a_4 : $\sim(\underline{0} \boxminus v_i^*)$ que nous écrivons: $\underline{0} \not\boxminus v_i^*$

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.

Questions :

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) $\vdash (t_i \boxplus t_k) \supset (t_k \boxplus t_i)$

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

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) $\Psi_{P2} : EP^2 \longrightarrow (\mathbb{N}^2)$ [organisation relationnelle]

4) $\Psi_{F1} : EF^1 \longrightarrow (\mathbb{N}^2)$ [organisation fonctionnelle unaire]

5) $\Psi_{F2} : EF^2 \longrightarrow (\mathbb{N}^2 \times \mathbb{N})$ [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:

Ψ_{F1} ($\underline{0}$*) =df Ψ_{F1} ($\underline{0}$) +1

=df 0 + 1

=df 1

Ψ_{F1} ($\underline{0}$**) =df Ψ_{F1} ($\underline{0}$*) +1

=df 1 + 1

=df 2

Ψ_{F1} ($\underline{0}$*···*) =df Ψ_{F1} ($\underline{0}$*···*) +1 (n fois ; n-1 fois)

=df (n - 1) +1

=df n

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:

$$\underline{0}\overbrace{*\ldots*}^{r \text{ fois}}$$

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:

$$\begin{array}{ll} & m + n, \quad \text{si } m + n = r \\ \text{ou} & k \,.\, p, \quad \text{si } k \,.\, p = r \end{array}$$

L'objet $\underline{0}*\ldots*$ peut donc ainsi être également associé aux expressions numérales $\underline{m + n}$ ou $\underline{k \,.\, p}$. 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 :

$$\underline{0}\overbrace{*\ldots*}^{n \text{ fois}}\overbrace{*}^{1 \text{ fois}} \boxminus \underline{0}\overbrace{*\ldots**}^{n+1 \text{ fois}}$$

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:

$$Pv_i\underline{0} =df \underline{0}^* \quad \text{et} \quad Pv_iv_j^* =df (Pv_iv_j) \boxdot v_i$$

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. $P\ \underline{m}\ \underline{0} \boxminus P\ \underline{m}\ \underline{0}$	ref
2. $P\ \underline{m}\ \underline{0} \boxminus \underline{0}^*$	Déf. 39
3. $\underline{0}^* \boxminus \underline{0 + 1}$	Mth. 34.1
4. $\underline{0 + 1} \boxminus \underline{1}$	0 + 1 = 1; Mth. 34.2
5. $\underline{0}^* \boxminus \underline{1}$	3, 4; rem
6. $P\ \underline{m}\ \underline{0} \boxminus \underline{1}$	5, 2; rem
7. $\underline{1} \boxminus \underline{m^0}$	$1 = m^0$; Mth. 34.2
8. $P\ \underline{m}\ \underline{0} \boxminus \underline{m^0}$	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. $P\ \underline{m}\ \underline{k} \boxminus \underline{m^k}$	hyp. d'ind.
2. $P\ \underline{m}\ \underline{k}^* \boxminus P\ \underline{m}\ \underline{k}^*$	ref
3. $P\ \underline{m}\ \underline{k}^* \boxminus ((P\ \underline{m}\ \underline{k}) \boxdot \underline{m})$	Déf. 39
4. $P\ \underline{m}\ \underline{k}^* \boxminus \underline{m^k} \boxdot \underline{m}$	1, 3; rem, t_i est P m k et $A(t_i)$ est $P\ \underline{m}\ \underline{k}^* \boxminus ((P\ \underline{m}\ \underline{k}) \boxdot \underline{m})$
5. $\underline{m^k} \boxdot \underline{m} \boxminus \underline{m^k . m}$	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 $(\exists v_k)((v_k \not\boxplus \underline{0}) \wedge ((v_i \boxplus v_k) \boxminus v_j))$

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

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. $(\underline{m + k})$ ⊟ $(\underline{m}$ ⊞ $\underline{k})$	Mth. 34.4
3. $(\underline{m}$ ⊞ $\underline{k})$ ⊟ $\underline{n}$	1, 2; rem, t_i est $(\underline{m + k})$ ⊟ $\underline{n}$ et $A(t_i)$ est $(\underline{m + k})$ ⊟ $(\underline{m}$ ⊞ $\underline{k})$
4. $\underline{k}$ ⊉ $\underline{0}$	1); Mth.. 34.2
5. $(\underline{k} \not\boxplus 0) \wedge ((\underline{m} \boxplus \underline{k}) \boxminus \underline{n})$	4, 5; $\wedge$i
6. $(\exists v_k)((v_k \not\boxplus \underline{0}) \wedge ((\underline{m} \boxplus v_k) \boxminus \underline{n}))$	5; $\exists$i
7. $\underline{m} < \underline{n}$	6; Déf. 40

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

Q u e s t i o n :

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:

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

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:

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

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. $t_i \boxminus t_j$	prêmisse
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. $t_i \boxminus t_j$	Prêmisse
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⊃ Q]
9. $B(t_i) \supset C(t_i)$	3, répétition [Q⊃ R]
10. $C(t_i) \supset C(t_i//t_j)$	1, 6; MP [R⊃ 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.

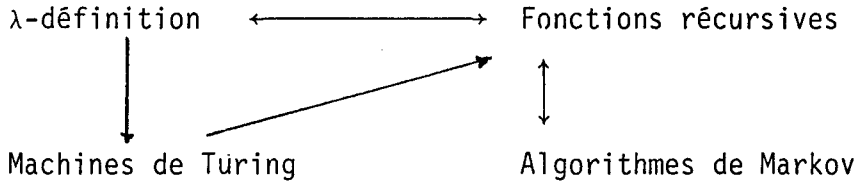
L'existence de ces différentes théories capables de représenter l'effectivement calculable posait bien entendu le problème de leur puissance représentative respective. En effet, chacune de ces démarches théoriques exprimait-elle un ensemble équivalent de fonctions calculables? En 1936, Kleene fournit 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 fonctions calculables 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

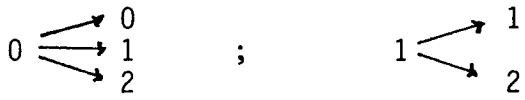
Nous avons utilisé le terme de fonction sans pour autant avoir pris la précaution de définir cette notion. Bien que, d'une certaine manière, celle-ci est tombée dans le 'domaine publique', derrière elle se profile quelques ambiguïtés qu'il est souhaitable de dissiper. Avec cette intention, étudions l'exemple 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 UNIVOQUE 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,

$$y = f(x) = x^3 (\mathrm{mod} 4)$$

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:

$$f : E_1x... \times E_n \rightarrow F,\ f(x_1,..., x_n) \text{ est } M(x_1,..., x_n)$$

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.

$f(x_1, x_2, x_3) = P_2^3(x_1, x_2, x_3)$

$h_1(x_1, x_2) = S(P_1^2(x_1, x_2))$

$h_2(x_1, x_2) = P_2^2(x_1, x_2)$

$h_3(x_1, x_2) = P_1^2(x_1, x_2)$