primitives et des principes fondateurs de l'arithmétique élémentaire. Hermann Grassmann [1809-1877], théologien et linguiste, exposait en 1861 une caractérisation de l'ensemble des nombres entiers et Julius Wilhelm Richard Dedekind [1831-1916] proposait dans son livre *Was sind und was sollen die Zahlen?* [1888] quatre conditions -axiomes- capables de caractériser adéquatement la structure des entiers naturels. Mais c'est à

Guiseppe Peano [1858-1932] que l'histoire a rendu hommage. En 1889, il publie les *Arithmetices Principia a nova methodo exposita* dans lesquels il montre qu'en plus des notions de pure logique, trois idées primitives -zéro, nombre, successeur- et cinq axiomes permettent de rendre compte de la structure des nombres entiers. Voici ces axiomes:

- 0 est un nombre
- le successeur d'un nombre quelconque est un nombre
- 0 n'est le successeur d'aucun nombre
- deux nombres différents ne peuvent pas avoir le même successeur
- toute propriété qui appartient à 0, ainsi qu'au successeur de chaque nombre qui possède la propriété, appartient à tous les nombres.

Ces éléments sont repris dans le *Formulaire Mathématique* [1895-1905, quatre volumes en français et le cinquième en italien] qui rendra célèbre Peano, et c'est ceux-ci que nous aménagerons afin de construire un système arithmétique minimal.

2. LA CONSTRUCTION DU SYSTEME S^a

Il s'agit d'un système formel du premier ordre qui contient:

- un seul symbole de constante d'objet: c_1 =df $\underline{0}$
- un ensemble de symboles de variables d'objet: $\{v_1, v_2, \ldots, v_i, \ldots\}$
- un unique symbole de prédicat de degré deux: p_1^2 =df $\boxminus$
- trois symboles de foncteurs:
  un de degré un: f_1^1 =df *
  deux de degré deux: f_1^2 =df $\boxplus$; f_2^2 =df $\boxdot$
- et bien entendu, les symboles de connecteurs logiques ainsi que les parenthèses.

Q u e s t i o n s :

112. Ecrire quelques termes de S^a.
113. Les termes de S^a contiennent-ils des variables libres? des variables liées? des constantes?
114. Expliciter la définition inductive qui donne accès à l'ensemble de tous les termes de S^a.
115. Ecrire quelques formules atomiques et ebf de S^a.
116. S^a contient-il des symboles de prédicat de degré zéro?

DEFINITION 38 - Un terme de S^a qui ne contient pas de variable est appelé
-numéral- un numéral.

R e m a r q u e. A cette étape de la construction, il n'est bien sûr pas encore question d'interprétation. Il semble cependant souhaitable d'anticiper la perspective interprétative. C'est la raison pour laquelle nous avons associé à différents objets formels du système la forme qu'ils possèdent dans la réalisation sémantique normale où ils prennent signification: l'arithmétique élémentaire. Afin d'éliminer toute ambiguïté entre syntaxe et sémantique, nous avons choisi de souligner les numéraux et d'entourer d'un carré les objets formels que sont les deux foncteurs de degré deux et le relateur.

- $\underline{0}$: il s'agit du zéro formel
- $\boxminus$: ce symbole représentera l'égalité
- * : ce symbole représentera la fonction successeur immédiat
- $\boxplus$: ce symbole représentera l'addition
- $\boxdot$: ce symbole représentera la multiplication

D'autre part, les définitions inductives que nous proposons pour inscrire les termes et les ebf rendent ceux-ci peu conformes à notre habitude d'écrire les expressions arithmétiques. En effet, ces derniers ne sont généralement pas des expressions préfixées. C'est la raison pour laquelle nous modifierons l'écriture partiellement préfixée pour admettre une écriture plus conventionnelle.

Dorénavant, si t, t_i et t_j sont des termes, nous écrirons

t^*	au lieu de	$*t$
$(t_i \boxplus t_j)$	"	$\boxplus t_i t_j$
$(t_i \boxdot t_j)$	"	$\boxdot t_i t_j$
$(t_i \boxminus t_j)$	"	$\boxminus t_i t_j$

et nous supprimerons dans les expressions complexes les parenthèses extérieures inutiles.

En acceptant ces diverses conventions, les axiomes propres de S^a se présentent ainsi.

Les axiomes propres de S^a

a_1 : $(v_i \boxminus v_j) \supset ((v_i \boxminus v_k) \supset (v_j \boxminus v_k))$

a_2 : $(v_i \boxminus v_j) \supset (v_i^* \boxminus v_j^*)$

a_3 : $(v_i^* \boxminus v_j^*) \supset (v_i \boxminus v_j)$

a_4 : $\sim(\underline{0} \boxminus v_i^*)$ que nous écrivons: $\underline{0} \boxplus v_i^*$

a_5 : $(v_i \boxplus \underline{0}) \boxminus v_i$

a_6 : $(v_i \boxplus v_j^*) \boxminus (v_i \boxplus v_j)^*$

a_7 : $(v_i \boxdot \underline{0}) \boxminus \underline{0}$

a_8 : $(v_i \boxdot v_j^*) \boxminus ((v_i \boxdot v_j) \boxplus v_i)$

a_9 : $A(\underline{0}) \supset ((\forall v_i)(A(v_i) \supset A(v_i^*)) \supset (\forall v_j)A(v_j))$

Remarques.

- L'axiome a_1 permet d'interpréter le symbole $\boxminus$ comme l'égalité [cf. l'appendice].
- Les axiomes a_2 et a_3 précisent une structure d'ordre.
- L'axiome a_4 impose que dans tout modèle, le domaine d'objet possède "un premier élément".
- Les axiomes a_5 et a_6 inscrivent les propriétés que l'on attribue à l'addition.
- Les axiomes a_7 et a_8 inscrivent les propriétés que l'on attribue à la multiplication.
- Le schéma d'axiome a_9 formalise le raisonnement par induction complète. Il offre la possibilité d'effectuer des preuves dans S^a. Il ne nous dispense cependant pas de faire des démonstrations par induction lorsqu'il s'agira de prouver des métathéorèmes à propos de S^a.
- De manière intuitive, et apparemment formelle, la multiplication se construit à l'aide de l'addition. L'apparence est trompeuse. En effet, Presburger a montré en 1929 que si l'on considère un système semblable à celui que nous exposons, mais sans les axiomes a_7 et a_8, il possède la propriété de complétude. Nous savons par ailleurs [cf. pp. 64 sqq.] que si un système possède les conditions minimales pour être un système arithmétique, il est indécidable. Il faut donc admettre que, à travers les axiomes a_7 et a_8, on introduit plus qu'une simple construction à partir de l'addition. L'introduction des axiomes associés à la multiplication modifie donc la nature du système. Elle l'étend de façon "essentielle".

Questions :

117. L'expression $(\underline{0} \boxminus \underline{0}) \supset (\underline{0}^* \boxminus \underline{0}^*)$ est-elle un axiome?

118. Combien S^a contient-il d'axiomes?

119. Nous avons associé l'objet formel 0 à l'unique symbole de constante c_1 de S^a. Nous voulons l'interpréter comme le zéro. Aurions-nous pu lui associer un autre objet formel? par exemple 13 ou ↯ ? Si cela est le cas, pouvons-nous interpréter cet objet comme le nombre treize sans compromettre notre projet de représenter l'arithmétique?

Quelques règles de déduction

Afin de simplifier les démarches démonstratives, il est utile de disposer de règles déductives dérivées. Certaines d'entre elles concernent les notions de substitution et de remplacement, d'autres se rapportent aux propriétés que supporte l'unique prédicat de degré deux de S^a. Nous nous y intéressons car nous nous proposons d'interpréter cet objet formel comme la relation d'égalité sur l'ensemble des nombres naturels. Il devrait donc posséder, dans S^a, les propriétés de réflexivité, de symétrie et de transitivité qui caractérisent cette relation.

De manière à ne pas distraire l'attention du lecteur par rapport au thème central de ce chapitre, nous exposons les démonstrations en appendice.

Règle sub (substitution)

Quelle que soit l'ebf A de S^a qui contient une variable libre v_i, un terme libre pour v_i peut y être substitué:

$$A(v_i) \vdash_{Sa} A(t)$$

Schéma:

m	$A(v_i)$	

	$A(v_i/t)$	m, sub, v_i/t, si t est libre pour v_i dans $A(v_i)$

Règle réf (réflexivité)

Quel que soit le terme t_i de S^a, $t_i \boxminus t_i$ est un théorème:

$$\vdash_{Sa} t_i \boxminus t_i$$

Schéma:

n	$t_i \boxminus t_i$	réf

Le prédicat $\boxminus$ est donc totalement réflexif. Une relation qui possède cette propriété "est définie pour tous les domaines d'objets que l'on pourra considérer" [Grize, 1972].

Règle sym (symétrie)

Quels que soient les termes t_i et t_j, si $t_i \boxminus t_j$, alors $t_j \boxminus t_i$:

$t_i \boxminus t_j \vdash_{S^a} t_j \boxminus t_i$

Schéma :

n	$t_i \boxminus t_j$	
	$t_j \boxminus t_i$	n, sym

Règle tra (transitivité)

Quels que soient les termes t_i, t_j et t_k, si $t_i \boxminus t_j$ et $t_j \boxminus t_k$, alors $t_i \boxminus t_k$:

$t_i \boxminus t_j, t_j \boxminus t_k \vdash_{S^a} t_i \boxminus t_k$

Schéma:

n	$t_i \boxminus t_j$	
m	$t_j \boxminus t_k$	
	$t_i \boxminus t_k$	n, m, tra

L'objet formel $\boxminus$ dans la structure syntaxique de S^a est totalement réflexif, symétrique et transitif. Il est donc capable de représenter une relation d'équivalence.

Q u e s t i o n s :

120. Démontrer les théorèmes suivants:

a) $\vdash (t_i \boxminus t_j) \supset ((t_i \boxplus t_k) \boxminus (t_j \boxplus t_k))$

b) $\vdash (t_i \boxminus t_j) \supset ((t_i \boxdot t_k) \boxminus (t_j \boxdot t_k))$

c) $\vdash (t_i \boxminus t_j) \supset (t_i^* \boxminus t_j^*)$

d) $\vdash (t_i \boxplus t_k) \boxminus (t_k \boxplus t_i)$

e) $\vdash (t_i \boxdot t_k) \boxminus (t_k \boxdot t_i)$

f) $\vdash (t_i \boxminus t_j) \supset (((t_i \boxminus t_k) \wedge (t_j \boxminus t_p)) \supset (t_k \boxminus t_p))$

Nous désirons également disposer d'une règle de remplacement. En effet, lorsque deux termes t_i et t_j sont dans un rapport d'égalité formelle, et que par ailleurs l'un d'entre eux, t_i par exemple, apparaît libre dans une expression bien formée $A(t_i)$, il semble souhaitable de pouvoir la remplacer par l'autre terme pour une, plusieurs ou toutes ses occurrences, de manière à obtenir l'expression bien formée $A(t_i$ ou $t_j)$, ce que nous écrirons $A(t_i//t_j)$. En prenant quelques précautions, on peut dis-

poser de cette règle dans S^a.

Règle de rem (remplacement)

Si $t_i \boxminus t_j$, à chaque occurrence de t_i pour laquelle t_j est libre pour t_i dans $A(t_i)$, on peut remplacer t_i par t_j: $t_i \boxminus t_j$, $A(t_i//t_j)$. La règle de remplacement offre donc une plus grande liberté que celle de substitution. En effet, cette dernière exige de changer partout le substitué par le substituant.

$$t_i \boxminus t_j,\ A(t_i) \vdash_{S^a} A(t_i//t_j)$$

Schéma:

m	$t_i \boxminus t_j$
n	$A(t_i)$
---	---
	$A(t_i//t_j)$ m, n, rem [sous réserve des conditions susmentionnées]

Remarques.

- Quel que soit le terme t_i, $t_i \boxminus t_i$ est un théorème de S^a.
  *] $\vdash_{S^a} t_i \boxminus t_i$ (règle ref)
- Quels que soient les termes t_i et t_j, et quelle que soit l'ebf $A(t_i)$ qui contient t_i libre, si $t_i \boxminus t_j$ alors à chaque occurrence de t_i pour laquelle t_j est libre pour t_i dans $A(t_i)$, on peut remplacer t_i par t_j:
  $t_i \boxminus t_j,\ A(t_i) \vdash_{S^a} A(t_i//t_j)$
  En utilisant deux fois le métathéorème 3 on obtient le résultat suivant:
  **] $\vdash_{S^a} (t_i \boxminus t_j) \supset (A(t_i) \supset A(t_i//t_j))$
  Un système formel du premier ordre qui, quels que soient t_i et t_j, possède les deux théorèmes *] et **] est appelé un système formel du premier ordre avec égalité.

3. INTERPRETATION DU SYSTEME S^a

Nous avons construit le système S^a dans l'intention de formaliser l'arithmétique élémentaire. Nous considérerons donc l'ensemble des nombres entiers naturels comme domaine d'objets: $\Omega = \mathbb{N}$.

La présentation de cette interprétation n'est cependant pas simple. En effet, il est nécessaire d'éviter toute confusion entre ce qui

relève du domaine syntaxique et ce qui concerne le domaine sémantique de notre développement. Il est donc indispensable de distinguer ce qui appartient au système S^a et ce qui appartient à l'arithmétique de notre enfance.

De manière à rendre plus explicite la construction de S^a, nous avons attribué à certains objets formels des formes qui correspondent aux signes utilisés dans l'arithmétique même. Et c'est ici qu'il y a quelques risques d'ambiguïté. Afin d'éviter cela, nous ferons la distinction suivante lorsque nous construirons l'interprétation:

Symboles de S^a	Signes arithmétiques	expression de la métalangue
$\underline{0}$	0	
*	+1	
⊞	+	
⊡	·	
⊟	=	=df
⊯	≠	

Il s'agit également de proposer des applications Ψ de telle manière qu'elles seront conformes à notre projet interprétatif. Nous voulons en effet établir une correspondance entre l'objet formel $\underline{0}$ et le zéro de l'arithmétique, entre l'objet formel ⊞ et l'addition, etc. Pour ce faire, il est nécessaire de disposer d'une application bien choisie Ψ, de chacune des espèces suivantes:

1) $\Psi_C : EC \longrightarrow \mathbb{N}$

2) $\Psi_V : EV \longrightarrow \mathbb{N}$

3) $\Psi_{P^2} : EP^2 \longrightarrow (\mathbb{N}^2)$ [organisation relationnelle]

4) $\Psi_{F^1} : EF^1 \longrightarrow (\mathbb{N}^2)$ [organisation fonctionnelle unaire]

5) $\Psi_{F^2} : EF^2 \longrightarrow (\mathbb{N}^2 \times \mathbb{N})$ [organisation fonctionnelle binaire]

Précisons d'emblée que nous éviterons d'attribuer aux objets formels que sont les foncteurs et le prédicat leur signification extensionnelle. Afin de ne pas compliquer davantage la présentation de cette interprétation, nous utiliserons la connaissance partagée par tous des propriétés opératoires ou relationnelles de la signification intensionnelle de l'égalité, de l'addition, etc. Ainsi, par exemple, au lieu d'associer à l'objet formel ⊟ la représentation extensionnelle suivante:

$$\{\langle 0,0\rangle\ ,\ \langle 1,1\rangle,\ \langle 2,2\rangle,\ \langle 3,3\rangle,\ldots,\ \langle n,n\rangle,\ldots\}\ ,$$

nous utiliserons la connaissance naïve que nous possédons de l'égalité dans l'arithmétique.

Nous expliciterons alors les applications Ψ de la manière suivante:

Ψ_{P2} ($\boxminus$) =df = [égalité]

Ψ_{F1} (*) =df +1 [successeur immédiat]

Ψ_{F2} ($\boxplus$) =df + [l'addition]

Ψ_{F2} ($\boxdot$) =df · [la multiplication]

Dans le système S^a, nous ne disposons que d'une constante $\underline{0}$. Avec celle-ci et le foncteur de degré un *, nous pouvons établir une correspondance entre un ensemble de termes t sans variable et l'ensemble des images numériques. Posons:

Ψ_C ($\underline{0}$) =df 0

Ψ_{F1} (t*) =df Ψ_{F1} (t) +1

Avec ce qui précède, on obtient les correspondances suivantes:

$$\begin{aligned}
\Psi_{F1}\ (\underline{0}^*) &=df\ \Psi_{F1}\ (\underline{0}) + 1\\
&=df\ 0 + 1\\
&=df\ 1\\
\Psi_{F1}\ (\underline{0}^{**}) &=df\ \Psi_{F1}\ (\underline{0}^*) + 1\\
&=df\ 1 + 1\\
&=df\ 2\\
&\ \ \vdots\\
\Psi_{F1}\ (\underbrace{\underline{0}^{*\cdots *}}_{n\ \text{fois}}) &=df\ \Psi_{F1}\ (\underbrace{\underline{0}^{*\cdots *}}_{n-1\ \text{fois}}) + 1\\
&=df\ (n - 1) + 1\\
&=df\ n
\end{aligned}$$

Par convention et suite à cette construction, nous associerons à l'objet formel $\underline{0}$ suivi de n astérisques, le symbole $\underline{n}$, c'est-à-dire son expression numérale. Il est dès lors possible de simuler à travers les ob-

jets formels que sont les numéraux, la suite des entiers naturels.

$\underline{0}, \underline{1}, \underline{2}, \underline{3}, \ldots, \underline{n}, \ldots$ [cf. p. 70]

Mais l'expression numérale d'un terme peut prendre d'autres formes encore. Pour s'en convaincre étudions l'exemple suivant:

$$\underbrace{\underline{0}^{*\cdots*}}_{r \text{ fois}}$$

En utilisant la convention sus-mentionnée, on peut désigner cet objet formel par le numéral $\underline{r}$. Mais il est possible d'agir autrement. En effet, le nombre d'astérisques qui suit $\underline{0}$ pourrait s'exprimer d'une autre manière en utilisant l'arithmétique naïve, par exemple:

$$m + n, \quad \text{si } m + n = r$$

ou

$$k \cdot p, \quad \text{si } k \cdot p = r$$

L'objet $\underline{0}^{*\cdots*}$ peut donc ainsi être également associé aux expressions numérales $\underline{m + n}$ ou $\underline{k \cdot p}$. Cette manière de faire ne détermine pas immédiatement que le numéral $\underline{r}$ possède la relation d'égalité formelle avec le numéral $\underline{m + n}$, par exemple. Il est donc nécessaire de s'assurer que l'interprétation choisie est adéquate, donc que les axiomes a_1-a_9 confèrent bien aux symboles formels les propriétés des signes arithmétiques. C'est un des deux problèmes que nous aurons à traiter. Quant à l'autre problème, il consistera à vérifier qu'il est possible de définir certains symboles que l'on trouve en arithmétique (l'opération de puissance, par exemple) et qui ne figurent pas dans S^a.

3.1 Quelques métathéorèmes

METATHEOREME 34.1 - Quel que soit le nombre entier naturel n: $\vdash \underline{n^*} \boxminus \underline{n + 1}$

Démonstration:

1) Le numéral $\underline{n}$ n'est rien d'autre que l'objet formel $\underline{0}$ suivi de n symboles *.
2) Le numéral $\underline{n^*}$ n'est rien d'autre que l'objet formel $\underline{0}$ suivi de n + 1 symboles *.

On a par la règle réf :

$$\underbrace{\underline{0}^{*\cdots*}}_{n \text{ fois}}\underbrace{*}_{1 \text{ fois}} \boxminus \underline{0}^{\underbrace{*\cdots*}_{n+1 \text{ fois}}}$$

on obtient donc $\vdash \underline{n^*} \boxminus \underline{n + 1}$

METATHEOREME 34.2 - Quels que soient les nombres m et n, si m = n alors
$\vdash \underline{m} \boxminus \underline{n}$

Démonstration. Les numéraux $\underline{m}$ et $\underline{n}$ ne sont rien d'autre que l'objet formel $\underline{0}$ suivi de m, respectivement n symboles *. Il suffit donc de compter les astérisques.

METATHEOREME 34.3 - Quels que soient les nombres m et n, si $m \neq n$ alors
$\vdash \sim(\underline{m} \boxminus \underline{n})$

Démonstration. Supposons que le nombre m est plus petit que le nombre n et raisonnons par l'absurde.
Hypothèse: si $m \neq n$ alors $\vdash \underline{m} \boxminus \underline{n}$

En appliquant m fois l'axiome a_4, on obtient

$$\vdash \underline{0} = \underline{0}\overbrace{*\ldots*}^{(n-m)\text{ fois}}$$

Mais supposons $n - m > 0$. Il existe donc un nombre k tel que:

$$\vdash \underline{0} = \underline{k}*$$

ce qui contredit l'axiome a_3.
Ainsi, si $m \neq n$ alors $\vdash \sim(\underline{m} \boxminus \underline{n})$

METATHEOREME 34.4 - Quels que soient les nombres m et n:
$\vdash (\underline{m + n}) \boxminus (\underline{m} \boxplus \underline{n})$

Démonstration. Nous procéderons par induction sur le le nombre n.

Base de l'induction : n = 0
Il faut donc prouver : $\vdash (\underline{m + 0}) \boxminus (\underline{m} \boxplus \underline{0})$

1.	$(v_i \boxplus \underline{0}) \boxminus v_i$	a_5
2.	$(\underline{m} \boxplus \underline{0}) \boxminus \underline{m}$	1; sub
3.	$(\underline{m + 0}) \boxminus \underline{m}$	m + 0 = m; Mth. 34.2
4.	$\underline{m} \boxminus (\underline{m} \boxplus \underline{0})$	2, sym
5.	$(\underline{m + 0}) \boxminus (\underline{m} \boxplus \underline{0})$	4,3; rem, t_i est $\underline{m}$ et $A(t_i)$ est $(\underline{m + 0}) \boxminus \underline{m}$

Hypothèse d'induction : n = k

Quel que soit le nombre m, si n = k alors $\vdash(\underline{m + k}) \boxminus (\underline{m} \boxplus \underline{k})$

Pas d'induction : n = n + k

Quel que soit le nombre m, si n = k + 1 alors
$\vdash(\underline{m} + (\underline{k} + 1)) \boxminus (\underline{m} \boxplus (\underline{k} + 1))$

1. $(\underline{m} + \underline{k}) \boxminus (\underline{m} \boxplus \underline{k})$	hyp. d'ind.
2. $(v_i \boxminus v_j) \supset (v_i^* \boxminus v_j^*)$	a_2
3. $((\underline{m} + \underline{k}) \boxminus (\underline{m} \boxplus \underline{k})) \supset ((\underline{m} + \underline{k})^* \boxminus (\underline{m} \boxplus \underline{k})^*)$	2;sub; $v_i/\underline{m} + \underline{k}$, $v_j/\underline{m} \boxplus \underline{k}$
4. $(\underline{m} + \underline{k})^* \boxminus (\underline{m} \boxplus \underline{k})^*$	1, 3; MP
5. $(\underline{m} \boxplus \underline{k})^* \boxminus (\underline{m} + \underline{k})^*$	4; sym
6. $(v_i \boxplus v_j^*) \boxminus (v_i \boxplus v_j)^*$	a_6
7. $(\underline{m} \boxplus \underline{k}^*) \boxminus (\underline{m} \boxplus \underline{k})^*$	6; sub, $v_i/\underline{m}$, $v_j/\underline{k}$
8. $(\underline{m} \boxplus \underline{k}^*) \boxminus (\underline{m} + \underline{k})^*$	5,7; rem, t_i est $(\underline{m} \boxplus \underline{k})^*$; $A(t_i)$ est $(\underline{m} \boxplus \underline{k}^*) \boxminus (\underline{m} \boxplus \underline{k})^*$
9. $(\underline{m} + \underline{k})^* \boxminus ((\underline{m} + \underline{k}) + 1)$	Mth. 34.1
10. $((\underline{m} + \underline{k}) + 1) \boxminus (\underline{m} + (\underline{k} + 1))$	((m + k) + 1) = (m + (k + 1))
11. $(\underline{m} + \underline{k})^* \boxminus (\underline{m} + (\underline{k} + 1))$	9, 10; tra
12. $(\underline{m} + (\underline{k} + 1)) \boxminus (\underline{m} \boxplus \underline{k}^*)$	8, 11; rem
13. $\underline{k}^* \boxminus \underline{k} + 1$	Mth. 34.1
14. $(\underline{m} + (\underline{k} + 1)) \boxminus (\underline{m} \boxplus (\underline{k} + 1))$	12, 13 rem

METATHEOREME 34.5 - Quels que soient les nombres m et n:
$\vdash(\underline{m} \cdot \underline{n}) \boxminus \underline{m} \boxdot \underline{n}$

Q u e s t i o n :

121. Démontrer le métathéorème 34.5.

Il est possible de définir dans le système S^a des objets formels capables de représenter des opérations et des relations arithmétiques autres que l'addition, la multiplication et l'égalité. A titre d'illustration, proposons deux études de cas.

DEFINITION 39 - -objet formel de l'opération de puissance- Il s'agit de l'objet formel P. Il appartient à la famille des foncteurs de degré deux et se définit ainsi:
$Pv_i\underline{0} =df \underline{0}^*$ et $Pv_iv_j^* =df (Pv_iv_j) \boxdot v_i$

Q u e s t i o n :

122. Quels sont les numéraux suivants:
P $\underline{3}$ $\underline{0}$, P $\underline{3}$ $\underline{0}^*$, P $\underline{3}$ $\underline{0}^{**}$?

METATHEOREME 35 - Quels que soient les nombres m et n; $\vdash P\ \underline{m}\ \underline{n} \boxminus \underline{m^n}$

Démonstration. Nous procéderons par induction sur le nombre n.

Base de l'induction: n = 0

Il faut donc prouver : $\vdash P\ \underline{m}\ \underline{0} \boxminus \underline{m^0}$

1. P $\underline{m}$ $\underline{0}$ ⊟ P $\underline{m}$ $\underline{0}$	ref
2. P $\underline{m}$ $\underline{0}$ ⊟ $\underline{0}^*$	Déf. 39
3. $\underline{0}^*$ ⊟ $\underline{0 + 1}$	Mth. 34.1
4. $\underline{0 + 1}$ ⊟ $\underline{1}$	0 + 1 = 1; Mth. 34.2
5. $\underline{0}^*$ ⊟ $\underline{1}$	3, 4; rem
6. P $\underline{m}$ $\underline{0}$ ⊟ $\underline{1}$	5, 2; rem
7. $\underline{1}$ ⊟ $\underline{m}^0$	$1 = m^0$; Mth. 34.2
8. P $\underline{m}$ $\underline{0}$ ⊟ $\underline{m}^0$	7, 6; rem

Hypothèse d'induction

Quel que soit le nombre m, si n = k : $\vdash P\ \underline{m}\ \underline{k} \boxminus \underline{m^k}$

Pas d'induction

Quel que soit le nombre m, si n = k + 1 :
$\vdash P\ \underline{m}\ \underline{(k + 1)} \boxminus \underline{m^{(k + 1)}}$

1. P $\underline{m}$ $\underline{k}$ ⊟ $\underline{m}^k$	hyp. d'ind.
2. P $\underline{m}$ $\underline{k}^*$ ⊟ P $\underline{m}$ $\underline{k}^*$	ref
3. P $\underline{m}$ $\underline{k}^*$ ⊟ ((P $\underline{m}$ $\underline{k}$) ⊡ $\underline{m}$)	Déf. 39
4. P $\underline{m}$ $\underline{k}^*$ ⊟ $\underline{m}^k$ ⊡ $\underline{m}$	1, 3; rem, t_i est P $\underline{m}$ $\underline{k}$ et $A(t_i)$ est P $\underline{m}$ $\underline{k}^*$ ⊟ ((P $\underline{m}$ $\underline{k}$) ⊡ $\underline{m}$)
5. $\underline{m}^k$ ⊡ $\underline{m}$ ⊟ $\underline{m^k . m}$	Mth. 34.5

6. P $\underline{m}$ $\underline{k}^*$ ⊟ $\underline{m^k \cdot m}$	5, 4; rem, t_i est $\underline{m^k}$ ⊡ $\underline{m}$ et $A(t_i)$ P $\underline{m}$ $\underline{k}^*$ ⊟ $\underline{m^k}$ ⊡ $\underline{m}$
7. $\underline{k}^*$ ⊟ $\underline{k + 1}$	Mth. 34.5
8. P $\underline{m}$ $\underline{k + 1}$ ⊟ $\underline{m^k \cdot m}$	7,6; rem, t_i est $\underline{k}^*$ ⊟ $\underline{k + 1}$ et $A(t_i)$ est P $\underline{m}$ $\underline{k}^*$ ⊟ $\underline{m^k \cdot m}$
9. $\underline{m^k \cdot m}$ ⊟ $\underline{m^{k+1}}$	$m^k \cdot m = m^{k+1}$; Mth. 34.2
10. P $\underline{m}$ $\underline{k + 1}$ ⊟ $\underline{m^{k+1}}$	9,8; rem, t_i est $\underline{m^k \cdot m}$ et $A(t_i)$ est P $\underline{m}$ $\underline{k + 1}$ ⊟ $\underline{m^k \cdot m}$

DEFINITION 40 - -objet formel de la relation d'inégalité- Il s'agit de l'objet formel ⊠. Il appartient à la famille des prédicats de degré deux.

v_i ⊠ v_j =df $(\exists v_k)((v_k$ ⊉ $\underline{0}) \wedge ((v_i \boxplus v_k)$ ⊟ $v_j))$

METATHEOREME 36.1 - Si m < n alors ⊢ $\underline{m}$ ⊠ $\underline{n}$

En arithmétique, m < n entraîne qu'il existe un nombre k tel que 1) $k \neq 0$ et 2) $m + k = n$

Démonstration.

1. $(\underline{m + k})$ ⊟ $\underline{n}$	2); Mth. 34.2
2. $(\underline{m + k})$ ⊟ $(\underline{m} \boxplus \underline{k})$	Mth. 34.4
3. $(\underline{m} \boxplus \underline{k})$ ⊟ $\underline{n}$	1, 2; rem, t_i est $(\underline{m + k})$ ⊟ $\underline{n}$ et $A(t_i)$ est $(\underline{m + k})$ ⊟ $(\underline{m} \boxplus \underline{k})$
4. $\underline{k}$ ⊉ $\underline{0}$	1); Mth. 34.2
5. $(\underline{k}$ ⊉ $0) \wedge ((\underline{m} \boxplus \underline{k})$ ⊟ $\underline{n})$	4, 5; $\wedge i$
6. $(\exists v_k)((v_k$ ⊉ $\underline{0}) \wedge ((\underline{m} \boxplus v_k)$ ⊟ $\underline{n}))$	5; $\exists i$
7. $\underline{m} < \underline{n}$	6; Déf. 40

METATHEOREME 36.2 - Si $m \neq n$ alors ⊢ $\sim(\underline{m} < \underline{n})$

Question :

123. Démontrer le métathéorème 36.2

Ce qui précède n'est, d'une certaine manière, qu'une illustration. En effet, il s'agissait de montrer d'une part que les axiomes a_1-a_9 conféraient bien aux symboles formels certaines des propriétés essen-

tielles des signes arithmétiques, et d'autre part, qu'il était possible de définir de nouveaux symboles capables d'être associés à d'autres opérations et relations arithmétiques que celles primitivement choisies. Un développement beaucoup plus complet est proposé dans l'admirable manuel de Mendelson [1979].

Remarques

* Le système S^a est capable de formaliser l'arithmétique élémentaire. Il s'agit d'un système du premier ordre avec égalité. Notre projet était d'associer au système S^a un modèle bien particulier. Celui-ci consiste en l'ensemble des nombres entiers naturels sur lequel, entre autres choses, la relation d'identité est définie. Cette relation est une relation d'équivalence.

* Quel que soit le modèle d'une théorie du premier ordre avec égalité, le correspondant sémantique du prédicat formel ≡ est une relation d'équivalence. Si cette relation d'équivalence est la relation d'identité, alors le modèle est appelé un modèle normal.

Question :

124. S^a possède-t-il un modèle normal de cardinalité finie?

Remarques

* L'ensemble des entiers naturels est donc un modèle normal de S^a. On le dira modèle standard dans la mesure où c'est intentionnellement que nous voulions représenter l'arithmétique naïve des nombres avec les différentes opérations élémentaires connues. Mais, contrairement à toute apparence, il n'y a pas qu'un modèle pour S^a. Tout modèle qui n'est pas isomorphe au modèle standard de S^a est appelé non standard. De plus, il existe des modèles non standard de S^a qui sont dénombrables, comme il en existe de cardinalité infinie non dénombrable.

* Ce qui précède met en évidence qu'il n'y a aucun moyen de caractériser formellement de manière univoque la théorie des nombres dits élémentaires. Et l'on en vient au résultat suivant qui est dû à Skolem [1933; 1934; 1971].

> Tout système du premier ordre avec égalité qui possède pour modèle, le modèle standard, possède également un autre modèle normal qui n'est pas isomorphe au modèle standard.

* Considérons un système formel qui possède pour modèle, le modèle standard. Si ce système contient une expression bien formée contenant une variable libre, A(v), alors deux situations peuvent être rencontrées:

1) Si les expressions suivantes sont des théorèmes:

$\vdash A(\underline{0})$
$\vdash A(\underline{1})$
$\vdash A(\underline{2})$
⋮
$\vdash A(\underline{n})$
⋮

et si de plus $\sim(\forall v)A(v)$ est un théorème du système, alors on le dira oméga-inconsistant. S'il n'y a pas d'ebf A telle que la situation précédente est vérifiée, on dira le système oméga-consistant.

2) Si les expressions suivantes sont des théorèmes:

$\vdash A(\underline{0})$
$\vdash A(\underline{1})$
⋮
$\vdash A(\underline{n})$
⋮

et si de plus $(\forall v)\,A(v)$ n'est pas un théorème du système, alors on le dira oméga-incomplet. S'il n'y a pas d'ebf A telle que la situation prédécente est vérifiée, on dira le système oméga-complet.

4. DEMONSTRATIONS DES REGLES UTILISEES

Règle sub : $A(v_i) \vdash_{Sa} A(t)$ si t libre pour v_i dans $A(v_i)$

1.	$A(v_i)$	prémisse
2.	$(\forall v_i)A(v_i)$	1; GEN
3.	$(\forall v_i)A(v_i) \supset A(v_i/t)$	A_4, si t est libre pour v_i dans $A(v_i)$
4.	$A(v_i/t)$	2, 3; MP

Règle réf : $\vdash_{S^a} t_i \boxminus t_i$ quel que soit le terme t_i

1. $(t_i \boxplus \underline{0}) \boxminus t_i$	a_5; v_i/t
2. $((t_i \boxplus \underline{0}) \boxminus t_i) \supset (((t_i \boxplus \underline{0}) \boxminus t_i) \supset (t_i \boxminus t_i))$	a_1; $v_i/t_i \boxplus \underline{0}$, v_j/t_i, v_k/t_i
3. $((t_i \boxplus \underline{0}) \boxminus t_i) \supset (t_i \boxminus t_i)$	1, 2; MP
4. $t_i \boxminus t_i$	1, 3; MP

Règle sym : Quels que soient les termes t_i et t_j, si $t_i \boxminus t_j$:

$$t_i \boxminus t_j \vdash_{S^a} t_j \boxminus t_i$$

1. $t_i \boxminus t_j$	prémisse
2. $(t_i \boxminus t_j) \supset ((t_i \boxminus t_i) \supset (t_j \boxminus t_i))$	a_1; v_i/t_i, v_j/t_j, v_k/t_i
3. $(t_i \boxminus t_i) \supset (t_j \boxminus t_i)$	1, 2; MP
4. $t_i \boxminus t_i$	réf
5. $t_j \boxminus t_i$	4, 3; MP

Règle tra : Quels que soient les termes t_i, t_j, t_k, si $t_i \boxminus t_j$ et $t_j \boxminus t_k$:

$$t_i \boxminus t_j,\ t_j \boxminus t_k \vdash_{S^a} t_i \boxminus t_k$$

1. $t_i \boxminus t_j$	prémisse
2. $t_j \boxminus t_k$	prémisse
3. $(t_j \boxminus t_i) \supset ((t_j \boxminus t_k) \supset (t_i \boxminus t_k))$	a_1; v_i/t_j, v_j/t_i, v_k/t_k
4. $t_j \boxminus t_i$	1; sym
5. $(t_j \boxminus t_k) \supset (t_i \boxminus t_k)$	4, 3; MP
6. $t_i \boxminus t_k$	2, 5; MP

Lemme *

Si deux termes t_i et t_j sont dans un rapport d'égalité formelle, alors, quel que soit le terme t qui contient t_i [ce que nous écrivons $t(t_i)$], $t(t_i) \boxminus t(t_i//t_j)$ est déductible dans S^a

$$t_i \boxminus t_j \vdash_{Sa} t(t_i) \boxminus t(t_i//t_j)$$

Démonstration: Nous procéderons par induction sur le nombre n des foncteurs de $t(t_i)$.

Base de l'induction: n = 0

Le terme $t(t_i)$ est t_i, et t_i est soit une variable, soit la constante.

1. $t_i \boxminus t_j$	prémisse
2. $t(t_i) \boxminus t(t_i//t_j)$	1; t_i est $t(t_i)$ et t_j est $t(t_i//t_j)$

Hypothèse d'induction :

Si $t_i \boxminus t_j$, et pour tout terme t qui contient le terme t_i et qui possède au plus n foncteurs :

$$t_i \boxminus t_j \vdash_{Sa} t(t_i) \boxminus t(t_i//t_j)$$

Pas d'induction :

Si $t_i \boxminus t_j$, et pour tout terme t qui contient le terme t_i et qui possède n + 1 foncteurs :

$$t_i \boxminus t_j \vdash_{Sa} t(t_i) \boxminus t(t_i//t_j)$$

A la commutativité près, $t(t_i)$ peut prendre l'une des trois formes suivantes:

a) $t_1(t_i) \boxplus t_2$

b) $t_1(t_i) \boxdot t_2$

c) $(t_1(t_i))^*$

Cas a):

1. $t_i \boxminus t_j$	prémisse
2. $t_1(t_i) \boxminus t_1(t_i//t_j)$	1; hyp. d'induction
3. $(t_1(t_i) \boxminus t_1(t_i//t_j)) \supset ((t_1(t_i) \boxplus t_2) \boxminus (t_1(t_i//t_j) \boxplus t_2))$	Quest. 120a
4. $(t_1(t_i) \boxplus t_2) \boxminus (t_1(t_i//t_j) \boxplus t_2)$	2,3; MP
5. $t(t_i) \boxminus t(t_i//t_j)$	4; $t_1(t_i) \boxplus t_2$ est $t(t_i)$ $t_1(t_i//t_j) \boxplus t_2$ est $t(t_i//t_j)$

Cas b) :

1. $t_i \boxminus t_j$	prémisse
2. $t_1(t_i) \boxminus t_1(t_i//t_j)$	1; hyp. d'induction
3. $(t_1(t_i) \boxminus t_1(t_i//t_j)) \supset ((t_1(t_i) \boxdot t_2) \boxminus (t_1(t_i//t_j) \boxdot t_2))$	Quest. 120b
4. $(t_1(t_i) \boxdot t_2) \boxminus (t_1(t_i//t_j) \boxdot t_2)$	2, 3; MP
5. $t(t_i) \boxminus t(t_i//t_j)$	4; $t_1(t_i) \boxdot t_2$ est $t(t_i)$ $t_1(t_i//t_j) \boxdot t_2$ est $t(t_i//t_j)$

Cas c) :

1. $t_i \boxminus t_j$	Prémisse
2. $t_1(t_i) \boxminus t_1(t_i//t_j)$	1; hyp. d'induction
3. $(t_1(t_i) \boxminus t_1(t_i//t_j)) \supset ((t_1(t_i))^* \boxminus (t_1(t_i//t_j))^*)$	Quest. 120c
4. $(t_1(t_i))^* \boxminus (t_1(t_i//t_j))^*$	2,3; MP
5. $t(t_i) \boxminus t(t_i//t_j)$	4; $(t_1(t_i))^*$ est $t(t_i)$ $(t_1(t_i//t_j))^*$ est $t(t_i//t_j)$

Règle rem :

Quels que soient les termes t_i et t_j, et quelle que soit l'ebf $A(t_i)$ qui contient t_i libre, si $t_i \boxminus t_j$ alors à chaque occurrence de t_i pour laquelle t_j est libre pour lui dans $A(t_i)$, on peut remplacer t_i par t_j

$$t_i \boxminus t_j,\ A(t_i) \vdash_{Sa} A(t_i//t_j)$$

Nous procéderons par induction sur le nombre n des connecteurs de $A(t_i)$.

Base de l'induction : n = 0

Si $A(t_i)$ ne contient aucun connecteur et si $t_i \boxminus t_j$, alors à chaque occurrence libre de t_i pour laquelle t_j est libre dans $A(t_i)$, on peut remplacer t_i par t_j: $A(t_i//t_j)$.

L'expression $A(t_i)$ est nécessairement de la forme $t_1 \boxminus t_2$, t_1 et t_2 sont des termes, et l'un et(ou) l'autre contiennent t_i.

Exemple $\underbrace{(v_i \boxplus v_k)}_{t_i} \boxminus \underbrace{(v_i \boxdot v_j)}_{t_j}{}^*$

$A(t_i) : (v_m \boxdot (v_i \boxplus v_k)) \boxminus (v_n \boxdot v_p)$

Démonstration:

1. $t_i \boxminus t_j$	prémisse
2. $A(t_i)$	prémisse
3. $t_1(t_i) \boxminus t_2(t_i)$	2; $A(t_i)$ est $t_1(t_i) \boxminus t_2(t_i)$
4. $t_1(t_i) \boxminus t_1(t_i)$	réf
5. $t_1(t_i) \boxminus t_1(t_i//t_j)$	1,4; Lemme *
6. $t_2(t_i) \boxminus t_2(t_i)$	réf
7. $t_2(t_i) \boxminus t_2(t_i//t_j)$	1, 6; Lemme *
8. $t_1(t_i//t_j) \boxminus t_2(t_i//t_j)$	3, 5, 7; Quest. 120f; MP
9. $A(t_i//t_j)$	8; $t_1(t_i//t_j) \boxminus t_2(t_i//t_j)$ est $A(t_i//t_j)$

Hypothèse d'induction

Si $A(t_i)$ contient au plus n connecteurs et si $t_i \boxminus t_j$, alors à chaque occurrence libre de t_i pour laquelle t_j est libre dans $A(t_i)$, on peut remplacer t_i par t_j : $A(t_i//t_j)$

Pas d'induction

Si $A(t_i)$ contient n + 1 connecteurs et si $t_i \boxminus t_j$, alors à chaque occurrence libre de t_i pour laquelle t_j est libre dans $A(t_i)$, on peut remplacer t_i par t_j: $A(t_i//t_j)$.

Trois cas sont à étudier:

a) $A(t_i)$ est de la forme $\sim B(t_i)$

b) $A(t_i)$ est de la forme $B(t_i) \supset C(t_i)$

c) $A(t_i)$ est de la forme $(\forall v)B(t_i)$

Démonstrations

Cas a) :

1. $t_i \boxminus t_j$	prémisse
2. $A(t_i)$	prémisse
3. $\sim B(t_i)$	2; $A(t_i)$ est $\sim B(t_i)$
4. $(t_i \boxminus t_j) \supset (B(t_i) \supset B(t_i//t_j))$	1,3; $B(t_i)$ entre dans le champ de l'hyp. d'ind. Mth.3
5. $t_j \boxminus t_i$	1; sym
6. $(t_j \boxminus t_i) \supset (B(t_i//t_j) \supset B(t_i))$	4, 5; $B(t_i//t_j)$ entre dans le champ de l'hyp. d'induction; chaque occurrence de t_j est remplacée par t_i Mth. 3
7. $B(t_i//t_j) \supset B(t_i)$	5,6; MP
8. $\sim B(t_i) \supset \sim B(t_i//t_j)$	7, contraposée
9. $\sim B(t_i//t_j)$	3,8; MP
10. $A(t_i//t_j)$	9, $\sim B(t_i//t_j)$ est $A(t_i//t_j)$

Cas b)

1. $t_i \boxminus t_j$	Prémisse
2. $A(t_i)$	Prémisse
3. $B(t_i) \supset C(t_i)$	$A(t_i)$ est $B(t_i) \supset C(t_i)$
4. $(t_i \boxminus t_j) \supset (B(t_i) \supset B(t_i//t_j))$	1,3; $B(t_i)$ entre dans le champ de l'hyp. d'ind. Mth. 3
5. $t_j \boxminus t_i$	1; sym
6. $(t_i \boxminus t_j) \supset (C(t_i) \supset C(t_i//t_j))$	1,3; $C(t_i)$ entre dans...
7. $(t_j \boxminus t_i) \supset (B(t_i//t_j)) \supset B(t_i))$	5,4; $B(t_i//t_j)$ entre dans le champ de l'hyp. d'ind.; chaque occurrence de t_j est remplacée par t_i Mth. 3
8. $B(t_i//t_j) \supset B(t_i)$	5, 7; MP $[P \supset Q]$
9. $B(t_i) \supset C(t_i)$	3, répétition $[Q \supset R]$
10. $C(t_i) \supset C(t_i//t_j)$	1, 6; MP $[R \supset T]$
11. $(P \supset Q) \supset ((Q \supset R) \supset ((R \supset T) \supset (P \supset T)))$	Mth. de L^0
12. $B(t_i//t_j) \supset C(t_i//t_j)$	8, 9, 10, 11; MP
13. $A(t_i//t_j)$	12; $B(t_i//t_j) \supset C(t_i//t_j)$ est $A(t_i//t_j)$

Cas c) :

1. $t_i \boxplus t_j$	Prémisse
2. $A(t_i)$	Prémisse
3. $(\forall v)B(t_i)$	2; $A(t_i)$ est $(\forall v)B(t_i)$
4. $(\forall v)B(t_i) \supset B(t_i)$	A_4; t_i est libre pour t_i dans $B(t_i)$
5. $B(t_i)$	3, 4; MP
6. $B(t_i//t_j)$	1, 5; hyp. d'ind.
7. $(\forall v)B(t_i//t_j)$	6; GEN
8. $A(t_i//t_j)$	7; $(\forall v)B(t_i//t_j)$ est $A(t_i//t_j)$

CHAPITRE 6 - LES FONCTIONS RECURSIVES

1. PREAMBULE

Dans les parties précédentes, nous avons marqué l'enjeu et l'intérêt d'une démarche qui vise à construire un système formel capable de représenter l'arithmétique, et nous avons exposé un système qui formalise la théorie des nombres. Mais cette théorie est également un instrument pour le logicien. En effet, un des problèmes fondamentaux de la théorie des systèmes formels est celui de la décidabilité. Il est donc important et nécessaire de s'intéresser à une méthode effective permettant d'affirmer, par exemple, qu'une ebf *est ou n'est pas* un théorème. La nécessité d'utiliser des fonctions caractéristiques [Déf. 36] et la connaissance que l'on possède de l'arithmétique élémentaire nous entraîne à nous intéresser à l'existence des fonctions arithmétiques définies sur les nombres entiers naturels qui sont effectivement calculables ainsi qu'à l'ensemble de plus grande extension qui les contiendrait. Mais pourquoi donc s'intéresser à un tel ensemble alors que nous sommes plus directement concernés par des systèmes formels dont la présentation syntaxique apparaît sans relation apparente avec le numérique? C'est que Gödel a rendu cette relation effective. Nous l'avons montré [pp. 37-40], il est possible d'arithmétiser la syntaxe d'un système formel. Nous avons fourni une méthode qui permet d'attribuer de manière univoque un nombre à chaque élément du vocabulaire, à chaque ebf et à chaque suite d'expressions bien formées. Mais la numérotation de Gödel ne s'applique pas uniquement à ces éléments. Par elle, il est également possible d'assigner un nombre de Gödel à des éléments de la métalangue tels que: "être un axiome", "être une preuve", "être telle définition",... Comme l'écrit Dumitriu [1977: 221]: par cette arithmétisation "the elements of a system S are arithmetically transposed in a metasystem". Ainsi, aux expressions syntaxiques, à leurs propriétés et à leurs relations correspondent des éléments, des propriétés et des relations arithmétiques. Dès lors, la recherche de procédures arithmétiques effectivement calculables se trouve pleinement justifiée.

Si l'aperception de la notion de ce qui est effectivement calculable ne semble guère poser de problème, son identification à une démarche effective de calcul ou à une approche algorithmique n'est pas élémentaire. En effet, la volonté de définir l'ensemble de plus grande extension des fonctions effectivement calculables pose le problème de la caractérisation de la cal-

culabilité. Dès la fin des années vingt, on observe différentes démarches dont l'objectif est de définir exactement l'ensemble des fonctions effectivement calculables. Nous mentionnerons quatre d'entre elles:

- Jacques Herbrandt [1908-1931], dans sa thèse de doctorat [1930] et Kurt Gödel [1906-1978] en 1931 exposent la notion de fonction récursive.

- En 1933, Alonzo Church [né en 1903] propose d'identifier l'idée intuitive de fonctions effectivement calculables aux fonctions λ-définissables. La définition de ces fonctions est due conjointement à A. Church et Stephen C. Kleene [né en 1909] en 1935. Suite à une discussion avec Gödel [KNEALE 1962: 733], Church propose également de les identifier aux fonctions récursives. Cette décision aboutit à ce qui est connu comme la thèse de Church.

> THESE DE CHURCH: Toute fonction effectivement calculable est récursive ou λ-définissable.

- Alan Mathison Turing [1912-1956] publie en 1936 un article dans lequel il définit les fonctions calculables par ce qu'on a appelé par la suite "les machines de Turing".

Andrë Andreïevitch Markov [1856-1922] en 1951 fonde une telle identification sur la théorie des algorithmes.

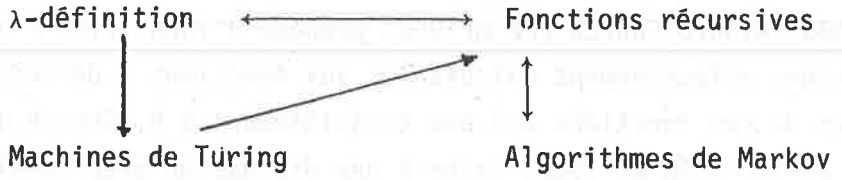
L'existence de ces différentes théories capables de représenter l'effectivement calculable posait bien entendu le problème de leur puissance représentative respective. En effet, chacune de ces démarches théoriques exprimait-elle un ensemble équivalent de fonctions calculables? En 1936, Kleene fournit une première réponse: l'ensemble des fonctions calculables par λ-définissabilité est équivalent à celui des fonctions récursives. L'année suivante, Turing démontre que toute fonction λ-définissable est calculable par une machine de Turing et que toute fonction calculable par une telle machine est une fonction récursive. Enfin, V. Detlovs [1953] a établi l'équivalence entre l'ensemble des fonctions récursives et celui des fonctionscalculables à l'aide des algorithmes de Markov. Ainsi, les quatre ensembles de fonctions ont même extension et on n'a pas trouvé de définition qui fournisse une classe plus étendue. On peut donc énoncer la thèse généralisée de Church:

THESE GENERALISEE DE CHURCH: Une fonction est effectivement calculable si c'est:

- une fonction récursive, ou
- une fonction λ-définissable, ou

- une fonction calculable par une machine de Turing, ou
- une fonction calculable par un algorithme de Markov.

Le schéma suivant est de nature à mieux faire comprendre les démarches qui ont abouti à la thèse généralisée de Church:



Nous présenterons la classe des fonctions effectivement calculables sous leur forme de fonctions récursives. Et nous consacrerons un nouveau cahier pour montrer l'usage qu'en a fait Gödel.

2. OU IL EST QUESTION DE LA NOTION DE FONCTION

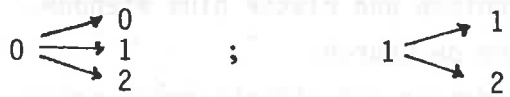
Nous avons utilisé le terme de fonction sans pour autant avoir pris la précaution de définir cette notion. Bien que, d'une certaine manière, celle-ci est tombée dans le 'domaine publique', derrière elle se profile quelques ambiguïtés qu'il est souhaitable de dissiper. Avec cette intention, étudions l'exemple suivant.

Soit le domaine d'objets Ω, $\Omega = \{0, 1, 2\}$.
Associons à ce domaine deux organisations relationnelles:

a) $O_1 = \{<0,0>, <0,1>, <0,2>, <1,1>, <1,2>, <2,2>\}$

b) $O_2 = \{<0,0>, <1,1>, <2,1>\}$

L'organisation O_1 représente de manière extensionnelle la relation "être plus petit ou égal à" sur Ω, alors que l'organisation O_2 exprime la relation "être associé à *sa* puissance deux modulo trois". La seconde relation possède une propriété que la première ne connaît pas. En effet, si l'on observe le jeu des correspondances associé à chaque couple, on remarque que dans a) une même valeur d'un argument antécédent est associée à plus d'une valeur d'un argument conséquent:



alors que dans le second cas, chaque valeur d'un argument antécédent est associée à *une et une seule* valeur d'un argument conséquent:

$0 \rightarrow 1$; $1 \rightarrow 1$; $2 \rightarrow 1$

Lorsqu'une relation est telle qu'à chaque valeur que contient l'ensemble des arguments antécédents correspond *une et une seule* valeur appartenant à l'ensemble des arguments conséquents, cette relation est appelée "RELATION UNI= VOQUE ou RELATION FONCTIONNELLE ou FONCTION" [TARSKI 1971: 91].

Q u e s t i o n :

125. La relation d'implication logique est-elle une relation univoque?

Ce caractère d'univocité attaché à la notion de fonction permet notamment, dans le domaine des nombres naturels, d'inscrire par une opération arithmétique ou une conjonction de telles opérations, de quelle manière les arguments antécédents et conséquents sont systématiquement articulés. Cette association nous intéresse directement dans la perspective d'engendrer un ensemble de fonctions effectivement calculables.

De ce qui précède, il semblerait que nous disposions de deux possibilités pour parler de fonctions: une représentation extensionnelle et une représentation "opératoire". Cette liberté n'est qu'apparente. En effet, si le domaine d'objets arithmétiques sur lequel la fonction est définie, est infini, seule une représentation qui est conçue sur une opération arithmétique garantit une correspondance relationnelle effective et systématique entre les arguments. Et si, bien souvent, on représente une fonction de manière extensionnelle en ne représentant que quelques couples d'une extension infinie, ce n'est qu'une manière de suggérer indirectement une régularité opératoire.

Exemple : $\Omega = \mathbb{N}$

$\sigma = \{<1,2>, <2,3>, <3,4>, <4,5>, \ldots\}$

Q u e s t i o n :

126. Existe-t-il des fonctions qui ne sont pas de nature arithmétique?

Il est nécessaire de disposer d'un vocabulaire et d'une terminologie pour représenter et parler des fonctions. Posons ce qui suit:

- Un ensemble de noms de fonction: {f, g, h, ...}
- Un ensemble pour désigner les arguments antécédents:

$$\{x_1, \ldots x_i, \ldots z_1, \ldots z_j, \ldots\}$$

- Un ensemble pour désigner les arguments conséquents: $\{y_1, \ldots y_k, \ldots\}$
- Un ensemble de noms d'ensembles d'arguments antécédents:

$$\{E_1, E_2, \ldots E_n, \ldots\}$$

- Un ensemble de noms d'ensembles d'arguments conséquents: $\{F_1, \ldots\}$
- Un ensemble d'opérations arithmétiques: $\{M_1, M_2, \ldots M_m, \ldots\}$

Dès lors, l'expression d'une relation univoque se présente ainsi:

Quelle que soit la valeur de l'argument antédécent x, $x \in E$, la fonction de nom f établit une correspondance univoque avec la valeur de l'argument conséquent y qui lui est associée, $y \in F$; cette valeur qui est f(x) est déterminée par l'opération arithmétique M liée à la fonction.

Exemple : $E = \{0, 1, 2, 3\}$; $F = \{0, 1, 2, 3\}$

$f = \{<0,0>, <1,1>, <2,0>, <3,3>\}$

Quelle que soit la valeur de l'argument antécédent x, $x \in \{0, 1, 2, 3\}$, la fonction de nom f établit une correspondance univoque avec la valeur de l'argument conséquent y qui lui est associée, $y \in \{0, 1, 2, 3\}$; cette valeur qui est f(x) est déterminée par l'opération arithmétique 'puissance trois modulo quatre'.

Cette manière complexe d'exprimer les choses se réduit traditionnellement à la forme très simplifiée suivante dans laquelle la quantification et le nom de la fonction sont sous-entendus, et le signe d'égalité apparaît comme celui d'une attribution calculable,

$$y = f(x) = x^3 (\text{mod} 4)$$

Jusqu'à maintenant, nous n'avons présenté que des relations univoques simples. Il s'agit de fonctions simples, elles ne possèdent qu'une seule variable, f(x). Il existe des fonctions plus complexes dans leur organisation. Ces fonctions se caractérisent par le fait que leurs arguments antécédents comportent n éléments, $n > 1$. Il s'agit de fonctions à n variables, $f(x_1, \ldots x_n)$. En voici un exemple:

$f : \{<<0,0>, 0>, <<0,1>, 0>, <<1,0>, 0>, <<1,1>, 1>\}$

Il s'agit bien d'une fonction. En effet, chaque argument antécédent (qui est complexe, mais qui n'est pas composé de nombres complexes!) est associé à une et une seule valeur d'argument conséquent. L'argument conséquent est donc toujours unique! Nous décrirons cette fonction ainsi:

Quelles que soient les valeurs x, z; $x \in \{0,1\}$ et $z \in \{0,1\}$; la fonction de nom f établit une correspondance univoque entre le couple <x,z> (argument antécédent) et la valeur de l'argument conséquent y qui lui est associée, $y \in \{0,1\}$; cette valeur qui est f(x,z) est déterminée par l'opération arithmétique "multiplication" sur {0,1}. Ce qui s'exprime de la manière réduite suivante : $y = f(x,z) = x.z$

A regarder de plus près ce qui précède, on observe qu'une fonction

est une application [fasc. I: 4.1]. Nous pouvons donc énoncer ce qui suit:

> Une fonction de nom f est une application de $E_1xE_2x...x\ E_n$ dans F, $[E_1xE_2x...x\ E_n \rightarrow F]$. Elle établit une correspondance univoque entre tout n-uple de $E_1xE_2x\ ...\ x\ E_n$ et la valeur de l'argument conséquent y qui lui est associé, $y \in F$; cette valeur qu'on note $f(x_1,..., x_n)$ est déterminée par l'opération arithmétique M; c'est-à-dire qu'elle est le résultat de l'opération M appliquée aux x_i.

Dorénavant, lorsque nous définirons une fonction, nous inscrirons son nom, les ensembles sur lesquels elle est définie et l'opération arithmétique qui lui est associée:

$$f : E_1x... \ x\ E_n \rightarrow F,\ f(x_1,..., x_n)\ \text{ est }\ M\ (x_1,..., x_n)$$

3. PRESENTATION NAIVE ET NON FORMALISEE DES FONCTIONS RECURSIVES

Notre intérêt à l'étude de la théorie des fonctions récursives réside dans le fait que son inscription au sein même d'un système formel permet d'établir des thèses métalogiques fondamentales. Avant de représenter ces fonctions dans un système formel, puis d'utiliser cette représentation, il convient de définir ces fonctions. Il n'est pas inutile de rappeler que nous nous intéressons aux *fonctions calculables définies sur les nombres entiers*, $[N^n \rightarrow N]$.

Cette notion de fonction calculable est quelque peu intuitive. Elle se doit donc d'être caractérisée par une théorie structurée. La théorie des fonctions récursives permet cette caractérisation. En structurant un ensemble de fonctions arithmétiques, elle offre la possibilité de définir un ensemble de fonctions calculables: l'ensemble des fonctions récursives [FR], dont on postule qu'il contient toutes les fonctions calculables définies sur les entiers, voir thèse de Church.

3.1 L'ensemble des fonctions récursives primitives

L'ensemble des fonctions récursives primitives [FRP] se construit de manière inductive. Il est donc nécessaire de disposer d'un ensemble de fonctions initiales [clauses initiales], d'un ensemble d'opérations permettant de générer de nouvelles fonctions récursives [clauses inductives] et enfin d'une clause finale.

Clauses initiales

1) La fonction ZERO [Z] est une fonction récursive primitive [FRP]

$Z : N \rightarrow N$, $Z(x) = 0$
Il s'agit d'une fonction constante.

2) La fonction SUCCESSEUR [S] est une FRP.
$S : N \rightarrow N$, $S(x) = x+1$

3) Les fonctions PROJECTIONS [P_i^n] sont des FRP.
$P_i^n : \underbrace{Nx \ldots xN}_{\underline{n} \text{ fois}} \rightarrow N$, $P_i^n(x_1,\ldots,x_n) = x_i$

Q u e s t i o n s :

127. Quelle est la valeur de Z(x) pour x = 128? x = 0?
128. Quelle est la valeur de S(x) pour x = 34? x =0?
129. Soit une fonction projection P_i^n. Quel rapport existe-t-il entre $\underline{n}$ et $\underline{i}$? Quelle condition est associée à $\underline{i}$ et à $\underline{n}$?
130. Quelle est la valeur des fonctions:
$P_2^3(x,y,z)$ pour x =113, y = 18, z = 12725?
$P_1^1(x)$ pour x = 29 ?

Clauses inductives

4) Opération de SUBSTITUTION [SUB]
Soit les fonctions $f, h_1,\ldots, h_n$ définies ainsi:

$f: \underbrace{Nx \ldots xN}_{\underline{n} \text{ fois}} \rightarrow N$, $f(x_1,\ldots, x_n)$ $\quad n > 0$

$h_1: \underbrace{Nx \ldots xN}_{\underline{k} \text{ fois}} \rightarrow N$, $h_1(x_1,\ldots, x_k)$ $\quad k > 0$

$\vdots$

$h_n: \underbrace{Nx \ldots xN}_{\underline{k} \text{ fois}} \rightarrow N$, $h_n(x_1,\ldots, x_k)$ $\quad k > 0$

Si $f, h_1,\ldots, h_n$ sont des FRP, alors la fonction g obtenue comme suit par l'opération de SUBSTITUTION est une FRP.

$g(x_1,\ldots x_k) = f(h_1(x_1,\ldots, x_k),\ldots, h_n(x_1,\ldots, x_k))$

on dit que la fonction g est obtenue par substitution à partir des fonctions $f, h_1,\ldots, h_n$. Cette opération permet entre autres choses de réduire le nombre des variables ou d'introduire de nouvelles variables à partir d'une FRP donnée.

Q u e s t i o n :

131. Dans cette opération SUB, quelle est la condition associée à n et à h?

Exemples :

a] Soit $f(x_1, x_2) = P_2^2(x_1, x_2)$

$h_1(x) = S(x)$

$h_2(x) = Z(x)$

Ces trois fonctions sont des FRP [clauses initiales]. Par l'opération SUB, la fonction suivante l'est également:

$g(x) = f(h_1(x), h_2(x))$

$g(x) = P_2^2(S(x), Z(x))$.

b] Soit $f(x_1, x_2) = P_1^2(x_1, x_2)$

$h_1(x_1, x_2, x_3) = P_2^3(x_1, x_2, x_3)$

$h_2(x_1, x_2, x_3) = P_1^3(x_1, x_2, x_3)$

Ces fonctions sont des FRP [clauses initiales]. Par l'opération SUB, la fonction g l'est aussi:

$g(x_1, x_2, x_3) = f(h_1(x_1, x_2, x_3), h_2(x_1, x_2, x_3))$

$g(x_1, x_2, x_3) = P_1^2(P_2^3(x_1, x_2, x_3), P_1^3(x_1, x_2, x_3))$

c] Soit $f(x) = S(x)$ FRP [clause initiale]

$h(x) = P_2^2(S(x), Z(x))$ FRP, Clauses initiales et SUB

$g(x) = f(h(x))$ est une FRP

$g(x) = S(P_2^2(S(x), Z(x)))$

Q u e s t i o n s :

132. Calculer les valeurs des fonctions g suivantes:

$g(x)$ de l'exemple a] pour $x = 13$

$g(x_1, x_2, x_3)$ de l'exemple b] pour $x_1 = 2$, $x_2 = 3$, $x_3 = 4$

$g(x)$ de l'exemple c] pour $x = 112$.

133. Inscrire, par l'opération SUB, la fonction $g(x_1, x_2)$ à partir des fonctions f, h_1, h_2, h_3.

$f(x_1, x_2, x_3) = P_2^3(x_1, x_2, x_3)$

$h_1(x_1, x_2) = S(P_1^2(x_1, x_2))$

$h_2(x_1, x_2) = P_2^2(x_1, x_2)$

$h_3(x_1, x_2) = P_1^2(x_1, x_2)$

134. La fonction $g(x_1, x_2) = P_2^2(x_1, S(x_2))$ est-elle récursive?

135. Définir:
   a) Une fonction constante différente de 0 : $f(x) = a$
   b) Une fonction constante généralisée : $f(x_1,\ldots, x_n) = a$

136. Construire la FRP dite permutation, pe. Elle permet de passer d'une fonction $f(x_1,\ldots, x_n)$ à la fonction $g(x_{i_1},\ldots, x_{i_n})$ en permutant les variables de f. Avant de construire une telle fonction, définir une fonction permutation à deux variables.

L'opération SUB permet de composer un très grand nombre de FRP. Cependant, l'ensemble de celles-ci ne contient aucune fonction 'évolutive'. Pour cela il faut disposer d'une autre opération.

5) L'opération de RECURRENCE [REC]

Par cette opération, on peut construire des FRP dont chaque valeur se calcule de manière progressive et ordonnée. C'est pour cela que nous les nommons 'évolutives'. Chacune d'entre elles se définit à l'aide de deux états: un état initial et un état inductif. Ces deux états sont représentés par deux fonctions de n, respectivement n+2 variables, et ils définissent une FRP de n+1 variables.

Soit les fonctions f et h définies ainsi:

$f: \underbrace{N \times \ldots \times N}_{n \text{ fois}} \to N,\ f(x_1,\ldots, x_n)$

$h: \underbrace{N \times \ldots \times N}_{n+2 \text{ fois}} \to N,\ f(x_1,\ldots, x_n, x_{n+1}, x_{n+2})$

Si f et h sont des FRP, alors la fonction g définie comme suit l'est aussi:

$g: \underbrace{N \times \ldots \times N}_{n+1 \text{ fois}} \to g(x_1,\ldots, x_n, x_{n+1})$

$$g(x_1,\ldots, x_n, x_{n+1}) : \begin{cases} \text{ETAT INITIAL} \\ g(x_1,\ldots, x_n, 0) = f(x_1,\ldots, x_n) \\ [\text{si } n = 0 \text{ on choisit une fonction constante}] \\ \text{ETAT INDUCTIF} \\ g(x_1,\ldots, x_n, a+1) = h(x_1,\ldots, x_n, a, g(x_1,\ldots, x_n, a)) \end{cases}$$

Lorsque nous voulons définir une fonction évolutive qui caractérise telle ou telle opération arithmétique, il est donc nécessaire d'analyser les états initial et inductif qui la fondent.

Exemples :

a] Intention: définition d'une FRP qui caractérise l'addition.

Analyse naïve des états associés à l'addition:

Etat initial : $x+0 = x$

Etat inductif: $x+(a+1) = (x+a)+1$

Construction d'une FRP + telle que

$+ : NxN \rightarrow N,\ +(x_1, x_2)$

et

$$+(x_1, x_2): \begin{cases} +(x_1, 0) \text{ soit } x_1 & \text{-état initial-} \\ +(x_1, a+1) \text{ soit } (x_1+a)+1 & \text{-état inductif-} \end{cases}$$

Détermination d'une FRP f à une variable et qui caractérise l'état initial.

$f: N \rightarrow N,\ f(x)$ telle que $f(x)$ soit x.

La FRP $P_1^1(x)$ remplit ces conditions.

Détermination d'une FRP h à trois variables et qui caractérise l'état inductif.

$h: NxNxN \rightarrow N,\ h(x_1, x_2, x_3)$ telle que $h(x_1, a, +(x_1, a))$ soit $(x_1+a)+1$

$h(x_1, x_2, x_3) = S(P_3^3(x_1, x_2, x_3))$ remplit ces conditions

Définition de la FRP +:

$$+(x_1, x_2) : \begin{cases} +(x_1, 0) = P_1^1(x_1) \\ +(x_1, a+1) = S(P_3^3(x_1, a, +(x_1, a))) \end{cases}$$

Questions :

137. Démontrer que la fonction $S(P_3^3(x_1, x_2, x_3))$ est une FRP.

138. Calculer "pas par pas" la valeur de $+(2, 2)$

b] Intention: définition d'une FRP qui caractérise la multiplication

Analyse naïve des états

Etat initial : $x.0 = 0$

Etat inductif : $x.(a+1) = (x.a)+x$

Construction d'une FRP . telle que

$. : NxN \rightarrow N,\ .(x_1, x_2)$

et

$$.(x_1, x_2) : \begin{cases} .(x_1, 0) \text{ soit } 0 & \text{-état initial-} \\ .(x_1, a+1) \text{ soit } (x_1.a)+x_1 & \text{-état inductif-} \end{cases}$$

Détermination d'une FRP f à une variable telle que:
f: N→N, f(x) telle que f(x) soit 0
La fonction Z(x) remplit ces conditions.

Détermination d'une FRP h à trois variables telle que
h: NxNxN → N, h (x_1, x_2, x_3) telle que
$h(x_1, a, .(x_1, a))$ soit $(x_1.a)+x_1$
La fonction $+(P_3^3(x_1, x_2, x_3), P_1^3(x_1, x_2, x_3))$ remplit ces conditions.

Définition de la FRP . :

$$.(x_1, x_2) : \begin{cases} .(x_1, 0) = Z(x_1) \\ . (x_1, a+1) = +(P_3^3(x_1, a, .(x_1, a)), P_1^3(x_1, a, .(x_1, a))) \end{cases}$$

Q u e s t i o n s :

139. Démontrer que $+(P_3^3(x_1, x_2, x_3), P_1^1(x_1, x_2, x_3))$ est une FRP.

140. Calculer "pas par pas" .(3, 2).

c] Intention: définition d'une FRP qui caractérise l'opération unaire 'factorielle'.

Analyse naïve des états

Etat initial : 0! = 1

Etat inductif : (a+1)! = (a+1).a!

Construction d'une FRP ! telle que :

! : N → N, !(x)

et

$$! : \begin{cases} !(0) \text{ soit } 1 \\ !(a+1) \text{ soit } (a+1).a! \end{cases}$$

Détermination d'une FRP f, constante, qui caractérise l'état initial:
f : N → N, f(x) telle que f(x) = 1
S(Z(x)) remplit ces conditions.

Détermination d'une FRP h, à deux variables qui caractérise l'état inductif:
h : NxN → N, $h(x_1,x_2)$ telle que $h(x_1, a+1)$ soit (a+1).a!
$.(S(P_1^2(x_1, x_2)), P_2^2(x_1, x_2))$ remplit ces conditions.

Définition de ! :

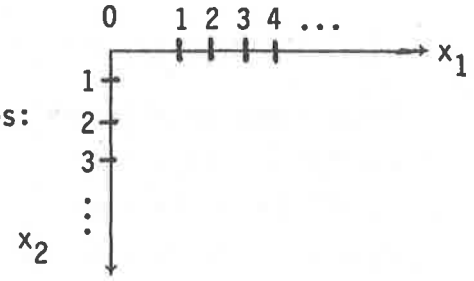
$$!(x) : \begin{cases} !(0) = S(Z(0)) \\ \\ !(a+1) = .(S(P_1^2(a, !(a))), P_2^2(a, !(a))) \end{cases}$$

Q u e s t i o n s :

141. Définir une FRP qui caractérise l'opération 'exponentielle'.
Suggestion: -poser $ex(x_1, x_2)$ pour $x_1^{x_2}$
-état initial : $x_1^0 = 1$ c'est-à-dire $ex(x_1, 0) = 1$
-état inductif, $ex(x_1, a+1) = h(x_1, a, ex(x_1, a))$
-la fonction h doit réaliser le produit de la première variable par la troisième.

142. Une fonction est dite polynomiale si elle a la forme suivante par exemple:
$f: NxN \rightarrow N$
$f(x_1, x_2) = ax^2+bx^3y^2+cy^9+ d$ avec a, b, c et d $\in$ N.
Les fonctions de ce type là sont-elles des FRP?

143. Soit la fonction suivante : $f: NxN \rightarrow N$
$f(x_1, x_2) = \frac{1}{2}(x_1+x_2)(x_1+x_2+1)+x_2$
Que détermine cette fonction si l'on applique la représentation suivante
Suggestion: calculer les valeurs suivantes:
f(0, 0), f(1, 0), f(0, 1), f(2, 0),
f(1, 1), f(0, 2), f(3, 0), ...



3.2 Etude de quelques FRP particulières

a) La fonction 'prédécesseur', pr:

$$pr(x) : \begin{cases} pr(0) = Z(0) \\ \\ pr(a+1) = S(P_2^2(a, pr(a))) \end{cases}$$

Cette fonction permet de calculer le prédécesseur de tout nombre entier naturel en respectant les conditions suivantes:
1] pr(x) = 0 si x est 0
2] pr(x) = x-1 si x est plus grand que 0.

b) La fonction 'monus', $\dot{-}$:

$$\dot{-}(x_1, x_2) : \begin{cases} \dot{-}(x_1, 0) = P_1^1(x_1) \\ \\ \dot{-}(x_1, a+1) = pr(P_3^3(x_1, a, \dot{-}(x_1, a))) \end{cases}$$

Cette fonction permet de calculer la différence positive de deux nombres en respectant les conditions suivantes:

1] $\dot{-}(x_1, x_2) = 0$ si x_1 est plus petit que x_2

2] $\dot{-}(x_1, x_2) = x_1 - x_2$ si x_1 est plus grand ou égal à x_2.

c) La fonction 'signe', si :

$$si(x) : \begin{cases} si(0) = Z(0) \\ \\ si(a+1) = S(Z(P_2^2(a, si(a)))) \end{cases}$$

Cette fonction attribue l'une des deux valeurs 1 ou 0 en respectant les conditions suivantes:

1] $si(x) = 0$ si x est 0

2] $si(x) = 1$ si x est différent de 0.

d) La fonction 'signe inversé', $\overline{si}$:

$$\overline{si}(x) = \dot{-}(S(Z(x)), P_1^1(x)).$$

Cette fonction attribue l'une des deux valeurs 1 ou 0 en respectant les conditions suivantes:

1] $\overline{si}(x) = 1$ si x est 0

2] $\overline{si}(x) = 0$ si x est différent de 0.

e) La fonction 'valeur absolue de la différence', va :

$$va(x_1, x_2) = +(\dot{-}(x_1, x_2), \dot{-}(x_2, x_1))$$

Dans la suite de cet exposé, nous nous autoriserons à mentionner les FRP d'une manière plus conforme à l'habitude mathématique. Nous écrirons, par exemple, $x_1 \dot{-} x_2$ en lieu et place de $\dot{-}(x_1, x_2)$.

Les fonctions précédentes ont un intérêt dont l'évidence n'apparaît pas immédiatement. Insistons tout d'abord sur le point suivant. Lorsque nous traitons des fonctions, bien souvent elles sont associées à des conditions. Ces conditions sont des relations. Il est donc nécessaire d'expliciter cette manière de faire. D'autre part, rappelons une des raisons pour laquelle nous nous intéressons aux fonctions récursives. Un de nos objectifs est de déter-

miner si une ebf donnée appartient ou non à l'ensemble des théorèmes. Nous exigeons plus: étant donné une suite d'ebf, celle-ci appartient-elle à l'ensemble des preuves? Ces deux questions se transposent en termes d'appartenance ou non d'un nombre à un ensemble de nombres. Dit autrement, une ebf (ou une suite d'ebf) arithmétiquement codée, appartient-elle à tel ou tel ensemble défini par une propriété ou une relation, elles aussi arithmétiquement codées? Il nous faut donc disposer d'une caractérisation de ces notions. Et pour rendre l'image de ces notions effective, il faut leur associer une procédure effectivement calculable, c'est-à-dire récursive.

Dans cette perspective, nous utiliserons à nouveau la notion de fonction caractéristique.

Soit R, une relation n-aire: $R(x_1,\ldots, x_n)$

$$f_R(x_1,\ldots, x_n) : \begin{cases} 0 \text{ si } x_1,\ldots, x_n & \text{ont entre eux la relation R} \\ 1 \text{ si } x_1,\ldots, x_n & \text{n'ont pas entre eux la relation R.} \end{cases}$$

DEFINITION : Une relation n-aire est primitive récursive [RPR] si et seulement si sa fonction caractéristique associée est une FRP.

Nous exposerons plus loin de quelle manière 'représenter' dans un SF ces relations n-aires.

Quelques propriétés et relations primitives récursives

a) La propriété ETRE UN NOMBRE ENTIER NATUREL, N :
$N(x)$; $f_N: N \rightarrow N$, $f_N(x) = Z(x)$

b) La propriété ETRE UN NOMBRE PAIR, P :
$P(x)$; $f_P: N \rightarrow N$,

$$f_P(x) : \begin{cases} f_P(0) = S(Z(0)) \\ f_P(a+1) = \overline{si}(a.f_P(a)) \end{cases}$$

Q u e s t i o n :

144. Calculer les valeurs de la fonction f_P pour $x \leq 6$.

c) La relation ETRE EGAL A, = :
$=(x_1, x_2)$; $f_= : NxN \rightarrow N$,
$f_=(x_1, x_2) = si(|x_1 \dot{-} x_2|)$

d) La relation ETRE PLUS GRAND QUE, > :
$>(x_1, x_2)$; $f_> : NxN \rightarrow N$,
$f_>(x_1, x_2) = \overline{si}(|x_1 \dot{-} x_2|)$

Q u e s t i o n :

145. Construire les fonctions $f_{\neq}$ et $f_{\geq}$ associées aux relations ETRE INEGAL A et ETRE PLUS GRAND OU EGAL A.

Quelques règles dérivées

Soit $R_1(x_1,\ldots, x_n)$ et $R_2(x_1,\ldots, x_n)$, deux RPR et $f_{R_1}(x_1,\ldots, x_n)$ et $f_{R_2}(x_1,\ldots, x_n)$, leurs FRP associées.

1] La conjonction des deux RPR est une RPR et sa FRP associée est:

$$f_{R_1}(x_1,\ldots, x_n) + f_{R_2}(x_1,\ldots,x_n)$$

2] La disjonction des deux RPR est une RPR si ces relations s'excluent mutuellement. La FRP associée est:

$$f_{R_1}(x_1,\ldots, x_n) \cdot f_{R_2}(x_1,\ldots, x_n)$$

3] La négation d'une RPR est une RPR. La FRP associée est:

$$(1\dot{-}f_R(x_1,\ldots, x_n))$$

Ces trois résultats sont généralisables et combinables.

4] Définition par cas.

Soit n RPR qui s'excluent mutuellement, $R_1,\ldots, R_n$ et telles que, quel que soit le k-uple $\langle x_1,\ldots, x_k\rangle$, il est vérifié par l'une des relations.

Soit les n FRP associées aux n RPR:

$f_{R_1},\ldots, f_{R_n}$

Soit enfin, n FRP:

$g_1,\ldots, g_n$

La fonction définie par cas comme suit est une FRP

$$h(x_1,\ldots, x_k) : \begin{cases} g_1(x_1,\ldots, x_k) & \text{si } R_1 \text{ est vraie} \\ \vdots & \\ g_n(x_1,\ldots, x_k) & \text{si } R_n \text{ est vraie} \end{cases}$$

Sa forme fonctionnelle est la suivante:

$h(x_1,\ldots, x_k) = g_1(x_1,\ldots, x_k)\cdot(1\dot{-}f_{R_1}(x_1,\ldots, x_k))+\ldots+g_n(x_1,\ldots, x_k)\cdot(1\dot{-}f_{R_n}(x_1,\ldots, x_k))$

Si $f(x_1,\ldots, x_n, z)$ est une FRP, alors

5] La fonction SOMMATION [SOM] définie comme suit l'est également:

$$SOM(x_1,\ldots, x_n, x) : \begin{cases} 0 & \text{si } z \text{ est } 0 \\ f(x_1,\ldots, x_n, 0)+\ldots+f(x_1,\ldots, x_n, z) & \text{si } z \text{ est plus grand que } 0 \end{cases}$$

$x \leq z$

Si $f(x_1,\ldots, x_n, z)$ est une FRP, alors

6] La fonction PRODUIT [PRO] définie comme suit est une FRP.

$$\underset{x\leq z}{PRO}(x_1,\ldots, x_n, x) : \begin{cases} 1 \text{ si } z \text{ est } 0 \\ f(x_1,\ldots, x_n, 0) \bullet \ldots \bullet f(x_1,\ldots, x_n, z) \\ \text{si } z \text{ est plus grand que } 0 \end{cases}$$

Soit $R(x_1,\ldots, x_n, x)$, une RPR, et f_R sa FRP associée.

7] La relation EXISTENTIELLE BORNEE [EB] est une RPR

$EB(x_1,\ldots, x_n, x)$: il a y un x, $x\leq z$, tel que $R(x_1,\ldots, x_n, x)$ est vraie.
$x\leq z$

Sa fonction associée se définit comme suit:

$$f_{EB}(x_1,\ldots, x_n, x) = \overline{si}(\underset{x\leq z}{SOM}(1\dot{-}f_R(x_1,\ldots, x_n, x)))$$

8] La relation UNIVERSELLE BORNEE [UB] est une RPR

$UB(x_1,\ldots, x_n, x)$: pour tout x, $x\leq z$, $R(x_1,\ldots, x_n, x)$ est vraie
$x\leq z$

Sa fonction associée se définit comme suit:

$$f_{UB}(x_1,\ldots, x_n, x) = \overline{si}\ (\underset{x\leq z}{PRO}(1\dot{-}f_k(x_1,\ldots, x_n, x))).$$

9] La fonction MINIMALISATION BORNEE [MB] est une FRP

$$MB(x_1,\ldots, x_n) : \begin{cases} \text{Le plus petit x plus petit que z (s'il existe)} \\ \text{tel que} \quad R(x_1,\ldots, x_n, x) \text{ est vraie} \\ z \text{ autrement.} \end{cases}$$

Construction de la fonction MB

Objectif: construire une fonction dont la valeur pour le k-ième x rencontré est k ($0\leq k\leq z$), pour autant que cet x particulier soit plus petit que z, qu'il valide la relation R, et qu'il soit le plus petit x remplissant ces conditions.

Analyse de la situation

Relations R avec les valeurs x, $x\leq z$

$$R(-, 0),\ R(-, 1),\ldots,\ R(-, k),\ R(-, k+1),\ldots,\ R(-, z)$$

Valeurs de la fonction caractéristique associée à R: f_R

$$1 \quad , 1 \quad ,\ldots, 0 \quad , 1 \quad ,\ldots, 0$$

↑ le premier x qui remplit les conditions

Modification des valeurs de la fonction f_R (quelles qu'elles soient) pour $x>k$

$$\underbrace{1 \quad , 1 \quad ,\ldots,}_{g(f_R(-, x)) = 1 \text{ pour } x<k}\ \underbrace{0 \quad , 0 \quad ,\ldots, 0}_{g(f_R(-, x)) = 0 \text{ pour } x\geq k}$$

$g(f(-, x))$: $si(PRO(f_R(-,x)))$
$x \leq z$

Sommation de la suite précédente :

1 , 2 1,..., k , k ,..., k
pour x = 0, x = ,..., x = k-1, x = k,..., x=z

Il s'agit de la fonction MB

$MB(x_1,..., x_n) = SOM(si(PRO(f_k(x_1,..., x_n, \bar{x}))))$
$x \leq z-1 \quad \bar{x} \leq x$

Le $\bar{x}$ est assujetti au x de la fonction SOM

Nous écrirons dorénavant cette fonction MB de la manière abrégée suivante:

$MB(x_1,..., x_n) = m[x<z](f_R(x_1,..., x_n, x))$

Pour toute RPR, un ensemble au plus dénombrable de fonctions MINIMALISATION BORNEE peut lui être associée. Il est intéressant de remarquer que toute FRP de type MB à n variables est définie à partir d'une FRP à n+1 variables.

Exemplification du mode de calcul d'une fonction MB.
Soit la RPR suivante:

$R(x_1, x_2, x) : x_1+x_2 = 2.x$

Soit la fonction caractéristique associée à cette relation R: f_R. Nous n'expliciterons pas cette fonction pour des raisons d'économie de place. Nous la mentionnerons chaque fois que nous en aurons l'usage sous sa forme générale: $f_R(x_1, x_2, x)$.

Détermination de la valeur de la fonction MB:

$MB: NxN \rightarrow N, MB(x_1, x_2) = m[x<z](f_R(x_1, x_2, x))$

pour les valeurs $x_1 = 3$, $x_2 = 1$ et $z = 3$.

Il s'agit donc de calculer le plus petit x, plus petit ou égal à 3 tel que 3+1 = 2.x
Dit autrement, il s'agit de calculer

$MB(3,1) = m[x<3](f_R(3, 1, x))$

$MB(3, 1) = SOM(si\ (PRO(f_R(3, 1, \bar{x})))$
$x \leq 2 \quad \bar{x} \leq x$

$si(PRO(f_R(3, 1, \overline{x}))) + si(PRO(f_R(3, 1, \overline{x}))) + si(PRO(f_R(3, 1, \overline{x})))$

$\underbrace{\overline{x} \leq 0}_{I} \qquad \underbrace{\overline{x} \leq 1}_{II} \qquad \underbrace{\overline{x} \leq 2}_{III}$

I. si $[\underbrace{f_R(3, 1, 0)}_{1}]$, et si(1) = 1

II. si $[\underbrace{f_R(3, 1, 0)}_{1} . \underbrace{f_R(3, 1, 1)}_{1}]$, et si(1) = 1

$1.1 = 1$

III. si $[\underbrace{f_R(3, 1, 0)}_{1} . \underbrace{f_R(3, 1, 1)}_{1} . \underbrace{f_R(3, 1, 2)}_{0}]$, et si(0) = 0

$1 \ . \ 1 \ . \ 0 = 0$

MB(3, 1) = si(1) + si(1) + si(0)
= 1 + 1 + 0
= 2

2 est bien la plus petite valeur de x, $x \leq 3$ tel que 3+1 = 2.x.

Questions :

146. Décrire à l'aide d'une fonction de type MB, la fonction $PER(x_1)$ qui calcule la partie entière de la racine carrée de x_1.

Ex. PER(1) = 1
PER(2) = 1
PER(3) = 1
PER(4) = 2
PER(5) = 2
⋮

Suggestion: Utiliser l'information suivante: $R(x_1, x)$: $x_1 < (x+1)^2$

147. Décrire à l'aide d'une fonction de type MB, la fonction $PEF(x_1, x_2)$ qui calcule la partie entière de la fraction x_1/x_2

Ex. PEF(1, 1) = 1
PEF(2, 1) = 2
PEF(1, 2) = 0
PEF(7, 3) = 2
⋮

Suggestion: Utiliser l'information suivante:

$$R(x_1, x_2, x): (x_1<x_2.(x+1))\vee(x_2 = 0))$$

Pour clore cette partie relative aux fonctions et relations récursives primitives, nous proposons deux exemples. Ils concernent la propriété "être un nombre premier". Le rôle central que joue cette propriété dans la numérotation de Gödel et dans l'arithmétisation de la syntaxe a motivé notre choix.

1] La propriété ETRE UN NOMBRE PREMIER [NP] est une RPR.

Analyse naïve: Si x est un nombre premier, x est différent de 0 et de 1, et quels que soient les nombres x_1 et x_2, $x_1 \leq x$, $x_2 \leq x$, on ne peut avoir à la fois

$x = x_1.x_2$ et

il n'est pas le cas que $[(x_1 = 1)$ ou $(x_2 = 1)]$

De manière plus formelle, les conditions attachées à cette propriété peuvent être représentées de la manière suivante:

$$NP(x): (\forall x_1)_{x_1\leq x}(\forall x_2)_{x_2\leq x}[(\sim(x=1)\wedge\sim(x=0))\wedge\sim(x=x_1.x_2\wedge\sim((x_1=1)\vee(x_2=1)))]$$

La quantification bornée, les relations et opérations qui apparaissent dans cette expression ont toutes été définies précédemment comme primitives récursives. La relation NP(x) est donc une RPR et nous poserons f_{NP} sa FRP associée.

2] La fonction $f_p(x)$ qui calcule le x+1 ème nombre premier est une FRP.

Analyse naïve:

Cette fonction, pour la valeur x = 0, doit avoir la valeur 2. De plus, quel que soit a, la valeur $f_p(a+1)$ doit posséder la propriété suivante:

a] être un nombre premier

b] être plus grand que $f_p(a)$

c] être le plus petit nombre premier plus grand que $f_p(a)$

La condition a] est associée à la FRP $f_{NP}(x)$

La condition b] est associée à la FRP $f_>(x_1, x_2)$

Quant à la condition c], elle exige une borne supérieure afin de pouvoir disposer de la fonction de minimalisation bornée. Connaissant que, pour tout nombre premier n, l'addition d'une unité au produit de celui-ci avec tous ses prédécesseurs, est un nombre premier plus grand que le nombre premier n, nous choisirons ce résultat comme borne supérieure. Nous pouvons représenter cette borne supérieure comme suit:

$$[PRO(f_p(q))+1]$$
$$q\leq a$$

Nous pouvons dès lors inscrire la fonction $f_p(x)$:

$$f_p(x) : \begin{cases} f_p(0) = 2 \\ f_p(a+1) = \text{le plus petit } n,\ n<[PRO(f_p(q))]+1 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad q\leq a \\ \qquad\qquad \text{tel que: } n \text{ est un nombre premier} \qquad \text{et} \\ \qquad\qquad\qquad\quad n \text{ est plus grand que } f_p(a) \end{cases}$$

L'inscription formelle en est la suivante:

$$f_p(x) : \begin{cases} f_p(0) = S(S(Z(0))) \\ f_p(a+1) = m[n<[PRO(f_p(q))]+1](f_R(f_p(a), n)) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad q\leq a \end{cases}$$

avec $f_R(x_1, x_2)$, la fonction caractéristique associée à la relation *x_2 est un nombre premier et x_2 est plus grand que x_1*: $NB(x_2)\wedge(x_2>x_1)$

Il est temps de conclure cette partie qui concerne les fonctions récursives primitives. Nous le ferons en proposant une définition et en inscrivant quelques remarques.

DEFINITION 40 -fonctions récursives primitives- Toute fonction définie par les clauses 1-3, les clauses inductives 4-5 et les règles dérivées 1-9 est une fonction récursive primitive, et rien d'autre n'est une telle fonction, sinon par ce qui précède.

R e m a r q u e s.

Les relations sont des sous-ensembles de l'ensemble produit $\underbrace{Nx...xN}_{n \text{ fois}}$ pour un n approprié.

Lorsque nous agissons avec des relations et des opérations logiques qui s'y appliquent, il est nécessaire de vérifier que l'on dispose bien d'un nombre correct d'arguments. Si R est une relation n-aire, $R\subseteq\underbrace{Nx...xN}_{n \text{ fois}}$

Dans les pages précédentes, nous avons mis en évidence une démarche de la pensée qui avait pour objectif de cerner de manière systématique et constructive le domaine des fonctions calculables. Peut-on admettre maintenant que l'ensemble des FRP coïncide avec celui des fonctions calculables?

Le raisonnement suivant répond par la négative.

La numérotation de Gödel rend possible d'ordonner l'ensemble des FRP d'une seule variable.
Soit $f_1(x)$, $f_2(x)$,..., $f_n(x)$,... la suite ordonnée de ces FRP
Soit g(x), la fonction ainsi définie:
$g: N \longrightarrow N$, $g(x) = S(f_x(x))$ $[f_x(x)+1]$

Bien que calculable, la fonction g n'est pas récursive primitive. Pour le montrer, imaginons l'hypothèse suivante: g(x) est une FRP.

Cette fonction est une fonction d'une variable. Sous l'hypothèse absurde qu'elle est une FRP, elle est donc dans la liste ordonnée des fonctions ne possédant qu'une variable. Elle est pour un indice k particulier $f_k(x)$. Et par définition de g(x), $f_k(x) = S(f_x(x))$, quelle que soit la valeur de la variable x.
Mais pour x = k, nous obtenons un résultat contradictoire. En effet :

$f_k(k) = S(f_k(k))$ $[f_k(k) = f_k(k)+1]$

La valeur de $f_k(k)$ serait égale à son successeur.
Bien que calculable, la fonction g(x) n'est pas une fonction récursive primitive .

Il est donc nécessaire d'élargir l'ensemble des FRP à un ensemble plus large: l'ensemble des fonctions récursives générales [FRG].

4. LES FONCTIONS RECURSIVES GENERALES

Il existe donc des fonctions calculables de manière effective qui ne sont pas des FRP. Il est cependant possible d'étendre la classe des FRP à une classe plus large: la classe des fonctions récursives générales, FRG. Pour réaliser cette expansion, il est nécessaire d'ajouter aux clauses inductives, une opération nouvelle; cette dernière consiste dans une généralisation de l'opération de minimalisation bornée.

Abordons cette nouvelle opération par le biais d'un exemple:
soit la relation R,
$R(x, z)$: $(z+1)^2 > x$

Pour tout x, $x \in N$, il existe des z différents, $z \in N$, qui valident cette relation. Intéressons-nous plus particulièrement au plus petit z [μz], qui pour chaque x, valide cette relation:

x :	1	2	3	4	5	6	7	8	9	10	...
μz :	1	1	1	2	2	2	2	2	3	3	

La relation R(x,z) est récursive; soit f_R sa fonction récursive associée: $f_R(x, z)$.

Dire d'une relation qu'elle est validée par deux valeurs particulières x et z, c'est reconnaître que sa fonction récursive associée est, pour ces deux valeurs, égale à zéro :

$$f_R(x, z) = 0$$

Par rapport à cet exemple particulier, l'opération de minimalisation généralisée introduit la fonction g(x) suivante comme une fonction récursive:

$$g(x) = \mu z\ (f_R(x, z) = 0)$$

Remarques .

La fonction g(x) calcule, quel que soit x, le plus petit z, s'il existe, tel que $f_R(x, z) = 0$

Aucune limite supérieure n'est associée à z.

De manière plus explicite, la fonction g(x) calcule la partie entière de la racine carrée de x.

Une condition fondamentale est associée à cette nouvelle opération: quel que soit x, il existe au moins un z tel que $(z+1)^2 > x$. Cette condition est essentielle pour garantir la nature d'"effectivité" de la fonction.

D'une manière plus générale, si h(x, z) est une fonction récursive, et si $(\forall x)(\exists z)(h(x, z) = 0)$, alors
$g(x) = \mu z(h(x, z) = 0)$ est une fonction récursive.

Cette opération de minimalisation a permis de définir, à partir d'une fonction récursive à deux variables, une fonction récursive d'une seule variable.

Proposons maintenant une définition plus générale de cette opération et ajoutons-la aux clauses inductives déjà exposées.

Clause inductive

6) L'opération de MINIMALISATION GENERALISEE [MG]
Soit $f(x_1,..., x_n, x)$ une fonction récursive à n+1 variables telle que pour tout n-uple de valeurs $<x_1,..., x_n>$, il existe x tel que $f(x_1,..., x_n, x) = 0$. Il s'agit de la condition d'"effectivité":

$$[(\forall x_1)(\forall x_2)...(\forall x_n)(\exists x)(f(x_1,..., x_n, x) = 0)]$$

S'il existe plusieurs x de cette sorte, appelons μx le plus petit d'entre eux. Alors, la fonction $g(x_1,\ldots, x_n) = \mu x(f(x_1,\ldots, x_n, x) = 0)$ est une fonction récursive définie par l'opération MG.

R e m a r q u e s.

Lorsqu'on utilise l'opération MG, il est indispensable de s'assurer que la condition d'"effectivité" est satisfaite. Nous ne disposons malheureusement pas d'un algorithme décidable permettant de déterminer dans tous les cas si cette condition est satisfaite.

L'opération MG permet de définir à partir d'une fonction récursive à n+1 variables, une fonction récursive de n variables.

Nous nous intéressons à des fonctions définies sur les nombres entiers [NxNx...xN $\rightarrow$ N]. Si le domaine de définition d'une fonction est la totalité du produit cartésien Nx...xN, on parle alors de *fonction totale*. Si son domaine de définition est un sous-ensemble au sens strict du produit cartésien, on l'appelle une *fonction partielle*.

$h(x) = x^2$ est une fonction totale.

$g(x) = \mu z(z^2-x = 0)$ est une fonction partielle.

L'opération de minimalisation associe à chaque fonction totale h(x, z), une fonction partielle g(x).

Q u e s t i o n s :

148. La relation $R(x_1, x_2, x)$ suivante entre-t-elle dans le champ de la condition d'"effectivité"?
$R(x_1, x_2, x) : (x+1).x_2 > x_1$

149. Soit $f(x_1, x_2, x) =_{df} (x_1+x_2)\div x$
calculer la valeur de $g(x_1, x_2) = \mu x(f(x_1, x_2, x) = 0)$

pour x_1	0	0	0	1	1	1	2	2	2	3	3	3
x_2	0	1	2	0	1	2	0	1	2	0	1	2

A l'aide de cette nouvelle opération de minimalisation, il est dès lors possible de définir l'ensemble des fonctions récursives générales.

DEFINITION 41 -fonctions récursives générales- Toute fonction définie par les clauses initiales 1-3 [pp. 95-96], par les clauses inductives 4-5 [pp. 96 et 98] et par la clause inductive 6 est une fonction récursive générale, et rien d'autre n'est une telle fonction, sinon par ce qui précède.

L'ensemble des fonctions récursives générales est de plus grande extension que celui des fonctions primitives. Ce nouvel ensemble réunit-il toutes les fonctions calculables?

> Il est impossible,..., de justifier par une démonstration véritable la réponse affirmative qui semble s'imposer, et on est réduit à présenter une pluralité d'arguments convergents. [Martin 1964: 141-142]

Cette pluralité d'arguments consiste essentiellement en la thèse généralisée de Church.

A travers ces quelques pages, nous nous sommes efforcé de donner de la notion de fonction récursive une idée aussi claire et opératoire que possible. Il est cependant nécessaire d'ajouter que la théorie des fonctions récursives est bien plus complexe et plus riche que ce que nous avons exposé. Le lecteur curieux trouvera dans les ouvrages suivants des exposés plus complets de cette théorie [Boolos 1985; Dalen 1983; Grzegorczyk 1974; Kleene 1971; Martin: 1964; Monk 1976].

5. 'REPRESENTABILITE' ET 'DEFINISSABILITE' DES FONCTIONS RECURSIVES

En définissant la notion de système arithmétique minimal, nous avons précisé cinq conditions fondamentales qu'on est en droit d'exiger d'une formalisation de l'arithmétique. L'une des conditions à satisfaire nous concerne plus particulièrement ici. Il s'agit de celle qui exige que, *si E est un ensemble décidable de nombres naturels, E est représentable dans le système* S^a. Dans ce contexte, rappelons deux définitions.

> Soit E un ensemble de nombres naturels. On dit que E est *représentable* en S^a s'il existe une ebf de S^a, de la forme A(v) et telle que, quel que soit n, $n \in E$,
>
> $n \in E$ ssi $\vdash_{S^a} A(\underline{n})$ [Déf. 37]
>
> Soit A(v), une ebf de S^a qui contient la variable libre v. On appelle *fonction caractéristique* de A(v), la fonction f(n) définie comme suit:
>
> $f(n) = 0$ ssi $\vdash_{S^a} A(\underline{n})$ [Déf. 36]

La propriété de décidabilité d'un ensemble de nombres naturels est associée à la notion de fonction, et plus précisément à celle de fonction effectivement calculable. A cet égard, nous disposons d'un outil efficace: l'ensemble des fonctions récursives. Nous l'utiliserons en posant ce qui suit: un ensemble E de nombres naturels est récursif si et seulement si il existe une fonction récursive f telle que pour chaque n, $n \in E$ ssi $f(n) = 0$.

Par ce biais, nous disposons d'un procédé effectif permettant de déterminer si, pour un nombre n donné, celui-ci appartient ou non à l'ensemble E. De cette manière, tout ensemble récursif est décidable. Dès lors, pour construire un ensemble décidable, on passera par une fonction récursive. Il suffira donc que toute fonction récursive soit représentable dans S^a pour que l'ensemble E le soit également. Seulement, la définition de 'représentable' qui suffisait avant d'avoir construit le système S^a n'est plus assez forte. D'une part nous avons maintenant affaire à des fonctions de plus d'une variable. Ensuite, poser $n \in E$ ssi $f(n) = 0$ ssi $\vdash_{Sa} A(\underline{n})$ permet bien d'inférer que si $n \in E$, alors $\vdash_{Sa} A(\underline{n})$, mais comme S^a n'est pas catégorique, on ne sait pas si $n \notin E$ conduit à $\vdash_{Sa} \sim A(\underline{n})$. Enfin, nous avons jusqu'alors volontairement ignoré le problème de l'unicité de la valeur d'une fonction. Tout ceci nous engage à faire appel à une notion plus forte que celle de 'représentabilité': la notion de 'définissabilité'.

DEFINITION 42 - Une fonction f à k éléments est *définissable* dans un système formel S s'il existe une ebf $A(v_1, \ldots, v_k, v_{k+1})$ telle que pour tout n-uple de nombres $< n_1, \ldots, n_k >$ on ait

-Définissabilité-

1) $f(n_1, \ldots, n_k) = n_{k+1} \Rightarrow \vdash_S A(\underline{n}_1, \ldots, \underline{n}_k, \underline{n}_{k+1})$

2) $f(n_1, \ldots, n_k) \neq n_{k+1} \Rightarrow \vdash_S \sim A(\underline{n}_1, \ldots, \underline{n}_k, \underline{n}_{k+1})$

3) $\vdash_S (\forall v_1) \ldots (\forall v_k)(\forall v_{k+1})[A(v_1, \ldots, v_k, v_{k+1}) \supset (A(v_1, \ldots, v_k, v_{k+2}) \supset (v_{k+1} = v_{k+2}))]$

clause d'unicité

Il s'agit de montrer maintenant que toute fonction récursive est définissable dans S^a.

METATHEOREME 37 - Toute fonction récursive est définissable dans S^a.

La démonstration consiste à montrer que chacune des fonctions initiales est définissable, et que les trois opérations de substitution, de récurrence et de minimalisation généralisée conservent cette propriété. Dorénavant, pour simplifier la lecture nous ne distinguerons plus graphiquement les signes de S^a et ceux de l'arithmétique, hormis les numéraux.

METATHEOREME 37.1 - La fonction ZERO est définissable dans S^a.

Il faut prouver qu'il existe une ebf $A(v_1, v_2)$ telle que

1) pour tout m, si z(m) = 0 alors $\vdash_{Sa} A(\underline{m}, \underline{0})$

2) pour tout m, si z(m) ≠ 0 alors $\vdash_{Sa} \sim A(\underline{m}, \underline{0})$

3) $\vdash_{Sa}(\forall v_1)(\forall v_2)(\forall v_3)[A(v_1, v_2) \supset (A(v_1, v_3) \supset (v_2 = v_3))]$

Démonstrations

Définition de l'ebf A:

$$A(v_1, v_2) =_{df} (v_1 = v_1) \wedge (v_2 = 0)$$

Pour tout nombre m, la fonction z prend valeur, soit n celle-ci: z(m) = n.
Dans le contexte de nombres n et m, A s'écrit ainsi :

$$A(\underline{m}, \underline{n}) = (\underline{m} = \underline{m}) \wedge (\underline{n} = \underline{0})$$

1) si n = 0, c'est-à-dire quand z(m) = 0, il faut prouver que:

$$\vdash_{Sa}(\underline{m} = \underline{m}) \wedge (\underline{0} = \underline{0})$$

1	$\underline{m} = \underline{m}$	=i
2	$\underline{0} = \underline{0}$	=i
3	$(\underline{m} = \underline{m}) \wedge (\underline{0} = \underline{0})$	1, 2, ∧ i

2) si n≠ 0, c'est-à-dire quand z(m) ≠ 0, il faut prouver que:

$$\vdash_{Sa} \sim[(\underline{m} = \underline{m}) \wedge (\underline{n} = \underline{0})]$$

1	$(\underline{m} = \underline{m}) \wedge (\underline{n} = \underline{0})$	hyp.
2	$\underline{n} = \underline{0}$	1, ∧e
3	$\sim(\underline{n} = \underline{0})$	n ≠ 0, Mth. 34.3
4	$\sim[(\underline{m} = \underline{m}) \wedge (\underline{n} = \underline{0})]$	1, 2, 3, ~i

3) Il faut encore prouver la troisième condition.

$$\vdash_{Sa} (\forall v_1)(\forall v_2)(\forall v_3)[((v_1 = v_1) \wedge (v_2 = \underline{0})) \supset (((v_1 = v_1) \wedge (v_3 = \underline{0})) \supset (v_2 = v_3))]$$

1	$(v_1 = v_1) \wedge (v_2 = \underline{0})$	hyp.
2	$(v_1 = v_1) \wedge (v_3 = \underline{0})$	hyp.
3	$(v_1 = v_1) \wedge (v_2 = \underline{0})$	1, reit.
4	$v_2 = \underline{0}$	3, ∧e
5	$v_3 = \underline{0}$	2, ∧e
6	$v_2 = v_3$	4, 5, =e
7	$((v_1 = v_1) \wedge (v_3 = \underline{0})) \supset (v_2 = v_3)$	2-6, ⊃ i
8	$((v_1 = v_1) \wedge (v_2 = \underline{0})) \supset (((v_1 = v_1) \wedge (v_3 = \underline{0})) \supset (v_2 = v_3))$	1-7, ⊃i
9	$(\forall v_1)(\forall v_2)(\forall v_3)[\text{----}]$	8, 3xGEN

METATHEOREME 37.2 - La fonction SUCCESSEUR est définissable dans S^a.
Il faut montrer qu'il existe une ebf $A(v_1, v_2)$ telle que:

1) pour tout m, si S(m) = m+1, donc si n = m+1
$\vdash_{Sa} A(\underline{m}, \underline{n})$

2) pour tout m, si S(m) ≠ m+1, donc si n ≠ m+1
$\vdash_{Sa} \sim A(\underline{m}, \underline{n})$

3) $\vdash_{Sa} (\forall v_1)(\forall v_2)(\forall v_3)[(v_1^* = v_2) \supset ((v_1^* = v_3) \supset (v_2 = v_3))]$

Démonstrations

Définition de l'ebf A:

$A(v_1, v_2) =_{df} v_1^* = v_2$

$A(\underline{m}, \underline{n}) = \underline{m}^* = \underline{n}$

1) Si n = m+1, c'est-à-dire quand S(m) = n+1, il faut prouver que:
$\vdash_{Sa} (\underline{m}^* = \underline{n})$

1	$\underline{n} = \underline{m+1}$	n = m+1, Mth. 34.2
2	$\underline{m+1} = \underline{m}^*$	Mth. 34.1
3	$\underline{m}^* = n$	1, 2, =e

2) Si n ≠ m+1, c'est-à-dire quand S(m) ≠ m+1, il faut prouver que:
$\vdash_{Sa} \sim(\underline{m}^* = \underline{n})$

1	$\sim(\underline{m+1} = \underline{n})$	m+1 ≠ n , Mth. 34.3
2	$\underline{m}^* = \underline{m+1}$	Mth. 34.1
3	$\sim(\underline{m}^* = \underline{n})$	2, 1, règle rem

3) Troisième condition
$\vdash_{Sa} (\forall v_1)(\forall v_2)(\forall v_3)[(v_1^* = v_2) \supset ((v_1^* = v_3) \supset (v_2 = v_3))]$

1	$\vdash v_1^* = v_2$	hyp.
2	$\quad \vdash v_1^* = v_3$	hyp.
3	$\quad v_1^* = v_2$	1, reit.
4	$\quad v_2 = v_3$	2, 3, =e
5	$(v_1^* = v_3) \supset (v_2 = v_3)$	2-4, ⊃ i
6	$(v_1^* = v_2) \supset ((v_1^* = v_3) \supset (v_2 = v_3))$	1-5, ⊃ i
7	$(\forall v_1)(\forall v_2)(\forall v_3)[\text{----}]$	6, 3xGEN

METATHEOREME 37.3 La fonction PROJECTION est définissable dans S^a.
Définition de l'ebf A:

$A(v_1,\ldots, v_k, v_{k+1}) =df (v_1 = v_1)\wedge \ldots\wedge (v_k = v_k)\wedge(v_{k+1} = v_i)$

Pour des nombres $n_1,\ldots, n_k$ donnés, la fonction P_i^k prend une valeur, soit n celle-ci:

$$P_i^k (n_1,\ldots, n_k) = n$$

Il faut montrer que :

1) Si $P_i^k(n_1,\ldots, n_k) = n_i$, donc si $n = n_i$
$\vdash_{Sa} A(\underline{n}_1,\ldots, \underline{n}_k, \underline{n})$

2) Si $P_i^k (n_1,\ldots, n_k) \neq n_i$, donc si $n \neq n_i$
$\vdash_{Sa} \sim A(\underline{n}_1,\ldots, \underline{n}_k, \underline{n})$

3) $\vdash_{Sa}(\forall v_1)\ldots(\forall v_k)(\forall v_{k+1})(\forall v_{k+2})[A(v_1,\ldots, v_k, v_{k+1})\supset((A(v_1,\ldots, v_k, v_{k+2})\supset (v_{k+1} = v_{k+2}))]$

Q u e s t i o n

150. Démontrer que la fonction PROJECTION est définissable dans S^a.

Les preuves de la conservation de la propriété de 'définissabilité' dans S^a pour les opérations de substitution, de récurrence et de minimalisation généralisée sont longues. Nous nous contenterons d'illustrer ou d'esquisser le procédé démonstratif de certaines d'entre elles. Des développements plus complets peuvent être trouvés notamment dans Mendelson [1979], Kleene [1980].

METATHEOREME 37.4 - L'opération de SUBSTITUTION conserve dans S^a la propriété de 'définissabilité'.

Nous caricaturerons la démonstration en ne considérant que deux fonctions à un seul argument: f(x) et h(x). Cette manière de procéder conserve l'esprit de la démonstration et a l'avantage d'en simplifier la forme.

Il s'agit donc de montrer que si f(x) et h(x) sont deux fonctions récursives définissables, alors g(x) = f(h(x)) est une fonction récursive définissable.

Affirmer que f est une fonction récursive définissable c'est admettre qu'il existe une ebf $A(v_1, v_2)$ telle que pour tout nombre n_1

* si $f(n_1) = n_2$ alors $\vdash_{Sa} A(\underline{n}_1, \underline{n}_2)$

** si $f(n_1) \neq n_2$ alors $\vdash_{Sa} \sim A(\underline{n}_1, \underline{n}_2)$

*** si $(\forall v_1)(\forall v_2)(\forall v_3)[A(v_1, v_2) \supset (A(v_1, v_3) \supset (v_2 = v_3))]$

Affirmer que h est une fonction récursive définissable, c'est admettre qu'il existe une ebf $B(v_1, v_2)$ telle que pour tout nombre n_1:

□ si $h(n_1) = n_2$ alors $\vdash_{Sa} B(\underline{n}_1, \underline{n}_2)$

□□ si $h(n_1) \neq n_2$ alors $\vdash_{Sa} \sim B(\underline{n}_1, \underline{n}_2)$

□□□ $(\forall v_1)(\forall v_2)(\forall v_3)[B(v_1, v_2) \supset (B(v_1, v_3) \supset (v_2 = v_3))]$

Sur la base de ces données, il faut montrer que l'on sait construire une ebf $C(v_1, v_2)$ telle que pour tout nombre n_1 :

\+ Si $g(n_1) = n_2$ alors $\vdash_{Sa} C(\underline{n}_1, \underline{n}_2)$

\++ Si $g(n_1) \neq n_2$ alors $\vdash_{Sa} \sim C(\underline{n}_1, \underline{n}_2)$

} avec, dans le contexte de l'opération de substitution: $n_2 = f(h(n_1))$, c'est-à-dire $g(n_1) = f(h(n_1))$

\+++ $(\forall v_1)(\forall v_2)(\forall v_3)\ [C(v_1, v_2) \supset (C(v_1, v_3) \supset (v_2 = v_3))]$

Avant de poursuivre cette démarche établissons un lemme.

LEMME I - Si j est une fonction à un argument et s'il existe une ebf $D(v_1, v_2)$ qui satisfasse aux conditions :

. $\vdash_{Sa} (\forall v_1)(\forall v_2)(\forall v_3)[D(v_1, v_2) \supset (D(v_1, v_2) \supset (v_2 = v_3))]$

.. $\vdash_{Sa} D(\underline{n}_1, \underline{j(n_1)})$ quel que soit le nombre n_1

alors $D(v_1, v_2)$ satisfait aux deux premières conditions de la 'définissabilité', c'est-à-dire :

≠ Si $j(n_1) = n_2$ alors $\vdash D(\underline{n}_1, \underline{n}_2)$

≠≠ si $j(n_1) \neq n_2$ alors $\vdash \sim D(\underline{n}_1, \underline{n}_2)$

Démonstration

Supposons les deux conditions .) et ..) réalisées; il en résulte que:

1) Si $j(n_1) = n_2$ alors $\vdash_{Sa} \underline{j(n_1)} = \underline{n}_2$ Mth. 34.2

Opérons dans ..) la substitution suivante: $\underline{j(n_1)} / \underline{n}_2$

On obtient alors ≠ : si $j(n_1) = n_2$ alors $\vdash_{Sa} D(\underline{n}_1, \underline{n}_2)$

2) Si $j(n_1) \neq n_2$ alors $\vdash_{Sa} \sim(\underline{j(n_1)} = \underline{n_2})$ Mth. 34.2 *

Opérons dans .) la substitution suivante:

$v_1 / \underline{n_1}$, $v_2 / \underline{j(n_1)}$, $v_3 / \underline{n_2}$, en éliminant les quantificateurs:

1	$(\forall v_1)(\forall v_2)(\forall v_3)[D(v_1, v_2) \supset (D(v_1, v_3) \supset (v_2 = v_3))]$	.
2	$D(\underline{n_1}, \underline{j(n_1)}) \supset (D(\underline{n_1}, \underline{n_2}) \supset (\underline{j(n_1)} = \underline{n_2}))$	1, sub, ∀e
3	$D(\underline{n_1}, \underline{j(n_1)})$	..
4	$D(\underline{n_1}, \underline{n_2}) \supset (\underline{j(n_1)} = \underline{n_2}))$	3, 2, ⊃ e
5	$\sim(\underline{j(n_1)} = \underline{n_2}) \supset \sim D(\underline{n_1}, \underline{n_2})$	4, contrap.
6	$\sim(\underline{j(n_1)} = \underline{n_2})$	*
7	$\sim D(\underline{n_1}, \underline{n_2})$	6, 5, ⊃ e

On obtient bien ≠# : si $j(n_1) \neq n_2$ alors $\vdash_{Sa} \sim D(\underline{n_1}, \underline{n_2})$.

Avant d'entreprendre la preuve du Mth. 37.4, il est utile de transformer la règle d'élimination d'un quantificateur existentiel pour obtenir la règle dite *règle de choix*, C. Celle-ci permet de présenter une démonstration plus élégante. La règle d'élimination du quantificateur ∃ a la forme suivante:

$(\exists v)A(v)$ v | $\underline{A(v)}$ | : | B B	Avec l'interdiction de réitérer une ebf qui contient v libre et à condition que B ne contienne pas v libre.

Si on élargit le système S en un système S^+ en ajoutant de nouvelles constantes d'objets $\{a_1, a_2, \ldots, a_n, \ldots\}$ et si a est l'une de ces constantes, on peut utiliser la règle de transformation suivante:

Règle C : Si $\Gamma \vdash_S (\exists v)A(v)$ et si $\Gamma, A(a) \vdash_{S^+} B$ alors $\Gamma \vdash_S B$, à condition que B ne contienne pas a [Rosser 1953: 128].

Prouvons maintenant que si f(x) est définissable par $A(w_1, w_2)$, et h(x) par $B(u_1, u_2)$, alors g(x) = f(h(x)) est définissable par l'ebf $C(v_1, v_2)$: $C(v_1, v_2) =_{df} (\exists v_k)(B(v_1, v_k) \wedge A(v_k, v_2))$.

Dans le contexte de l'opération de substitution, les fonctions h et f s'articulent ainsi: f(h(x))

posons ce qui suit :

$$h(n_1) = i \quad \text{et} \quad f(i) = n_2$$

on a alors

$$f(h(n_1)) = n_2$$

et $g(n_1)$ est $f(h(n_1))$

Prouvons tout d'abord la condition ..), c'est-à-dire, $C(\underline{n_1}, \underline{g(n_1)})$ qui, par la définition précédente est :

$(\exists v_k)(B(\underline{n_1}, v_k) \wedge A(v_k, \underline{g(n_1)})$ ou écrit en fonction de f et h :

$(\exists v_k)(B(\underline{n_1}, v_k) \wedge A(v_k, \underline{f(h(n_1))}))$

1	$B(\underline{n_1}, \underline{i})$	h est définissable, $h(n_1) = i$ □
2	$\underline{h(n_1)} = \underline{i}$	$h(n_1) = i$, Mth. 34.2
3	$A(\underline{i}, \underline{n_2})$	f est définissable, $f(i) = n_2$ *
4	$\underline{f(i)} = \underline{n_2}$	$f(i) = n_2$, Mth. 34.2
5	$A(\underline{i}, \underline{f(i)})$	3, 4, rem
6	$A(\underline{i}, \underline{f(h(n_1))})$	2, 5, rem
7	$B(\underline{n_1}, \underline{i}) \wedge A(\underline{i}, \underline{f(h(n_1))})$	1, 4, $\wedge$i
8	$(\exists v_k)(B(\underline{n_1}, v_k) \wedge A(v_k, \underline{f(h(n_1))}))$	7, $\exists$i, i / v_k
9	$(\exists v_k)(B(\underline{n_1}, v_k) \wedge A(v_k, \underline{g(n_1)}))$	8, $\underline{f(h(n_1))}$ est $\underline{g(n_1)}$
10	$C(\underline{n_1}, \underline{g(n_1)})$	9, déf. de C.

En prouvant de plus la clause d'unicité, c'est-à-dire :

.) $\vdash_{Sa} (\forall v_1)(\forall v_2)(\forall v_3)[((v_1, v_2) \supset (C(v_1, v_3) \supset (v_2 = v_3))]$

on aura ainsi démontré toutes les conditions que g(x) doit remplir pour être définissable.

Preuve de la clause d'unicité

Par définition de l'ebf C, cette clause s'écrit ainsi:

$$\vdash_{Sa} (\forall v_1)(\forall v_2)(\forall v_3)[(\exists v_k)(B(v_1, v_k) \wedge A(v_k, v_2)) \supset ((\exists v_k)(B(v_1, v_k) \wedge A(v_k, v_3)) \supset (v_2 = v_3))]$$

Posons les abréviations suivantes:

$P =_{df} (\forall v_1)(\forall v_2)(\forall v_3)(A(v_1, v_2) \supset (A(v_1, v_3) \supset (v_2 = v_3)))$

$Q =_{df} (\forall v_1)(\forall v_2)(\forall v_3)(B(v_1, v_2) \supset (B(v_1, v_3) \supset (v_2 = v_3)))$

$M(v_k)$ =df $B(v_1, v_k) \wedge A(v_K, v_2)$

$N(v_k)$ =df $B(v_1, v_k) \wedge A(v_k, v_3)$

Sur la base de ces abréviations, il faut donc prouver:

$$\vdash_{Sa} (\forall v_1)(\forall v_2)(\forall v_3)[(\exists v_k)M(v_k) \supset ((\exists v_k)N(v_k) \supset (v_2 = v_3))]$$

Pour ce faire, utilisons un nouveau lemme.

LEMME II - Soit $S^{a+} = S^a + \{a_1, a_2, \ldots, a_n, \ldots\}$

Soit $S^{a++} = S^{a+} + \{b_1, b_2, \ldots, b_n, \ldots\}$

Alors, si a est un a_i quelconque et b un b_i quelconque,

$M(a), (\exists v_k)N(v_k), N(b) \vdash_{Sa++} v_2 = v_3$

Démonstration du lemme

1	$B(v_1, a) \wedge A(a, v_2)$	$M(a)$
2	$(\exists v_k)[B(v_1, v_k) \wedge A(v_k, v_3)]$	$(\exists v_k)N(v_k)$ prémisses
3	$B(v_1, b) \wedge A(b, v_3)$	$N(b)$
4	v_k | $B(v_1, v_k) \wedge A(v_k, v_3)$	Hyp. $\exists e$
5	$B(v_1, a)$	1, reit, $\wedge e$
6	$A(a, v_2)$	
7	$B(v_1, b)$	3, reit, $\wedge e$
8	$A(b, v_3)$	
9	$B(v_1, a) \supset (B(v_1, b) \supset (a = b))$	Q, $\forall e$, v_2/a, v_3/b
10	$B(v_1, b) \supset (a = b)$	9, 5, $\supset e$
11	$a = b$	10, 7, $\supset e$
12	$A(b, v_2)$	6, 11, rem
13	$A(b, v_2) \supset (A(b, v_3) \supset (v_2 = v_3))$	P, $\forall e$, v_1/b
14	$A(b, v_3) \supset (v_2 = v_3)$	13, 12, $\supset e$
15	$v_2 = v_3$	8, 14, $\supset e$
16	$v_2 = v_3$	2, 4-15, $\exists e$

Nous avons ainsi montré que:

1. $M(a), (\exists v_k)N(v_k), N(b) \vdash_{Sa++} v_2 = v_3$ Lemme II

De plus:

2. $M(a), (\exists v_k)N(v_k), \vdash_{Sa+} (\exists v_k)N(v_k)$ — Mth.: B, A ⊢A

3. $\underbrace{M(a), (\exists v_k)N(v_k)}_{\Gamma_1} \vdash_{Sa+} v_2 = v_3$ — 1, 2, règle C

4. $(\exists v_k)M(v_k), (\exists v_k)N(v_k), M(a) \vdash_{Sa+} v_2 = v_3$ — 3, Mth. 1.1

5. $(\exists v_k)M(v_k), (\exists v_k)N(v_k) \vdash_{Sa} (\exists v_k)M(v_k)$ — Mth.: A, B ⊢A

6. $\underbrace{(\exists v_k)M(v_k), (\exists v_k)N(v_k)}_{\Gamma_2} \vdash_{Sa} v_2 = v_3$ — 4, 5, Règle C

7. $(\exists v_k)M(v_k) \vdash_{Sa} (\exists v_k)N(v_k) \supset (v_2 = v_3)$ — 6, Mth. 3

8. $\vdash_{Sa} (\exists v_k)M(v_k) \supset ((\exists v_k)N(v_k) \supset (v_2 = v_3))$ — 7, Mth. 3

9. $\vdash_{Sa} (\forall v_1)(\forall v_2)(\forall v_3)$ [----] — 8, 3x GEN

Il s'agit de la clause d'unicité.

L'opération de SUBSTITUTION conserve la propriété de définissabilité. Bien que la démonstration ait été faite en ne considérant que des fonctions f et h à un seul argument, ce résultat reste valide pour un nombre quelconque d'arguments.

METATHEOREME 37.5 - L'opération de RECURRENCE conserve la propriété de définissabilité.

Si f, une fonction à k arguments, est définissable dans S^a par une ebf A à k+1 arguments et si h, une fonction à k+2 arguments, est définissable dans S^a par une ebf B à k+3 arguments, alors la fonction g, à k+1 arguments:

$$g(n_1,\ldots, n_k, n_{k+1}) : \begin{cases} g(n_1,\ldots, n_k, 0) = f(n_1,\ldots, n_k) \\ g(n_1,\ldots, n_k, a+1) = \\ \qquad h(n_1,\ldots, n_k, a, g(n_1,\ldots, n_k, a)) \end{cases}$$

est définissable, et il existe donc une ebf C à k+2 arguments qui lui est associée. Nous ne ferons que présenter l'ebf C.

Esquisse d'une construction de l'ebf C.

Présentons tout d'abord un résultat qui sera utile: la β-fonction de Gödel.

Soit $n_1,\ldots, n_k$, une succession de nombres naturels, il existe alors une fonction β et deux nombres naturels m et p tels que:

$\beta\ (m, p, i) = n_i$ avec $1 \leq i \leq n$.

La fonction β est récursive:
Soit la relation récursive R_1, $R_1(x, y, z) : (y = 0) \vee (y.(z+1) > x)$ et soit $f_{R_1}\ (x, y, z)$, la fonction récursive qui lui est associée; alors la fonction PED(x, y) est également récursive:

$$PED(x, y) = \mu z(f_{R_1}(x, y, z) = 0)$$

La fonction PED représente la partie entière de la division de x par y. Soit RD une nouvelle fonction récursive: $RD(x, y) = x \dot{-} (PED(x, y).y)$; elle représente le reste de la division de x par y. Sur la base de ce qui précède, la fonction β s'écrit ainsi:

$$\beta\ (x, y, z) = RD(1+S(z).y, x).$$

De plus, cette fonction β est définissable dans S^a. L'ebf G à quatre arguments qui lui est associée a la forme suivante:

$$G(x, y, z, w) =_{df} (\exists v)[(x = ((1+S(z).y).v+w)) \wedge (w < (1+(S(z).y))]$$

[Kleene 1980: § 41 et § 48].

Revenons, avec ce bagage, à l'ebf C qui est associée à la fonction g définie par l'opération de récurrence. Cette fonction $g(n_1,\ldots, n_k, n_{k+1})$ est définissable dans S^a par l'ebf $C(v_1,\ldots, v_k, v_{k+1}, v_{k+2})$ telle que:

si $g(n_1,\ldots, n_k, n_{k+1}) = n$ alors $\vdash_{S^a} C(\underline{n}_1,\ldots, \underline{n}_k, \underline{n}_{k+1}, \underline{n})$

si $g(n_1,\ldots, n_k, n_{k+1}) \neq n$ alors $\vdash_{S^a} \sim C(\underline{n}_1,\ldots, \underline{n}_k, \underline{n}_{k+1}, \underline{n})$

plus clause d'unicité.

Définition de l'ebf C

$C(v_1,\ldots, v_k, v_{k+1}, v_{k+2}) =_{df}$

$(\exists u)(\exists v)[(\exists w)(G(u, v, \underline{0}, w) \wedge A(v_1,\ldots, v_n, w) \wedge$

$G(u, v, v_{k+1}, v_{k+2}) \wedge$

$(\forall s)((s < v_{k+1}) \supset$

$(\exists y)(\exists z)(G(u, v, s, y) \wedge$

$G(u, v, S(s), z) \wedge$

$B(v_1,\ldots, v_n, s, y, z)))]$

avec l'ebf A, respectivement B, associée par définissabilité à la fonction f, respectivement h [Mendelson 1979: 149].

METATHEOREME 37.6 - L'opération de MINIMALISATION GENERALISEE conserve la propriété de définissabilité.

Soit f une fonction récursive telle que, quel que soit le k-uple $<n_1,\ldots, n_k>$, il existe un n tel que $f(n_1,\ldots, n_k, n) = 0$.
f est définissable dans S^a. Il existe donc une ebf A, à n+2 arguments qui lui est associée.

$$A(v_1,\ldots, v_k, v_{k+1}, v_{k+2})$$

Soit $g(n_1,\ldots, n_k)$, la fonction récursive définie par l'opération de minimalisation sur f

$$g(n_1,\ldots, n_k) = \mu n(f(n_1,\ldots, n_k, n) = 0).$$

Cette fonction g est définissable dans S^a par l'ebf C à k+1 arguments:

$$C(v_1,\ldots, v_k, v_{k+1}) =df A(v_1,\ldots, v_k, v_{k+1}, \underline{0}) \wedge (\forall v)((v < v_{k+1}) \supset \sim A(v_1,\ldots, v_k, v, \underline{0}))$$

[Mendelson 1979: 150].

Terminons cette partie qui concerne la définissabilité par une dernière question.

Q u e s t i o n :

151. Esquisser les grandes lignes d'une démonstration qui vérifierait que toute relation récursive est définissable dans S^a.

EPILOGUE

La théorie des systèmes formels est l'aboutissement d'une longue réflexion sur la nature du raisonnement hypothético-déductif et sur le problème des fondements des théories mathématiques et logiques. A cet égard, l'apport des logiciens et mathématiciens des XIXème et XXème siècles est déterminant. A travers notamment les travaux de Boole, Cantor, Frege, Russell, Hilbert, les théorèmes de limitation de Gödel, on observe une formalisation progressive de la pensée déductive. Cette mise en forme s'achève par la réalisation d'un édifice théorique particulièrement complexe et structuré, où langue et métalangue sont soigneusement séparées et où la syntaxe et la sémantique apparaissent comme deux domaines strictement différenciés bien que pensés l'un par rapport à l'autre.

Les deux premiers fascicules des *Travaux de Logique* du Centre de Recherches Sémiologiques ont pour objectif de présenter la théorie des systèmes formels, tout en mettant en évidence l'instrument d'analyse qu'elle offre, sa rigueur et sa précision. Mais cette contribution voudrait offrir davantage. A travers les propriétés métalogiques -notamment les théorèmes de Löwenheim et de Skolem, les résultats de Gödel, la thèse de Church- elle vise à susciter une réflexion sur les faits de limitation et l'esprit de construction qui sont associés à la théorie des systèmes formels. Elle voudrait mettre en évidence que la formalisation ne saurait se dispenser de la pensée naturelle. Ces deux fascicules aimeraient également exposer une connaissance qu'il est utile de dominer pour aborder d'autres manières de concevoir les langues formelles. Ils voudraient aussi être un argument pour justifier la nécessité et la légitimité d'une réflexion qui se prolonge dans le champ de la logique naturelle. D'autres monographies s'emploieront à développer davantage ces différents aspects.

Nous conclurons en citant un passage de l'ouvrage de D. Dubarle: *Initiation à la logique*. Bien qu'écrites en 1957, ces lignes restent aujourd'hui encore très actuelles. Leur intérêt excusera la relative longueur de la citation.

> Les formalismes logico-mathématiques que nous sommes capables de mettre sur pied sont du genre des herbiers. Ils nous font voir distinctement un état de la pensée mathématique. Ils ne nous montrent pas directement ces virtualités antérieures aux états mêmes, ces virtualités préscientifiques que la pensée mathématique vivante et en instance d'évolution emporte avec elle comme son plus précieux capital d'avenir. Leur fonction est précisément *de ne pas* les représenter, de les faire perdre au clair concept de la science afin de mieux faire sentir, comme par un choc en retour, l'originalité et le prix de ce qui est absent de ce clair concept. Que ce quelque chose existe comme une source indéfinie de renouvellement, ils l'at-

testent d'une façon indirecte. Les théorèmes critiques de Gödel, Church, Löwenheim-Skolem sont des théorèmes qui forcent à comprendre la non-autarchie de ces formalismes, l'impossibilité qu'ils ont de se clore de façon suffisante sur eux-mêmes. Les formalismes manifestent alors, pour ainsi dire, l'adhérence du résultat qu'ils sont à un indéfini qui n'est *pour eux* que néant et obscurité, mais d'où montera leur renouvellement essentiel. *Pour l'esprit du mathématicien* qui vit sa pensée, l'indéfini en question n'est en effet nullement néant et obscurité, mais faculté indéfinie et encore inexplorée des clartés ultérieures. Le bienfait des formalismes à cet égard est d'apprendre où il faut désormais regarder pour entrer dans le radicalement nouveau, dans le véritable imprévu qui seul fait les grandes conquêtes.

La logique de la pensée mathématique paraît ainsi s'être conquise à la fois en vertu d'une espérance naïve de la rationalité mathématique et comme en vue de démontrer à l'esprit le succès bien relatif de cette espérance c'est-à-dire au fond sa catastrophe. Mais les résultats de cette conquête ne sont pourtant pas aussi négatifs qu'il peut le paraître au terme de cette démonstration toute neuve (il y a tout juste vingt cinq ans que Gödel a démontré ses théorèmes). Un certain départ se fait. Ce qui passe des mathématiques et de leur logique dans les formalismes c'en est précisément le passé, si riche soit-il encore d'avenues à parcourir et incomplètement parcourues. Mais la nette conscience de ce passé, une fois bien vu qu'il ne saurait être tout, permet d'aborder le tout avec des yeux renouvelés, formés à l'exploration de l'avenir, aussi bien ouverts à la création mathématique la plus essentielle que préparés à la logique, inédite encore, de ces créations qui viendront. [pp. 81-82]

BIBLIOGRAPHIE

BOOLOS G.S. & JEFFREY R. [1985]: *Computability and Logic*. Cambridge, Cambridge University Press.

BOUVIER A. & GEORGE M. [1979]: *Dictionnaire des mathématiques*. Paris, PUF.

CHURCH A. [1932]: "A set of postulates for the foundation of logic", *Annals of Mathematics, 33*, no 2, part I, pp. 346-366.

----- [1933]: "A set of postulates for the foundation of logic", *Annals of Mathematics, 34*, part II, pp. 839-864.

CORCORAN J. [1973]: "Gaps between logical theory and mathematical practice", in M. Bunge (ed.): *The methodological unity of science*. Dordrecht, Reidel Pub., pp. 23-49.

DALEN D. van [1983]: "Algorithms and decision problems: a crash course in recursion theory", in D. Gabbay & F. Guenthner (eds): *Elements of classical logic*. Dordrecht, Reidel Pub., pp. 409-478.

DAVIS M. [1965]: *The undecidable*. New York, Raven Press.

DEDEKIND D.W.R. [1932]: "Was sind und was sollen die Zahlen?", *Ges. Math. Werke, t. III*. Vieweg, Braunschweig, pp. 335-391 (parution 1888).

DETLOVS V.K. [1958]: "Equivalence of normal algorithms and recursive functions", *Tr. Mat. Inst. Steklov, LII*, pp. 75-139.

DIEUDONNE J. [1978]: *Abrégé d'histoire des mathématiques, II*. Paris, Hermann.

DUBARLE D. [1957]: *Initiation à la logique*. Paris, Gauthier-Villars, Collec. de Logique mathématique, XIII.

----- [1967]: "Critique du réductionnisme" in *Logique et connaissance scientifique*. Paris, Gallimard, La Pléiade, pp. 334-356.

DUMITRIU A. [1977]: *History of logic*. Tunbridge Wells (Kent), Abacus Press, 4t. en 1 vol. Transl. by D. Zamfriescu.

EUCLIDE [1956] : *The thirteen books of Euclid's elements*. New York, Dover. Traduction, introduction et commentraire de T. Heath.

GENTZEN G. [1935]: "Die Wiederspruchfreiheit der reinen Zahlentheorie", *Mathematischen Annalen, vol. 112*, pp. 493-565.

GODEL K. [1931]: "Ueber formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I", *Monatsch. für Math. und Physik, 38*, pp. 193-198.

----- [1965]: "On formally undecidable propositions of Principia Mathematica and related Systems", in M. Davis (ed.) [1965], pp. 5-38. (Première publication 1931).

----- [1967]: "The completeness of the axioms of the functional calculus of logic", in J. van Heijenoort (ed.) [1967], pp. 582-591. (Première publication 1930).

GRASSMANN H. [1984]: *Gesammelte Werke*. Leipzig, Teubner, 3. vol.

GRIZE J.-B. [1972]: *Logique moderne I*. Paris/ Mouton, Gauthier-Villars/ La Haye.

GRZEGORCZYK A. [1974]: *An outline of mathematical logic*. Dordrecht, Reidel Pub.

HEIJENOORT J. van [1967]: *From Frege to Gödel*. Cambridge, Harvard University Press.

HENKIN L. [1949]: "The completeness of the first-order fonctional calculus", *The Journal of Symbolic Logic, vol. 14,* no 3, pp. 159-166.

HERBRANDT J. [1930]: "Recherches sur la théorie de la démonstration", *Travaux de la Société des Sciences et des Lettres de Varsovie, III,* 33, pp. 33-160.

HILBERT D. & BERNAYS P. [1934]: *Grundlagen der Mathematik*. Berlin, Springer, vol. 1.

------ [1939]: *Grundlagen der Mathematik*. Berlin, Springer, vol. 2.

HILBERT D. [1967]: "The foundation of mathematics", in J. van Heijenoort (ed.) [1967], pp. 464-479. (Première publication 1927).

HUNTER G. [1973]: *Metalogic. An introduction to the metatheory of standard first-order logic*. Berkeley, University of California Press.

KLEENE S.C. [1935]: "A theory of positive integers in formal logic", *American Journal of Mathematics, vol. 57,* part I, pp. 153-173, part II, pp. 219-244.

------ [1936]: "λ-definability and recursiveness", *Duke Math. Journal,* 2, 340-353.

------ [1971]: *Introduction to metamathematics*. Amsterdam, North-Holland.

KNEALE N. & KNEALE M. [1962]: *The development of logic*. Oxford, Clarendon Press.

LOWENHEIM L. [1967]: "On possibilities in the calculus of relatives", in J. van Heijenoort (ed.) [1967], pp. 228-251. (Première parution 1915].

MARKOV A. [1954]: "The theory of algorithms", *Tr. Mat. Inst. Steklov, XLII.*

MARTIN R. [1964]: *Logique contemporaine et formalisation*. Paris, PUF.

MENDELSON E. [1979]: *Introduction to mathematical logic*. New York, Van Nostrand.

MONK J.B. [1976]: *Mathematical logic*. New York, Springer.

PEANO G. [1967]: "The principles of arithmetic, presented by a new method" in J. van Heijenoort (ed.) [1967], pp. 23-97. (Première publication 1889).

PRESBURGER M. [1929]: "Ueber die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt", *Sprawozdanre z I Kongresu matematyków krojów slowianskich, Warszawa 1929.* (Warsaw, 1930), pp. 92-101, 395.

ROBINSON R.M. [1950]: "An essentially undecidable axiom system", *Proceedings of the International Congress of Mathemacians.* Cambridge, University Press.

ROSSER D.B. [1978]: *Logic for mathematicians.* New York, Chelsea.

SKOLEM T. [1933]: "Ueber die Unmöglichkeit einer vollständigen Charakterisierung der Zahlenreihe mittels eines eindlichen Axiomensystems, *Norsk matematisk forenings skrifter,* série 2, no 10, pp. 73-82.

----- [1934]: "Ueber die Nicht-Charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen, *Fundamenta Mathematicae, 23,* pp. 150-161.

----- [1967]: "On mathematical logic", in J. van Heijenoort (ed.) [1967], pp. 508-524. (Première publication 1923).

----- [1971]: "Peano's axioms and models of Arithmetic", in T. Skolem *et al.: Mathematical interpretation of formal systems.* Amsterdam, North-Holland, 1-14.

TARSKI A. [1971]: *Introduction à la logique.* Paris, Gauthier-Villars.

----- [1972]: *Logique, sémantique, métamathématique.* Paris, A. Colin, vol. 1.

----- [1974]: *Logique, sémantique, métamathématique.* Paris, A. Colin, vol. 2.

TURING A. [1936-37]: "On computable numbers, with an application to the Entscheidungsproblem", *Proceedings of London Math. Society, 42:* pp. 230-265, *43:* pp. 544-546.

----- [1937]: "Computability and λ-definability", *The Journal of Symbolic Logic, vol. 2,* no 4, pp. 153-165.

WHITEHEAD A.N. & RUSSELL B. [1910]: *Principia Mathematica.* Cambridge, University Press, vol 1.

INDEX DES AUTEURS

Les nombres qui sont en italiques renvoient aux pages du présent fascicule; ceux qui ne le sont pas concernent le premier fascicule (Travaux de logique, Nº 4).

INDEX DES MATIERES

Les définitions numérotées se trouvent aux pages soulignées ici. Les nombres en italiques renvoient aux pages du présent fascicule; ceux qui ne le sont pas concernent le premier fascicule (Travaux de logique, Nº 4).

Couverture : Atelier Seth, Peseux
Impression : Zentralstelle der Studentenschaft der Universität Zürich