THEORIE ELEMENTAIRE DE LA MULTIPLICATION DES ENTIERS NATURELS

Patrick CEGIELSKI
27, rue Dézobry
93200 SAINT-DENIS(France)

INTRODUCTION.- Soit M la théorie du premier ordre de la multiplication des entiers naturels non nuls, c'est-à-dire de la structure $(\mathbb{N},.)$ de langage L = (.), où . est un signe fonctionnel binaire.

Comme pour toute théorie d'une structure infinie, on sait que M est non-contradictoire, complète et non-catégorique (la structure ci-dessus, appelée modèle standard de la théorie étudiée, n'est pas le seul modèle (même à isomorphisme près))(cf. [ME]).

Dans ce qui suit, je donne une axiomatique explicite de cette théorie, puis une élimination des quantificateurs, ce qui permet de caractériser les types, je montre qu'elle est conséquence de la Σ_0-induction (théorie bien plus faible que l'arithmétique de Péano), et enfin que les quantificateurs de Ramsey sont éliminables dans le modèle standard.

Presburger [Pr] a étudié la théorie de l'addition, i.e. de la structure $(\mathbb{N},+)$, en 1929 : il en a donné une axiomatique explicite, une élimination des quantificateurs et montré ainsi qu'elle était décidable. Skolem montrait l'année suivante que la théorie de la multiplication était décidable (résultat bien connu, cf. [SK],[MO] et [FV]). Récemment, il y a eu des travaux de Jensen et Ehrenfeucht [JE], de Rackoff sur la complexité de l'algorithme de décision [RA], de

Lessan [LE] et enfin de Nadel qui montre que la théorie complète de la multiplication est conséquence de l'arithmétique de Péano [NA]. D'autre part, Zoé Chatzidakis [CH] a caractérisé tous les modèles de la théorie de la multiplication en termes de faisceaux.

Cet article est une version révisée de ma thèse de troisième cycle soutenue le 25 mars 1980 à l'Université Paris VI (François Aribaud, président, Roland Fraïssé, Angus Macintyre, Kenneth Mc Aloon et Bruno Poizat, examinateurs). Je tiens à remercier tous ceux sans qui cette thèse n'aurait pas été menée jusqu'à son terme, et plus particulièrement Kenneth Mc Aloon qui m'a proposé les sujets, Bruno Poizat qui m'a guidé durant toute sa préparation ainsi que l'Ecole Normale Supérieure de l'Enseignement Technique (Cachan).

A.- PRELIMINAIRES : LA THEORIE DE L'ADDITION

1.- AXIOMATISATION DE LA THEORIE DE L'ADDITION

Soit PRESB la théorie de l'addition des entiers naturels, i.e. de la structure $(\mathbb{N},+)$, de langage $(+)$, où $+$ est un signe fonctionnel binaire. Voici une axiomatique de cette théorie (cf. [PR] ou [FR]) :

A1. (Associativité) $\forall x \forall y \forall z \ (x+(y+z)=(x+y)+z)$

A2. (Element neutre) $\exists y \ \forall y \ (x+y=y+x=y)$
cet élément neutre est unique et on le note 0).

A3. (Commutativité) $\forall x \forall y \ (x+y=y+x)$

A4. (Régularité) $\forall x \forall y \forall z \ (x+z=y+z \rightarrow x=y)$

A5. (Positivité) $\forall x \forall y \ (x+y=0 \rightarrow x=y=0)$
(On note $n.x$ le terme défini par récurrenxe sur $n \in \mathbb{N}$ par :

$(0.x=0$ et $(n+1).x=n.x+x.)$

$A6^n$. (Pas de torsion) (pour tout $n \in \mathbb{N}^*$:) $\forall x \ (n.x=0 \rightarrow x=0)$
(On définit la relation $\leq$ par : $x \leq y$ ssi $\exists z \ (y=z+x)$.)

A7. (Ordre total) $\forall x \forall y \ (x \leq y \vee y \leq x)$

A8. (Discrétion) $\exists x \forall y \ (x \neq 0 \wedge (0 \leq y \leq x \rightarrow (y=0 \vee y=x)))$
(Cet x est unique et on le note 1.)

$A9^n$. (Divisibilité) (pour tout $n \in \mathbb{N}^*$:)

$\forall x \exists y \exists z \ (x=n.y+z \wedge z \leq n.1 \wedge z \neq n.1)$

2.- ELIMINATION DES QUANTIFICATEURS POUR LA THEORIE DE L'ADDITION

D1 1°.- On dit qu'une formule d'un langage L est ouverte (ou sans quantificateurs) ssi aucune occurrence d'un quantificateur n'y intervient ;

2°.- On dit qu'une théorie T de langage L élimine les quantificateurs ssi toute formule ϕ de L est T-équivalente à une formule ψ de L ouverte.

3°.- Là où il n'y a pas de risque de confusion, et où il est clair de quelle théorie T il s'agit, on écrira simplement ϕ au lieu de $T \vdash \phi$

D2.- Pour n entier on note, dans la théorie de l'addition, $x \leq_n y$ pour : $\exists\, z\ (y = n \cdot z + x)$.

Remarque.- Pour n = 0, on retrouve ainsi l'égalité ; pour n = 1, ce n'est rien d'autre que la relation d' ordre. Pour $n \geq 2$, $x \leq_n y$ signifie non seulement que x est congru à y modulo n au sens classique mais aussi que $x \leq y$. On peut définit $x \equiv_n y$ par :

$$(x \leq_n y \vee y \leq_n x).$$

Presburger a montré que la théorie de l'addition de langage $(+,0,1, \leq, (\equiv_n)_{n\geq 2})$ (ou $(+,0,1,(\leq_n)_{n\in\mathbb{N}})$) élimine les quantificateurs (c'est en fait le résultat qui sert à montrer la complétude de PRESB). Nous le redémontrons ci-dessous en T2.

3.- FONCTIONS DE SKOLEM

D3.-On dit qu'une théorie T admet des fonctions de Skolem ssi pour toute $(n+1)$-formule $\theta(x,x_1,\ldots,x_n)$ de L(T) il existe une relation fonctionnelle (ou application définissable) $y = f(x_1,\ldots,x_n)$ telle que :

$$T \vdash \forall x_1 \ldots \forall x_n\ (\exists x\, \theta(x,x_1,\ldots,x_n) \longleftrightarrow \theta(f(x_1,\ldots,x_n),(x_1,\ldots,x_n))).$$

T1.- La théorie de l'addition admet des fonctions de Skolem.

Démonstration.- En effet, on prend pour $f(x_1,\ldots,x_n)$ le plus petit x convenant, i.e. : - si $\neg\exists\, x\, \theta(x_1,\ldots,x_n)$ alors x = 0 ;

- sinon le x tel que :

$$\theta(x,x_1,\ldots,x_n) \wedge \forall y\ (\theta(y,x_1,\ldots,x_n) \rightarrow y \geq x),$$

un tel x existe car c'est vrai dans le modèle standard (principe du bon ordre) et puisque la théorie est complète (nous le verrons d'ailleurs directement dans T2). On note cet x: $\mu y\, \theta(y,x_1,\ldots,x_n)$ (lire : "le plus petit y tel que ...").

T2.- Les fonctions de Skolem $y = f(x_1,\ldots,x_n)$ sont définies par :

$$\bigwedge_{1\le i\le k} (C_i(x_1,\ldots,x_n) \to y = t_i(x_1,\ldots,x_n))$$

avec C_i formule du langage de l'élimination des quantificateurs et t_i terme du langage $L' = (+,\dot{-},([\frac{-}{n}])_{n\in\mathbb{N}^*},0,1)$, où

- $\dot{-}$ est la soustraction complète : $x \dot{-} y = \begin{cases} x - y & \text{si } x \ge y \\ 0 & \text{sinon} \end{cases}$

- $[\frac{x}{n}]$ est le quotient dans la division euclidienne de x par n, dont l'existence est affirmée par $A9^n$.

Démonstration.- Nous allons, en fait, en plus montrer l'élimination des quantificateurs, ce qui se fait par récurrence sur la complexité de la formule. Le seul cas non trivial est celui de : $\exists\, x\ \theta(x,x_1,\ldots,x_n)$. Par hypothèse de récurrence et d'après la mise sous forme normale, nous avons, en remarquant de plus les équivalences :

- $x = y \leftrightarrow (x \le y \wedge y \le x)$
- $x \ne y \leftrightarrow (x+1 \le y \vee y+1 \le x)$
- $\neg(x \le y) \leftrightarrow y+1 \le x$
- $\neg(x \equiv_n y) \leftrightarrow (x+1 \equiv_n y \vee \ldots \vee x+n-1 \equiv_n y)$,

la forme canonique

$$\theta(x,x_1,\ldots,x_n) \leftrightarrow \bigvee_{1\le i\le k} (u_1 \le u_1' \wedge \ldots \wedge u_p \le u_p' \wedge v_1 \equiv_{m_1} v_1' \wedge \ldots \wedge v_q \equiv_{m_q} v_q')$$

avec les u et v termes de $(+,0,1)$.

On voit, par récurrence sur la complexité, que tout terme t en $x, x_1,\ldots,x_n$ de $(+,0,1)$ est, à PRESB-équivalence près, de la forme :

$$a_1x_1 + \ldots + a_nx_n + ax + a' \quad , \quad \text{avec } a_1,\ldots,a_n,a,a' \in \mathbb{N} \ .$$

D'autre part, pour $m \in \mathbb{N}^*$ on a : $\forall\, x\ (x \equiv_m 0 \vee x \equiv_m 1 \vee \ldots \vee x \equiv_m m-1)$.

D'où $t \equiv_m t' \leftrightarrow \bigvee (x_1 \equiv_m a_1 \wedge \ldots \wedge x_n \equiv_m a_n \wedge x \equiv_m a)$

avec : $a_1,\ldots,a_n,a < m$. Enfin, on a

$$a\,x+u \leq u' \leftrightarrow x \leq \left[\frac{u' \dot{-} u}{a}\right] \quad , \qquad \text{pour } a \in \mathbb{N}^* \quad , \text{ et :}$$

$$u' \leq a\,x+u \longleftrightarrow (u' \leq u \vee \left[\frac{u' \dot{-} u}{a}\right] \leq x).$$

Ainsi : $\theta(x,x_1,\ldots,x_n) \leftrightarrow \bigvee_{1\leq i\leq k} (C_i(x_1,\ldots,x_n) \wedge x \equiv_{m_1} a_1 \wedge\ldots\wedge x \equiv_{m_p} a_p$

$$\wedge\, u_1 \leq x \wedge\ldots\wedge u_r \leq x \wedge x \leq v_1 \wedge \ldots\wedge x \leq v_s)$$

avec un autre k que celui ci-dessus, C_i conjonction de formules de la forme : $w \leq w'$, $x_j \equiv_m b$ avec $m \in \mathbb{N}^*$, $b < m$, w et w' termes en $x_1,\ldots,x_n$ du langage $(+,0,1)$, et les u_j et v_j termes en $x_1,\ldots,x_n$ du langage L'.

Si, dans les C_i, nous incorporons des $x_j \equiv_{m_r} b_{jr}$ pour $1 \leq r \leq p$ $1 \leq j \leq n$ (en augmentant k et le nombre de termes de la disjonction), ainsi que pour σ,τ permutations de $[1,r]$ et $[1,p]$ respectivement:

$$u_{\sigma(1)} \leq\ldots\leq u_{\sigma(r)} \ , \ v_{\tau(1)} \leq\ldots\leq v_{\tau(s)} \quad ,$$

nous avons, en posant $u = u_{\sigma(r)}$, $v = v_{\tau(s)}$, éventuellement $u = 0$ si $r = 0$, " $\leq v$" le mot vide si $s = 0$:

$$\theta(x,x_1,\ldots,x_n) \longleftrightarrow \bigvee_{1\leq i\leq k} (C_i(x_1,\ldots,x_n) \wedge u \leq x \leq v$$

$$\wedge\, x \equiv_{m_1} a_1 \wedge\ldots\wedge x \equiv_{m_p} a_p)$$

Or dès que nous connaissons les restes modulo les m_r pour les x_j nous les connaissons aussi pour u, nous savons donc exprimer le plus petit u' plus grand que u tel que : $u' \equiv_{m_1} a_1 \wedge\ldots\wedge u' \equiv_{m_p} a_p$, il est de la forme : $u' = u+N$, avec $N \in \mathbb{N}$.

Remarquons enfin que pour w, w' termes de L' nous avons : $w \leq w' \leftrightarrow \phi$, avec ϕ formule sans quantificateur de $(+,0,1)$, par récurrence sur la complexité, car :

$$x \dot{-} y \leq z \longleftrightarrow ((x \geq y \wedge x \leq z+y) \vee x \leq y), \quad \left[\frac{x}{n}\right] \leq y \leftrightarrow x \leq n\,.\,y.$$

Aussi peut-on considérer les conditions C_i comme étant des formules du langage de l'élimination. Par conséquent :

$$\exists\, x\ \theta(x,x_1,\ldots,x_n) \longleftrightarrow \bigvee (C_i(x_1,\ldots,x_n) \wedge u' \leq v)$$

(sans " $u' \leq v$ " éventuellement s'il n'y a pas de v), ce qui montre le théorème de l'élimination, et d'autre part,

$$(C_i(x_1,\ldots,x_n) \wedge u' \leq v) \rightarrow y = u' \ ,$$

ce qui donne la forme des fonctions de Skolem (remarquons que les conditions peuvent ne pas être indépendantes, mais cela n'a pas d'importance). □

B.- AXIOMATISATION

1.- SOMME DIRECTE DE STRUCTURES

D1.- Soient L un langage ayant une et une seule constante, notée O, $(\mathcal{A}_i)_{i\in I}$ une famille non vide de L-structures telle que pour tout i de I et tout symbole fonctionnel F de L, on ait : $F(O,\ldots,O) = O$.
La somme directe de cette famille est la L-structure $\mathcal{B}$, notée $\bigoplus_{i\in I} \mathcal{A}_i$, définie par :

- $B = \{f \in \prod_{i\in I} A_i / f(i) = O$ sauf pour au plus un nombre fini de $i\}$;
- pour R prédicat n-aire de L : $\bar{R}^{\mathcal{B}}(f_1,\ldots,f_n)$ ssi pour tout i de I on a $\bar{R}^{\mathcal{A}_i}(f_1(i),\ldots,f_n(i))$;
- pour F symbole fonctionnel n-aire de L :

$$\bar{F}^{\mathcal{B}}(f_1,\ldots f_n) = (\bar{F}^{\mathcal{A}_i}(f_1(i),\ldots,f_n(i)))_{i\in I} .$$

Remarques : 1°.- $\bigoplus_{i\in I} \mathcal{A}_i$ est bien une L-structure, la clôture pour les fonctions étant assurée par la condition sur la famille ;

2°.- Si I est fini, la somme directe est la même chose que le produit direct.

Exemples : 1°.- On a $(\mathbb{N}^*,.) = \bigoplus_{n\in\mathbb{N}} \mathcal{A}_n$ avec $\mathcal{A}_n = (\mathbb{N},+)$ pour tout n ;

2°.- On a $(\mathbb{N}^*,|) = \bigoplus_{n\in\mathbb{N}} \mathcal{A}_n$ avec $\mathcal{A}_n = (\mathbb{N},\leq)$ pour tout n, où | est la relation de divisibilité.

2.- AXIOMATIQUE.

Introduction.- Pour donner une axiomatique de la théorie M, nous allons commencer par exhiber une théorie de langage L dont $(\mathbb{N}^*,.)$ est un modèle (et que nous noterons encore M par abus de langage), puis nous montrerons que cette théorie est complète.

L'axiomatique est une modélisation, dans le langage du premier ordre L, du fait que M est une somme directe de modèles de la théorie de l'addition (ce qui ne veut pas dire, bien sûr, que les modèles de cette théorie soient de cette forme). Pour cela, on définit l'ensemble $\mathbb{P}$ des nombres premiers, qui jouera le rôle de l'ensemble indiciel I, les nombre p-primaires PR(p,) (c'est-à-dire tel que p soit le seul nombre premier les divisant), la valuation p-adique d'un nombre x, V(p,x) (c'est-à-dire le plus grand nombre p-primaire divisant x, et non l'exposant de p de celui-ci, qu'il n'est pas possible de définir dans ce langage).

D2.- On appelle théorie de la multiplication la théorie M de langage L = (.), où . est un signe fonctionnel binaire, et dont les axiomes propres sont les axiomes et schémas d'axiomes suivants.

A1.- (Associativité) $\forall x \forall y \forall z \quad (x . (y . z) = (x . y) . z)$

A2.- (Elément neutre) $\exists x \forall y (x . y = y . x = y)$

(cet élément neutre qui est unique est noté 1).

A3.- (Commutativité) $\forall x \forall y (x . y = y . x)$

A4.- (Régularité) $\forall x \forall y \forall z (x . z = y . z \to x = y)$

A5.- (Positivité) $\forall x \forall y (x . y = 1 \to x = y = 1)$

(on note x^n le terme défini par récurrence sur $n \in \mathbb{N}$ par : $x^0 = 1$ et : $x^{n+1} = x^n . x$).

$A6^n$.- (Pas de torsion) (Pour $n \in \mathbb{N}^*$) : $\forall x \forall y (x^n = y^n \to x = y)$

d1.- On dit que x divise y, et on note $x \mid y$, ssi on a : $\exists z (y = z . x)$. ce z qui est unique, se note : $\frac{y}{x}$

$A7^n$.- (Divisibilité) (Pour $n \in \mathbb{N}^*$) :

$\forall x \exists y \exists z (x = y^n . z \wedge \forall y' \forall z' (x = y'^n . z' \to z \mid z'))$

d2.- p est un nombre premier, et on note $\mathbb{P}(p)$, ssi on a :

$p \neq 1 \wedge \forall x (x \mid p \to (x = 1 \vee x = p))$

A8.- (Existence de nombres premiers) $\forall x \exists p (\mathbb{P}(p) \wedge p \nmid x)$
(cet axiome dit beaucoup plus que l'existence de nombres premiers, à savoir l'existence d'une infinité de nombres premiers).

d3.- x est un nombre p-primaire, et on note PR(p,x), ssi on a :

$$\mathbb{P}(p) \wedge \forall q((\mathbb{P}(p) \wedge q \neq p) \rightarrow q \nmid x)$$

A9.- (| total sur PR(p,))

$$\forall p \forall x \forall y ((PR(p,x) \wedge PR(p,y)) \rightarrow (x \mid y \vee y \mid x))$$

d4.- On définit la valuation p-adique de x, et on note V(p,x) par :

$$y = V(p,x) \leftrightarrow (\mathbb{P}(p) \wedge PR(p,y) \wedge y \mid x \wedge \forall z((PR(p,z) \wedge z \mid x) \rightarrow z \mid y))$$

A10.- (Existence des valuations) $\forall x \forall p (\mathbb{P}(p) \rightarrow \exists y (y = V(p,x)))$.

A11.- (x est caractérisé par ses valuations)

$$\forall x \forall y (x = y \leftrightarrow \forall p (\mathbb{P}(p) \rightarrow V(p,x) = V(p,y)))$$

A12.- (Linéarité de la valuation)

$$\forall x \forall y \forall p (\mathbb{P}(p) \rightarrow V(p,x \cdot y) = V(p,x) \cdot V(p,y))$$

A13.- (Division)

$$\forall x \forall y (\forall p (\mathbb{P}(p) \rightarrow V(p,x) \mid V(p,y)) \rightarrow x \mid y)$$

A14.- (Troncage)

$$\forall x \forall y \exists z \forall p (\mathbb{P}(p) \rightarrow ((p \mid x \rightarrow V(p,z) = V(p,y)) \wedge (p \nmid x \rightarrow V(p,z) = 1)))$$

(ce z qui est unique, est noté T(x,y)).

(c'est-à-dire, si $y = \prod p^{\alpha}$ alors $T(x,y) = \prod_{p/x} p^{\alpha}$).

A15.- (Incrémentation)

$$\forall x \exists y \forall p (\mathbb{P}(p) \rightarrow ((p \nmid x \rightarrow V(p,y) = 1) \wedge (p \mid x \rightarrow V(p,y) = p \cdot V(p,x))))$$

(ce y, qui est unique, est noté Ix).

(c'est-à-dire, si $x = \prod p^{\alpha}$ alors $Ix = \prod_{p|x} p^{\alpha+1}$).

d5.- Pour $n \in \mathbb{N}$, on note $x \equiv_n y$ ssi on a : $\exists z\ (y = z^n . x)$.

(Attention : ceci ne signifie pas seulement que les valuations au sens usuel de x sont congrues modulo n aux valuations de y, mais aussi que $x|y$).

A16.- (Séparation) (pour $n \in \mathbb{N}$) :

$$\forall x \forall y \exists z \forall p\ (\mathbb{P}(p) \rightarrow ((p \mid x . y \wedge V(p,x) \equiv_n V(p,y)) \rightarrow V(p,z) = p)$$

$$\wedge\ (p \nmid x . y \vee V(p,x) \not\equiv_n V(p,y)) \rightarrow V(p,z) = 1)))$$

(ce z, qui est unique, est noté $SP_n(x,y)$).

(c'est-à-dire, si $x = \prod p^{\alpha}$, $y = \prod p^{\beta}$, $SP_n(x,y) = \prod_{\substack{p^{\alpha} \equiv_n p^{\beta} \\ p \mid x . y}} p$,

La condition $p \mid x . y$ est là pour assurer qu'on est en présence d'un produit "fini").

3.- DEVELOPPEMENT DE LA THEORIE

D3.- Soient $\mathcal{A}$ un modèle de M, p un nombre premier de $\mathcal{A}$ (i.e. $p \in A$ et $\mathcal{A} \models \mathbb{P}(p)$). On note $\mathcal{A}_p$ la structure $(A_p, .)$ où

$$A_p = \{x \in A / \mathcal{A} \models PR(p,x)\}$$

et . est la restriction de . à A_p.

T1.- $\mathcal{A}_p$ est un modèle de la théorie de l'addition.

Démonstration. $\forall p\ (\mathbb{P}(p) \rightarrow PR(p,1))$: en effet, si $q \mid 1$ alors, d'après la positivité(A5), $q = 1$. Ainsi $A_p \neq \emptyset$.

o (Discrétion) $\forall p \forall x\ ((\mathbb{P}(p) \wedge PR(p,x)) \rightarrow$

$\exists y\ (x \mid y \wedge PR(p,y) \wedge x \neq y \wedge \forall z\ ((x \mid z \wedge z \mid y) \rightarrow (z = x \vee z = y))))$:

posons $y = p.x$; si $x \mid z$ alors $z = t.x$; si $z \mid y$ alors : $y = u.z = u.t.x = p.x$ d'où, d'après la régularité (A4), $u.t = p$ et, par définition d'un nombre premier, $t = 1$ ou $t = u$, d'où le résultat.

o $\forall x \forall p\ (PR(p,x) \rightarrow (V(p,x) = x \wedge \forall q\ ((\mathbb{P}(q) \wedge q \neq p \rightarrow V(q,x) = 1)))$: il résulte immédiatement de la définition que $V(p,x) = x$; si $V(q,x) \neq 1$ alors $q \mid V(q,x)$ (d'après la discrétion), or $V(q,x) \mid x$, d'où $q \mid x$, soit $q = p$ par définition de PR.

o $\forall x \forall p\ (PR(p,p))$: en effet, on a $p \mid p$ et pour q nombre premier si $q \mid p$ alors $q = p$, par définition même d'un nombre premier.

o $\forall x \forall y \forall p\ ((\mathbb{P}(p) \wedge PR(p,x) \wedge PR(p,y)) \rightarrow PR(p,x.y))$: si pour q nombre premier différent de p, on avait $q \mid x.y$ alors il existerait z tel que $x.y = z.q$, d'où $V(q,x.y) = V(q,z.q)$, soit, d'après la linéarité (A12), $V(q,x).V(q,y) = V(q,z).V(q,q)$, soit encore $q \mid 1$ d'après ce qui précède, impossible.

Ainsi A_p est stable pour la multiplication et $\mathcal{A}_p$ est bien une structure.

o Que $\mathcal{A}_p$ vérifie les axiomes d'associativité, d'existence d'un élément neutre, de commutativité, de régularité, de positivité, de non-torsion résulte immédiatement des axiomes A1, A2 (et du fait que $1 \in A_p$), A3, A4, A5, et $A6^n$ de la théorie M. D'autre part, nous avons montré la discrétion plus haut.

o L'ordre total résulte de A6 en remarquant que le z tel que $y = z.x$ si $x \mid y$, par exemple, est tel que $PR(p,z)$: en effet, sinon il existe q différent de p tel que $q \mid z$, d'où $q \mid y$, impossible.

o (Divisibilité) (pour tout $n \in \mathbb{N}^*$:)

$$\forall p \forall x\ ((\mathbb{P}(p) \wedge PR(p,x)) \rightarrow \exists y \exists z\ (PR(p,y) \wedge PR(p,z) \wedge x = y^n.z \wedge z \mid p^n \wedge z \neq p^n)$$:

d'après $A7^n$, il existe y et z tels que $x = y^n.z$ et z minimal ; on a

$y \mid x$ et $z \mid x$ d'où $PR(p,y)$ et $PR(p,z)$; si $z \nmid p^n$ alors, d'après l'ordre total, $p^n \mid z$ d'où $z = p^n . z'$ et $x = y^n . p^n . z' = (y . p)^n . z'$ avec $z' \mid z$ et $z' \neq z$, contradiction. □

Conséquence.- Indifféremment dans la suite on utilisera la notation additive (avec $0,1,+,\leq,S,\ldots$) ou multiplicative (avec $1,p,.,\mid,I,\ldots$) lorsqu'on parlera des éléments de A_p.

P1.- Tout modèle de M a une infinité de nombres premiers, plus précisément : $\forall x \exists p (\mathbb{P}(p) \wedge p \nmid x)$.

Démonstration.- En effet, supposons qu'il y ait seulement un nombre fini de nombres premiers, soit $p_1,\ldots,p_n$. Posons alors $x = p_1,\ldots,p_n$ (éventuellement $x = 1$), d'après A8 il existe un nombre premier p qui ne divise pas x, donc $p \neq p_1,\ldots,p_n$, contradiction. □

Remarque.- Si on dit qu'un sous-ensemble P' de nombres premiers est fini si, et seulement si, il existe un élement x de A tel que : $p \in P' \leftrightarrow p \mid x$. Alors un modèle $\mathcal{A}$ de M a aussi une infinité de nombres premiers au sens qu'aucun élément n'est divisible par tous les nombres premiers.

$P2^n$ (pour tout $n \in \mathbb{N}^*$)

$$\forall x \exists y \forall p (\mathbb{P}(p) \rightarrow V(p,y) = [\frac{V(p,x)}{n}])$$

Démonstration.- En effet, d'après l'axiome de divisibilité $A7^n$, il existe y et z tels que : $x = y^n . z$ et z le plus petit possible ; c'est ce z qui convient. □

P3.- $\forall x \forall y \exists z \forall p (\mathbb{P}(p) \rightarrow V(p,z) = V(p,x) \dot{-} V(p,y))$

Démonstration.- On a : $T(SP_1(y,x),y) \mid T(SP_1(y,x),x)$, il suffit de prendre $z = \frac{T(SP_1(y,x),x)}{T(SP_1(y,x),y)}$. □

Ce z est noté $x \dot{-} y$, et on parle de division complète).

T2.- (Existence de tout produit "fini" de nombres p-primaires)

Soit $z = f(\vec{y})$ une relation fonctionnelle de la théorie de l'addition, alors on a

$$\forall\, \vec{x}\ \forall\, x_o\ \exists\, y\ \forall\, p\ (\mathbb{P}(p) \rightarrow ((p \mid x_o \rightarrow V(p,y) = f(V(p,\vec{x}))) \wedge (p \nmid x_o \rightarrow V(p,y) = 1\ )))$$

Démonstration.- On a $z = \mu u(u = f(\vec{y}))$ donc, d'après la forme des fonctions de Skolem pour la théorie de l'addition (A III T2), f est de la forme : $\bigvee_{1\le i\le k} (C_i(\vec{y}) \rightarrow z = t_i(\vec{y}))$, avec C_i formule du langage de l'élimination des quantificateurs pour l'addition et t_i terme du langage $L' = (+, \dot{-}, ([\frac{-}{n}])_{n\in\mathbb{N}^*}, 0, 1)$.

D'après la mise sous forme normale et le fait que la négation d'une formule atomique du langage de l'élimination est une combinaison booléenne positive de formules atomiques, on a f de la forme :

$$\bigvee_{1\le i\le k} \Big(\bigwedge_{1\le j\le m_i} C_{ij}(\vec{y}) \rightarrow z = t_i(\vec{y}) \Big)\ ,$$

avec k éventuellement différent de celui ci-dessus et les $C_{ij}(\vec{y})$ de la forme : $u(\vec{y}) \equiv_{n_{ij}} u'(\vec{y})$, avec $n_{ij} \in \mathbb{N}$, u et u' termes de $(+, 0, 1)$.

Considérons x et x_o. Posons, pour $i \in [1,k]$, $j \in [1,m_i]$:

- $P_{ij} = SP_{n_{ij}}(u(\vec{x}), u'(\vec{x}))\ .\ (x_o \dot{-} (u(\vec{x})\ .\ u'(\vec{x})))$

l'intervention du premier facteur se comprend aisément, le deuxième facteur est dû à ce que si $p \nmid u(\vec{x})\ .\ u'(\vec{x})$ alors on a :

$$u(V(p,\vec{x})) = u'(V(p,\vec{x})) = 1, \text{ d'où : } u(V(p,\vec{x})) \equiv_{n_{ij}} u'(V(p,\vec{x})),$$

mais $p \nmid SP_{n_{ij}}(u(\vec{x}), u'(\vec{x}))$).

- $P_i = \bigcap_{1\le j\le m_i} P_{ij}$ (ceci est obtenu grâce au troncage).

- $b_i = t_i(\vec{x})$ (ceci a un sens en remplaçant + par ., $\dot{-}$ par $\dot{-}$, $[\frac{-}{n}]$ par l'opération exhibée en $P2^n$, O par 1 et 1 par I).

- $a_i = T(P_i, b_i)$, et enfin $a = T(x_o, a_1. \ \ldots \ .a_k)$ alors a est le y cherché. □

4.- COMPLETUDE ET DECIDABILITE DE LA THEORIE M

D4.- Soit L' = (.,V) le langage obtenu à partir de L en ajoutant un signe fonctionnel binaire. A toute formule ϕ de L on associe la formule ϕ^p de L' dont l'ensemble des variables libres est celui de ϕ plus la variable p (mise en exposant dans notre notation), obtenue en remplaçant chaque variable libre x par le terme V(p,x).

P3.- Soit $\mathcal{A}$ un modèle de M, ϕ une n-formule de L, p un nombre premier de $\mathcal{A}$ et $\vec{f} \in A^n$, alors :

$$\mathcal{A} \models \phi^p[\vec{f}] \text{ si et seulement si } \mathcal{A}_p \models \phi\,[V(p,\vec{f})]$$

où $V(p,(f_1,\ldots,f_n)) = (V(p,f_1),\ldots,V(p,f_n))$.

Démonstration.- Par récurrence sur la longueur de ϕ. □

D5.- On note M" la théorie de langage L" = (.,V,P), extension par définition évidente de M.

D6.- Soit θ une formule de L et $k \in \mathbb{N}^*$ alors on pose $R_k(\theta)$ la formule de L" suivante :

$$\exists\, p_1 \ldots \exists\, p_k \Big(\bigwedge_{1\le i\le j\le k} p_i \neq p_j \wedge \bigwedge_{1\le i\le k} \mathbb{P}(p_i) \wedge \theta^{p_i} \Big).$$

T3.- Toute formule ϕ de L est M"-équivalente à une combinaison booléenne de formules du type $R_k(\theta)$.

Démonstration.- Par récurrence sur la longueur de ϕ.

- Pour ϕ atomique, i.e. de la forme t = t', on a :

$$\phi(x_1,\ldots,x_n) \leftrightarrow (\forall\, p \in \mathbb{P})\ (V(p,t) = V(p,t'))$$

$$\leftrightarrow (\forall\, p \in \mathbb{P})\ (t(V(p,x_1),\ldots,V(p,x_n)) = t'(V(p,x_1),\ldots, V(p,x_n))) \leftrightarrow \neg\, R_1(\neg\,\phi)$$

- Pour ϕ négation ou disjonction, l'étape de la récurrence est évidente.

- Pour ϕ de la forme $\exists\, x\, \psi$ on a, par hypothèse de récurrence, et la mise sous forme normale :

$$\phi \leftrightarrow \exists\, x \bigvee (R_{k_1}(\theta_1) \wedge \ldots \wedge R_{k_m}(\theta_m) \wedge \neg R_{k_{m+1}}(\theta_{m+1}) \wedge \ldots \wedge \neg R_{k_{m+n}}(\theta_{m+n}))$$

$$\leftrightarrow \bigvee \exists\, x(R_{k_1}(\theta_1) \wedge \ldots \wedge \neg R_{k_{m+n}}(\theta_{m+n}))$$

Il suffit donc de le montrer pour une formule du genre :

$$\exists\, x(R_{k_1}(\theta_1) \wedge \ldots \wedge \neg R_{k_{m+n}}(\theta_{m+n})).$$

Pour faciliter l'exposé, montrons-le pour une formule du genre :

$$\exists\, x(R_{k_1}(\theta_1) \wedge \ldots \wedge R_{k_m}(\theta_m) \wedge S_{k_{m+1}}(\theta_{m+1}) \wedge \ldots \wedge S_{k_{m+n}}(\theta_{m+n})$$

$$\wedge \neg R_{k_{m+n+1}}(\theta_{m+n+1}) \wedge \ldots \wedge \neg R_{k_{m+n+p}}(\theta_{m+n+p}))$$

où $\underline{S_k}$ est l'abréviation de $R_k \wedge \neg R_{k+1}$ (pour $k \geq 1$).

o Lemme 1.- On peut supposer $\theta_1, \ldots, \theta_{m+n+p}$ deux à deux indépendantes (θ et θ' sont dites indépendantes ssi $\neg(\theta \wedge \theta')$ est une tautologie), et de plus que $\bigvee \theta_i$ est une tautologie.

Démonstration.- En effet, pour $r \subseteq [1, m+n+p]$ posons $\theta'_r = \bigwedge_{i \in r} \theta_i \wedge \bigwedge_{i \notin r} \neg\theta_i$. Alors les θ'_r sont indépendantes et on a le résultat voulu en utilisant les faits suivants et autres transformations analogues :

$$+ (R_k(\theta) \wedge R_{k'}(\theta')) \leftrightarrow \bigvee_{\substack{n,n',n'' \in \mathbb{N} \\ n+n'=k \\ n'+n''=k'}} (R_n(\theta \wedge \theta') \wedge R_{n'}(\theta \wedge \theta') \wedge R_{n''}(\neg\theta \wedge \theta'))$$

(où $R_o(\theta)$ doit être considérée comme la formule vide).

$$+ (R_k(\theta) \wedge \neg R_{k'}(\theta')) \leftrightarrow \bigvee_{\substack{n,n',n'' \in \mathbb{N} \\ n' \leq k'-1 \\ n+n'=k \\ n'+n''=k'}} (R_n(\theta \wedge \neg\theta') \wedge S_{n'}(\theta \wedge \theta') \wedge \neg R_{n''}(\neg\theta \wedge \theta'))$$

□

o Lemme 2.- Etant donné une formule :

$$\psi = \bigwedge_{1\leq i\leq m} R_{l_i}(\theta_i) \wedge \bigwedge_{m+1\leq i\leq m+n} S_{l_i}(\theta_i) \wedge \bigwedge_{m+n+1\leq i\leq m+n+p} \neg R_{l_i}(\theta_i)$$

il existe une formule ψ', combinaison booléenne de formules du type $R_l(\theta)$, telle que pour $\mathcal{A}$ modèle de M, on ait : $\mathcal{A} \models \psi'[\vec{f}]$ si, et seulement si, il existe une "partition" $P_1,\ldots,P_{m+n}$ de $\mathbb{P}$ (c'est-à-dire que les P_i sont deux à deux disjoints), avec :

- pour $i \in [1,m+n]$ P_i contient exactement l_i éléments ;
- pour $i \in [1,m+n]$ si $p \in P_i$ alors $\mathcal{A} \models \theta^p[\vec{f}]$.

Démonstration.- La difficulté provient de ce que même si θ et θ' sont indépendants, i.e. $\neg(\theta \wedge \theta')$ est une tautologie, on peut avoir $\exists x\, \theta \wedge \exists x\, \theta'$.

Cependant, il existe bien une telle formule (c'est un problème de combinatoire) de la forme :

$$\bigvee_{k : 2^{m+n} \to \mathbb{N}} \bigwedge_{j\in 2^{m+n}} S_{k(j)} \left(\bigwedge_{1\leq i\leq m+n} \varepsilon(i,j)\, \exists x\, \theta_i \right)$$

avec $\varepsilon(i,j)$ rien ou le signe de négation, k application correspondant aux parties "convenables" (il y en a un nombre fini, car de toute façon, $k(j) \leq l$, avec $l = \sum_{1\leq i\leq m+n} l_i$). □

o Lemme 3.- On peut supposer ψ de la forme :

$$\bigwedge_{1\leq i\leq m} R_{k_i}(\theta_i) \wedge \bigwedge_{m+1\leq i\leq m+n} S_{k_i}(\theta_i) \wedge \neg R_l(\theta).$$

Démonstration.- On remarque que : $\neg R_{k+1}(\theta) \leftrightarrow \neg R_1(\theta) \vee S_1(\theta) \vee \ldots \vee S_k(\theta)$ et : $\neg R_1(\theta_1) \wedge \ldots \wedge \neg R_1(\theta_k) \leftrightarrow \neg R_1(\theta_1 \vee \ldots \vee \theta_k)$ et on ajoute

des disjonctions. □

o Alors $\exists x\ \psi$ est M"-équivalente à :

$$\psi' \wedge \bigvee_{1\le i\le m} R_1(\theta_i(O,\vec{O})) \wedge \neg R_1(\neg \exists x \neg\theta) \wedge$$

$$\Big(\bigwedge_{m+1\le i\le m+n} \neg R_{k_i+1}\ (\exists x\ \theta_i \wedge \neg\Big(\bigvee_{\substack{1\le j\le m+n\\ i\neq j}} \exists x\ \theta_j\Big)) \qquad (1)$$

$$\wedge \bigwedge_{m+1\le i_1\le i_2\le m+n} \neg R_{k_{i_1}+k_{i_2}+1}\ (\exists x\ \theta_{i_1} \quad \exists x\ \theta_{i_2} \wedge \neg\Big(\bigvee_{\substack{1\le j\le m+n\\ j\neq i_1,i_2}} \exists x\ \theta_j\Big)) \quad (2)$$

$$\wedge \neg R_{\left(\sum_{m+1\le i\le m+n} l_i\right)+1}\ \Big(\bigwedge_{m+1\le i\le m+n} \exists x\ \theta_i \wedge \neg\Big(\bigvee_{1\le j\le m} \exists x\ \theta_j\Big)\Big) \qquad (n)$$

CN : Seul le deuxième terme n'est pas évident. Soit $\mathcal{A}$ un modèle de M, et $\vec{f}$ tel que $\mathcal{A} \models \phi[\vec{f}]$, alors il existe a tel que $\mathcal{A} \models \psi[a,\vec{f}]$. Si $\vec{f} = (f_1,\ldots,f_n)$, soit $a' = a \cdot f_1 \cdot \ldots \cdot f_n$, alors d'après A8, il existe un nombre premier p (et même une infinité) qui ne divise pas a', donc $\mathcal{A} \models \theta_i(O,\ldots,O)$ pour un certain $i \in [1,m+n]$, car $\theta \vee \bigvee_{1\le i\le m+n} \theta_i$ est une tautologie et on a $\neg R_1(\theta)[a,\vec{f}]$, or $\theta_i(O,\ldots,O)$ est un énoncé et $\mathcal{A}_p$ est un modèle de la théorie de l'addition, qui est complète, donc pour tout p on a $\mathcal{A}_p \models \theta_i(\vec{O})$, ce qui montre que l'on a : $\bigvee_{1\le i\le m+n} \neg R_1(\neg\theta_i(\vec{O}))$.
On ne peut pas avoir $i \in [m+1,m+n]$ car sinon on n'aurait pas :

$$\mathcal{A} \models \neg R_{k_i}(\theta_i)\ [a,\vec{f}].$$

CS : D'après (1) à (n) il existe $(P_i)_{m+1\le i\le m+n}$, P_i ensemble de moins de k_i nombres premiers tel que : $p \in P_i \to (\exists x\ \theta_i)^p$, et tel que pour $p \in \mathbb{P} \setminus \big(\bigcup_{m+1\le i\le m+n} P_i\big)$, on a $\big(\bigvee_{1\le i\le m} \exists x\ \theta_i\big)^p$ (par l'absurde).

D'après ψ', il existe $(P'_i)_{1\le i\le m+n}$, les P'_i étant disjoints deux à deux, P'_i a exactement k_i éléments et pour $p \in P'_i$, on a : $(\exists x\ \theta_i)^p$.

Alors, on construit x_o de la façon suivante, grâce au théorème III T2 :

- pour $i \in [m+1,m+n]$, pour $p \in P_i$ et pour $k_i - |P_i|$ éléments de P'_i on prend : $V(p,x_o) = \mu\, x(\theta_i(x))$;

- pour $i \in [1,m]$, pour $p \in P'_i$ on prend : $V(p,x_o) = \mu\, x(\theta_i(x))$;

- pour $p \mid f_1 . \ldots . f_p$ et non encore considéré :

$$V(p,x_o) = \mu\, x(\bigvee_{1\le i\le m} \theta_i(x)) ;$$

- pour les autres p : $V(p,x_o) = 0$. Alors cet x_o convient. □

Remarque.- Toute formule ϕ de L" est également M"-équivalente à une combinaison booléenne de formules du type $R_k(\theta)$, car M"-équivalente à une formule de L.

Corollaire.- La théorie M est complète et décidable.

Démonstration.- La théorie M" étant une extension par définition de M il suffit de raisonner sur M". Or lorsque ϕ est un énoncé on est ramené, de façon effective, à une combinaison booléenne de formules du type $R_k(\theta)$ avec θ énoncé ; d'après P3, $R_k(\theta)$ est vrai si, et seulement si, est vrai dans la théorie de l'addition, or cette dernière théorie est complète et décidable, d'où le résultat. □

5.- LA THEORIE DE LA MULTIPLICATION N'EST PAS FINIMENT AXIOMATISABLE

T4.- La théorie de la multiplication n'est pas finiment axiomatisable.

Démonstration.- Cela provient essentiellement du fait que la théorie de l'addition n'est pas finiment axiomatisable (Cf. [PR] ou[FR]).

En effet, supposons que cette théorie soit finiment axiomatisable, alors ce nombre fini d'axiomes (en fait leur conjonction) serait conséquence d'un nombre fini d'axiomes exhibés ci-dessus, et en particulier d'un nombre fini d'axiomes de divisibilité $A7^n$. Soit N le plus grand entier n tel que $A7^n$ soit nécessaire (avec, éventuellement, N = 1). Pour $i \in \mathbb{N}$, considérons la structure $\mathcal{A}_i = (A_i,+)$ avec :

$A_i = \{(x,y) \in Q^+ \times \mathbb{Z} / (x = \frac{a}{\mathbb{N}} \text{ avec } a \in \mathbb{N}) \text{ et } (x = 0 \to y \in \mathbb{N})\}$

$(x,y) + (x',y') = (x+x', y+y')$ (avec les additions habituelles dans Q et $\mathbb{Z}$) .

Posons : $\mathcal{A} = \bigoplus_{i \in \mathbb{N}} \mathcal{A}_i$. Alors $\mathcal{A}$ est un modèle de tous les axiomes autres que les axiomes de divisibilité $A7^n$ pour $n > N$. □

C.- ELIMINATION DES QUANTIFICATEURS

CARACTERISTION DES TYPES

1.- PREMIERE ELIMINATION DES QUANTIFICATEURS

D1.- Pour $n \in \mathbb{N}^*$ on pose E_n ("a au moins n éléments") la relation unaire suivante :

$$\exists\, p_1 \ldots \exists\, p_n \left(\bigwedge_{1 \le i < j \le n} p_i \neq p_j \wedge \bigwedge_{1 \le i \le n} (\mathbb{P}(p_i) \wedge p_i \mid x) \right).$$

T1.- (Elimination des quantificateurs pour la théorie M)

La théorie M^o de langage $L^o = (.,1,I,T,(SP_n)_{n\in\mathbb{N}},(E_k)_{k\in\mathbb{N}^*})$, extension par définition évidente de M, élimine les quantificateurs.

Démonstration.- o D'après le théorème BT3, toute formule ϕ de L^o est M^o-équivalente à une combinaison booléenne de formules du genre $R_k(\theta)$. Il résulte alors de ce que la théorie de l'addition de langage $(+,(\equiv_n)_{n\in\mathbb{N}},0,1)$ élimine les quantificateurs, de la mise sous forme normale et de la distributivité des quantificateurs existentiels par rapport à la disjonction, que les formules θ des $R_k(\theta)$ peuvent être prises comme conjonction de formules de la forme : $t \equiv_n t'$, avec t, t' termes de (.,I,1).

o Soit $\theta = \bigwedge_{1\le i\le k} \theta_i$ avec θ_i de la forme : $t_i \equiv_{n_i} t'_i$.

Premier cas.- Pour tout i de [1,k] on a : $t_i(1,\ldots,1) \equiv_{n_i} t'_i(1,\ldots,1)$. Alors $R_k(\theta)$ est vrai dans M^o, car il y a une infinité de nombres premiers ne divisant aucun des paramètres, et on a, par exemple : $R_k(\theta) \leftrightarrow \neg E_1(1)$.

Deuxième cas.- Sinon pour tout i de [1,k] posons : $t''_i = SP_{n_i}(t_i,t'_i)$, puis : $t = t''_1 \wedge \ldots \wedge t''_k$.

(c'est-à-dire : $T(t''_1,T(t''_2,\ldots,T(t''_{k-1},t''_k)\ldots))$). Alors on a : $R_k(\theta) \leftrightarrow E_k(t)$. D'où le résultat. □

Remarque.- Nous venons de voir que M^o élimine les quantificateurs, en particulier les relations définies jusqu'ici s'expriment dans le langage L^o ; vérifions-le :

- $x \mid y \leftrightarrow T(SP_1(x,y),x) = x$;
- $\mathbb{P}(x) \leftrightarrow (Ix = x^2 \wedge E_1(SP_o(Ix,x^2)) \wedge \neg E_2(SP_o(Ix,x^2)))$;
- $PR(p,x) \leftrightarrow (\mathbb{P}(p) \wedge T(p,x) = x)$.

De plus, on a : $V(p,x) = T(p,x)$ (en fait, on n'a plus l'égalité si p n'est pas premier, mais ce n'est pas important).

2.- LA COMBINATOIRE SOUS-JACENTE A LA THEORIE DE LA MULTIPLICATION

D2.- 1°. On dit qu'un entier x est un ensemble fini de nombre premiers et on note Fin(x) ssi pour tout p de $\mathbb{P}$ on a : $V(p,x) = 1$ ou p, i.e. : $x = SP_o(x,x)$.

2°. A tout entier x on associe l'ensemble fini de nombres premiers associé, noté F(x), et défini par : $F(x) = SP_o(x,x) (= \prod_{p \mid x} p)$.

3°. On définit l'union de x et y (tels que Fin(x) et Fin(y)), et on note $x \cup y$, par $x \cup y = F(x \cdot y)$.

4°. On définit l'intersection de x et y (tels que Fin(x) et Fin(y)), et on note $x \cap y$, par $x \cap y = T(x,y)$.

5°. On définit la différence de x et y (tels que Fin(x) et Fin(y)), et on note $x \setminus y$, par $x \setminus y = \frac{x}{T(x,y)}$.

Remarque.- On a, pour p premier, $V(p,x\setminus y) = \begin{cases} p & \text{si } p \mid x \text{ et } p \nmid y \\ 1 & \text{sinon.} \end{cases}$

Notation.- Dans la suite on notera $\underline{\lambda}$ le langage $(\cup,\cap,\setminus,(E_k)_{k\in\mathbb{N}^*})$

D3.- Pour $(s_1,\ldots,s_n) \in \{-1,1\}^n \setminus \{(-1,\ldots,-1)\}$ on définit $y = s_1x_1 \cap \ldots \cap s_nx_n$ par $z = \bigcap_{\substack{1\le i\le n \\ s_i=1}} x_i$, $z' = \bigcup_{\substack{1\le i\le n \\ s_i=-1}} x_i$, $y = z\setminus z'$.

3. CARACTERISATION DES n-TYPES DE LA THEORIE DE LA MULTIPLICATION

D4.- On appelle ensemble fini primitif définissable à partir de $x_1,\ldots,x_n$ un terme de la forme $SP_k(t(x_1,\ldots,x_n),t'(x_1,\ldots,x_n))$ avec $k \in \mathbb{N}$, t et t' n-termes du langage (.,I,1).

T2.- (Deuxième élimination des quantificateurs)

Toute formule $\phi(x_1,\ldots,x_n)$ de L est équivalente à une formule $\Phi(Y_1,\ldots,Y_p)$ où Φ est une formule de λ et les Y_i des ensembles finis primitifs définissables à partir de $x_1,\ldots,x_n$.

Démonstration.- o D'après l'élimination des quantificateurs, on peut supposer que ϕ est une formule du langage L^o. Une formule de ce langage est une combinaison booléenne de formules de la forme : $t = t'$ ou $E_k(t)$; mais la première forme est équivalente à :

$$\neg E_1(SP_1(It,t') \cdot SP_1(It',t)) ,$$

on n'a donc à ne considérer que des formules atomiques de la seconde forme.

o Lemme.- Pour t, t' n-termes du langage $(.,1,I,T,(SP_k)_{k\in\mathbb{N}})$, $SP_m(t,t')$ est équivalent à un λ-terme d'ensembles finis primitifs définissables à partir de $x_1,\ldots,x_n$.

Démonstration.- Par récurrence sur les complexités de t et t'. On a, à équivalence près : $t = I^p x_1^{\alpha_1} \ldots x_n^{\alpha_n} \cdot y_1^{\beta_1} \ldots y_r^{\beta_r}$ et $t' = I^q x_1^{\alpha'_1} \ldots x_n^{\alpha'_n} \cdot z_1^{\gamma_1} \ldots z_s^{\gamma_s}$ avec les y_i et les z_j de la forme SP(,) ou T(,).

- Si r = s = 0, on est en présence d'un terme primitif.

  Si $r \neq 0$, posons $u' = y_r$, $u = \frac{t}{u'}$.

- Si $u' = T(v,v')$, on a :

$$SP_k(t,t') = \pi\{p \in \mathbb{P} / p|t'.u.T(v,v') \text{ et } V(p,u) + V(p,T(v,v')) \equiv_k V(p,t')\}$$

$$= \pi\{p \in \mathbb{P} / (p|v \text{ et } p|v' \text{ et } V(p,u) + V(p,v') \equiv_k V(p,t'))$$

$$\text{ou } ((p \nmid v \text{ ou } p \nmid v') \text{ et } p|t'.u \text{ et } V(p,u) \equiv_k V(p,t'))\}$$

$SP_k(t,t') = (SP_k(u\,.\,v',t') \cap F(v)) \cup (SP_k(u,t') \setminus (F(v) \cup F(v')))$

- Si $u' = SP_m(v\,,\,v')$ on a :

$SP_k(t,t') = \pi\{p \in \mathbb{P} / p|t'.u.SP_m(v,v')$ et $V(p,u) + V(p,SP_m(v,v')) \equiv_k V(p,t')\}$

$= \pi\{p \in \mathbb{P} / (p|t'.u.SP_m(v,v')$ et $p|v.v'$ et $V(p,v) \equiv_m V(p,v')$

et $V(p,u) + 1 \equiv_k V(p,t'))$

ou $(p|t.u'$ et $(p \nmid v.v'$ ou $V(p,v) \not\equiv_k V(p,v'))$ et $V(p,u) \equiv_k V(p,t'))\}$

$= (SP_m(v,v') \cap SP_k(Iu,t')) \cup (SP_k(u,t') \setminus SP_m(v,v'))$

- Analogue si $s \neq 0$. □

o Démontrons par récurrence sur la complexité du terme t que $E_m(t)$ est équivalente à une formule de la forme indiquée.

- Si $t = 1$ ou $t = x$ alors $E_m(t)$ est équivalente à $E_m(SP_o(t,t))$.

- Si $t = t'.t"$, alors $E_m(t)$ est équivalente à $E_m(F(t') \cup F(t"))$ et $F(u)$ est un terme primitif d'après le lemme.

- Si $t = It'$ alors $E_m(t)$ est équivalente à $E_m(t')$.

- Si $t = T(t',t")$, alors $E_m(t)$ est équivalente à $E_m(F(t') \cap F(t"))$ et on applique le lemme.

- Si $t = SP_k(t',t")$ alors cela résulte immédiatement du lemme. □

Remarque.- Les n-termes de $(.,I,1)$ sont, à équivalence près, de la forme : $I^k x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ avec $k,\alpha_1,\ldots,\alpha_n \in \mathbb{N}^*$.

Corollaire.- (Caractérisation des n-types). Les n-uplets $(a_1,\ldots,a_n)$ et $(b_1,\ldots,b_n)$ ont même type si, et seulement si, ils vérifient les mêmes formules de la forme :

$$E_m(s_1 Y_1 \cap \ldots \cap s_k Y_k) \ ,$$

avec $n,k \in \mathbb{N}^*$, $(s_1,\ldots,s_k) \in \{-1,1\}^k \setminus \{(-1,\ldots,-1)\}$, Y_i ensemble fini primitif définissable à partir de $x_1,\ldots,x_n$.

4.- CAS DES 1-TYPES

D5. Pour $k,r,n \in \mathbb{N}$ tels que : $k \neq 0$ et $0 \leq r < k$, on note :

- $VE_n(x) = \pi\{p \in \mathbb{P} / V(p,x) = n\}$ (valuation égale à n)

- $VC_{k,r}(x) = \pi\{p \in \mathbb{P} / r \equiv_k V(p,x)\}$ (valuation congrue à r modulo k).

T3. (Caractérisation des 1-types)

a et b ont même type si, et seulement si, ils vérifient les mêmes formules de la forme : $E_n(s_1Y_1 \cap \ldots \cap s_pY_p)$, avec $n,p \in \mathbb{N}^*$, $(s_1,\ldots,s_p) \in \{-1,1\}^p \setminus \{(-1,\ldots,-1)\}$, Y_i de la forme $F(x)$, $VE_k(x)$ ou $VC_{k,r}(x)$.

Démonstration.- D'après T2, il suffit de montrer que les termes de la forme $SP_k(I^mx^n, I^rx^s)$ sont des combinaisons (à l'aide de $\cap$, $\cup$ et $\setminus$) de $F(x)$, $VE_m(x)$ et $VC_{p,q}(x)$, ce que l'on voit facilement à l'aide de quelques manipulations. □

D.- LA THEORIE DE LA MULTIPLICATION CONSEQUENCE DE $I\Sigma_o$

1.- La théorie $I\Sigma_o$

La théorie $I\Sigma_o$ (cf. [PA] ou[Mc]) est la théorie du premier ordre de langage $(S,+,.,\leq,0)$, et dont les axiomes propres sont ceux de l'arithmétique de Péano avec le schéma d'axiomes d'induction restreint aux Σ_o-formules.

D1.- L'ensemble des Σ_o-formules (ou formules à quantification bornée) est le plus petit sous-ensemble de formules du langage ci-dessus contenant les formules atomiques et clos par la négation, la disjonction et les quantifications bornées :

- $(\exists x \leq y)\Phi \longleftrightarrow \exists x(x \leq y \wedge \Phi)$

- $(\forall x \leq y)\Phi \longleftrightarrow \forall x(x \leq y \rightarrow \Phi)$.

D2.- La théorie $I\Sigma_o$ est la théorie du premier ordre de langage le langage ci-dessus et dont les axiomes propres sont les suivants :

- $\forall x\ (Sx \neq 0)$
- $\forall x \forall y\ (Sx = Sy \rightarrow x = y)$
- $\forall x\ (x + 0 = x)$
- $\forall x \forall y\ (x + Sy = S(x + y))$
- $\forall x\ (x . 0 = 0)$
- $\forall x \forall y\ (x . (Sy) = x . y + x)$
- $\forall x \forall y\ (x \leq y \longleftrightarrow \exists z\ (y = z + x))$
- Pour $\phi(x,y_1,\ldots,y_n)$ $(n+1)$-Σ_o-formule on a :

$$\forall y_1 \ldots \forall y_n((\phi(0,y_1,\ldots,y_n) \wedge \forall x(\phi(x,y_1,\ldots,y_n) \rightarrow \phi(Sx,y_1,\ldots,y_n))) \rightarrow \forall x\ \phi(x,y_1,\ldots,y_n))$$

Le développement de l'arithmétique élémentaire avec les axiomes

de Péano (informels) correspond en fait jusqu'à un certain point assez avancé à la théorie $I\Sigma_0$. Plus exactement, il en est ainsi pour les propriétés suivantes :

- Associativité , existence d'un élement neutre (0), commutativité et régularité de l'addition ;

- tout entier non nul est successeur ;

- 0 est le seul élement inversible pour l'addition ;

- 1 est élément neutre, 0 est absorbant pour la multiplication ;

- distributivité à droite de la multiplication par rapport à l'addition ;

- commutativité, associativité, intégrité, "régularité" de la multiplication ;

- 1 seul élement inversible pour la multiplication ;

- $\leq$ est une relation d'ordre total ;

- compatibilité des opérations et de la relation d'ordre ;

- l'odre est archimédien et discret (il n'y a pas d'entiers entre x et Sx) ;

- les résultats sur la soustraction ;

- les procédés de récurrence habituels pour les Σ_0-formules (induction complète, récurrence à partir de x_0, induction complète à partir de x_0, principe du bon ordre, principe de la borne supérieure) ;

- l'existence de la division euclidienne ;

- la relation de divisibilité est une relation d'ordre moins fine que la relation d'inégalité ;

- tout entier différent de 1 est divisible par un nombre entier ;

$\mathbb{Z}$ - par contre, a priori, le théorème d'Euclide sur l'existence d'une infinité de nombres premiers ($\forall x \exists p (x < p \wedge \mathbb{P}(p))$) n'est pas un

théorème de la Σ_o-induction (problème ouvert) ;

- le théorème de Bezout sur les nombres premiers entre eux

$$\forall x \forall y ((x \wedge y = 1) \leftrightarrow \exists u \exists v (u . x - v . y = 1))$$

- le théorème de Gauss ; l'existence du pgcd

$$\forall x \forall y \forall z ((x \mid y . z \text{ et } x \wedge y = 1) \rightarrow x \mid z) ;$$

$\mathbb{Z}$ - par contre on ne peut pas définir l'exponentiation (et donc la valuation sous la forme classique).

En particulier, on voit que la théorie de l'addition de Presburger est conséquence de la Σ_o-induction.

2.- LE DEVELOPPEMENT SPECIFIQUE

Nous allons maintenant établir quelques autres théorèmes de la Σ_o-induction, ne reprenant pas des théorèmes classiques de l'arithmétique élémentaire (tout au moins sous leur forme originale), mais permettant de démontrer que la théorie de la multiplication est conséquence de la Σ_o-induction.

d1.- On définit, par récurrence extérieure sur $n \in \mathbb{N}$, le terme x^n par : $x^o = 1$ et $x^{n+1} = x^n . x$. On parlera de puissance extérieure.

Remarque.- Il ne faut pas confondre la puissance extérieure que nous venons de définir avec la puissance intérieure x^y, avec x, y variables, qu'il n'est pas possible de définir dans la Σ_o-induction.

P1^n.- (Pour $n \in \mathbb{N}^*$:) $\forall x (x^n = 0 \rightarrow x = 0)$.

Démonstration.- Par récurrence extérieure sur n en utilisant l'intégrité. □

P2^n.- (Pour $n \in \mathbb{N}^*$:) 1°.- $\forall x \forall y (x \leq y \rightarrow x^n \leq y^n)$

2°.- $\forall x \forall y (x < y \rightarrow x^n < y^n)$.

Démonstration.- Par récurrence extérieure sur n en utilisant la compatibilité de . par rapport à ≤ .

P3^n.- (Pas de torsion) (Pour $n \in \mathbb{N}^*$:) $\forall x \forall y (x^n = y^n \to x = y)$.

Démonstration.- Premier cas : $x = 0$ alors $x^n = 0$ (par récurrence extérieure), d'où $y^n = 0$, donc $y = 0$ (d'après P1). Ainsi $x = y$.

Deuxième cas : $x \neq 0$. Alors on a, par exemple, $x \geq y$ et puisque $x^n = y^n$, alors :

$$0 = x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$$

(récurrence extérieure classique). Puisque $x \neq 0$, alors $x^{n-1} \neq 0$ (P1) d'où : $x^{n-1} + \ldots + y^{n-1} \neq 0$, et, par intégrité, $x - y = 0$, soit $x = y$. □

P4.- (Existence d'une infinité de nombres premiers).
$\forall x (x > 2 \to \exists p (\mathbb{P}(p) \wedge p < x \wedge p \nmid x)$

Démonstration.- On a $x = y + 1$, avec $y > 1$. Soit p un nombre premier divisant y, alors $p \nmid x$. □

Corollaire.- $\forall x (x \neq 0 \to \exists p (\mathbb{P}(p) \wedge p \nmid x))$

Démonstration.- Si $x = 1$ ou 2 il suffit de prendre $p = 3$. Sinon cela résulte de P4. □

Remarque.- Ce théorème dit beaucoup moins que le théorème d'Euclide. Il y a bien une infinité standard de nombres premiers, mais on ne dit rien sur une infinité au sens du modèle (c'est-à-dire un ensemble non borné).

d2.- x est un nombre p-primaire, et on note PR(p,x), ssi :
$\mathbb{P}(p) \wedge \forall q ((\mathbb{P}(p) \wedge q \neq p) \to q \nmid x)$.

Remarque.- PR(p,x) se définit aussi par la Σ_0-formule suivante :
$\mathbb{P}(p) \wedge \forall q ((q \leq x \wedge q \mid x \wedge \mathbb{P}(p)) \to q = p)$.

P5.- (| total sur PR(p,.))
$\forall p \forall x \forall y ((PR(p,x) \wedge PR(p,y)) \rightarrow (x \mid y \vee y \mid x))$

Démonstration.- On a $xy \neq 0$. Posons $d = pgcd(x,y)$, $x = dx'$, $y = dy'$. Si $x' \neq 1$ alors il existe un nombre premier q divisant x', qui ne peut être que p, ainsi $p \mid x'$. De même si $y' \neq 1$ on a $p \mid y'$. On ne peut donc pas avoir $x' \neq 1$ et $y' \neq 1$, puisque $x' \wedge y' = 1$.
Si,par exemple, $x' = 1$ alors $x = d$, $y = xy'$, d'où $x \mid y$. □

P6.- (Justification de d3)
$\forall x \forall p ((\mathbb{P}(p) \wedge x \neq 0) \rightarrow \exists ! y (PR(p,y) \wedge y \mid x \wedge$
$\forall z ((PR(p,z) \wedge z \mid x) \rightarrow z \mid y)))$

Démonstration.- L'unicité est évidente, démontrons l'existence. Posons : $F(z) = (PR(p,z) \wedge z \mid x \wedge z \leq x)$. On a $\exists z F(z)$ en prenant $z = 1$. Soit alors y le plus grand entier tel que F(z). On a PR(p,y) et $y \mid x$. Si $z \mid x$ et PR(p,z) alors $z \leq x$ et, d'après P5, $z \mid y$ ou $y \nmid z$; par définition de y on a : $z \mid y$. □

d3.- Le y dont l'existence et l'unicité sont affirmées dans P6, se note V(p,x) et s'appelle la valuation p-adique de x.

Remarque.- Contrairement à la définition classique, ici la valuation p-adique n'est pas le coefficient de p dans la factorisation de x en facteurs premiers (qui ne peut pas être définie) mais la puissance de p par ce coefficient.

P7.- (Caractérisation de la valuation)
$\forall x \forall y \forall p(\mathbb{P}(p) \rightarrow (y = V(p,x) \leftrightarrow \exists z (x = yz \wedge PR(p,y) \wedge p \nmid z)))$

Démonstration.- CN. Soit $y = V(p,x)$ alors on a PR(p,y) et $y \mid x$ donc il existe z tel que : $x = yz$. Si $p \mid z$ alors on a PR(p,py), $py \mid x$ et $py \nmid y$, contradiction avec la définition de la valuation.

CS. S'il existe z tel que $x = yz$, PR(p,y) et $p \nmid z$, alors on a PR(p,y) et $y \mid x$, d'où $y \mid V(p,x)$, il existe donc u tel que $V(p,x) = uy$, d'où $u \mid z$ et $p \nmid z$ d'où $u = 1$ et $y = V(p,x)$. □

P8.- (Linéarité de la valuation)

$\forall x \forall y \forall p\ (\mathbb{P}(p) \rightarrow V(p,x.y) = V(p,x).V(p,y))$

Démonstration.- Soient $x_o = V(p,x)$, $y_o = V(p,y)$. On a : $x = x'x_o$, $y = y'y_o$ avec $p \nmid x'$ et $p \nmid y'$ (d'après P7), d'où $xy = x'y'x_oy_o$ avec $PR(p,x_o.y_o)$, $p \nmid x'y'$ (Théorème de Gauss), d'où, d'après P7, $V(p,xy) = x_oy_o = V(p,x).V(p,y)$. □

P9.- $\forall x \forall y((y < x \rightarrow \exists p\ (\mathbb{P}(p) \wedge V(p,y) < V(p,x))$

$\wedge\ ((y < x \wedge y \nmid x) \rightarrow \exists p(\mathbb{P}(p) \wedge V(p,x) < V(p,y)))$

Démonstration.- Premier cas $y \mid x$. On a $x = uy$ avec $u \neq 1$ car $x \neq y$. Il existe un nombre premier divisant u d'où, d'après la linéarité (P8) :

$V(p,x) = V(p,u).V(p,y)$ avec $V(p,u) \neq 1$, donc $V(p,y) < V(p,x)$.

Deuxième cas $y \nmid x$. Posons $d = pgcd(x,y)$, $x = dx'$, $y = dy'$. On a $x' \neq 1$ car $x \nmid y$, et $y' \neq 1$ car $y \nmid x$.
Il existe un nombre premier p divisant x', et donc ne divisant pas y' car x' et y' sont premiers entre eux, d'où : $V(p,y) < V(p,x)$. Il existe de même un nombre premier q divisant y', et donc ne divisant pas x', d'où : $V(q,x) < V(q,y)$. □

Corollaire 1.-(Division et valuation)

$\forall x \forall y\ (y \mid x \longleftrightarrow \forall p(\mathbb{P}(p) \rightarrow V(p,y) \mid V(p,x)))$

Démonstration.- CN : Ceci provient de la linéarité de la valuation.

CS : Si $y \nmid x$ et $y < x$ alors, d'après P9, il existe un nombre premier p tel que : $V(p,x) < V(p,y)$ et donc $V(p,y) \nmid V(p,x)$.

Si $x < y$ alors, d'après P9, il existe un nombre premier p tel que $V(p,x) < V(p,y)$ et donc : $V(p,y) \nmid V(p,x)$. □

Corollaire 2.- (x est caractérisé par ses valuations)

$\forall x \forall y\ (x = y \longleftrightarrow \forall p(\mathbb{P}(p) \rightarrow V(p,x) = V(p,y)))$.

Démonstration.- CN : Evident.

CS : D'après le corollaire 1 et l'antisymétrie de $|$.

P10.- (Divisibilité) (Pour $n \in \mathbb{N}^*$)

$\forall x\ (x \neq 0 \to \exists y\ \exists z\ (x = y^n . z \wedge \forall y'\ \forall z'\ (x = y'^n . z' \to z \mid z')))$

Démonstration.- Considérons la formule : $F(u) = \exists v\ (v \leq x \wedge x = u^n . v)$. On a $\exists u\ F(u)$ (en prenant $u = 1$, $v = x$) et $(F(u) \to u \leq x)$. Soit y le plus grand u tel que F(u). Alors il existe un et un seul z tel que $x = y^n . z$.

Soient y', z' tels que : $x = y'^n . z'$.

o Soit p un nombre premier, on a : $\underline{V(p,z) \mid V(p,z')}$.

Sinon, on aurait $V(p,z') \mid V(p,z)$ d'après P5, posons $z''_o = \frac{V(p,z)}{V(p,z')}$ alors, on aurait : $V(p,y)^n . z''_o = V(p,y')^n$ avec $p \mid z''_o$.
On a soit $V(p,y) \mid V(p,y')$, soit $V(p,y') \mid V(p,y)$ d'après P5.
Si $V(p,y) \mid V(p,y')$ alors soit $y''_o = \frac{V(p,y')}{V(p,y)}$, on a : $y''^n_o . z''_o = 1$, d'où $z''_o = 1$, en contradiction avec le fait que $p \mid z''_o$.
Si $V(p,y') \mid V(p,y)$ alors soit $y''_o = \frac{V(p,y)}{V(p,y')}$, on a : $z''_o = y''^n_o$ avec $y''_o \neq 1$ (car $p \mid z''_o$) donc y ne serait pas le plus grand u tel que F(u).

o Ainsi, d'après P9 Corollaire 1, on a $z \mid z'$, ce qu'on voulait. □

P11.- (Justification de d4)

$\forall x\ (x \neq 0 \to \exists y\ \forall p(\mathbb{P}(p) \to ((p \mid x \to V(p,y) = p) \wedge (p \nmid x \to V(p,y) = 1)))$

Démonstration.- Par induction complète sur x à partir de 1 pour la formule :

$F(x) = \exists y\ (y \leq x \wedge \forall p((p \leq x \wedge \mathbb{P}(p)) \to ((p \mid x \to V(p,y) = p) \wedge (p \nmid x \to V(p,y) = 1))))$

Si $x = 1$, il suffit de prendre $y = 1$.

Si $x \neq 1$ il existe un nombre premier p divisant x. Posons $x' = \frac{x}{p}$ alors $x' < x$, donc il existe y' associé à cet x' répondant à la question. Si $p \mid x'$ alors posons $y = y'$. Sinon posons $y = p \cdot y'$. Cet y répond à la question. □

d4.- Le y dont l'existence est affirmée par P11 (et qui est unique) s'appelle l'ensemble fini de x et se note F(x).

Corollaire.- (Incrémentation)

$\forall x \exists y \forall p(\mathbb{P}(p) \rightarrow ((p \mid x \rightarrow V(p,y) = p \cdot V(p,x)) \wedge (p \nmid x \rightarrow V(p,y) = 1)))$

Démonstration.- Il suffit de prendre $y = x \cdot F(x)$. □

Notation.- Cet y sera noté Ix.

P12.- (Troncage)

$\forall x \forall y (y \neq 0 \rightarrow \exists z \forall p(\mathbb{P}(p) \rightarrow ((p \mid x \rightarrow V(p,z) = V(p,y)) \wedge (p \nmid x \rightarrow V(p,z) = 1))))$

Démonstration.- o Si $x = 0$ il suffit de prendre $z = y$.

o Soit x fixé non nul. Posons :

$F(y) = (y \neq 0 \rightarrow \exists z(z \mid y \wedge \forall p((p \mid y \wedge \mathbb{P}(p)) \rightarrow ((p \mid x \rightarrow V(p,z) = V(p,y)) \wedge (p \nmid x \rightarrow V(p,z) = 1)))))$

Montrons par induction complète sur y que : $\forall y\ F(y)$.
Supposons montré $\forall t\ (t < y \rightarrow F(t))$ et montrons $F(y)$.
Si $y = 1$, il suffit de prendre $z = 1$.
Si $y \neq 1$ alors il existe un nombre premier q divisant y. Posons $y' = \frac{y}{q}$. Alors $y' < y$ donc, par hypothèse de récurrence, il existe z' associé à y' répondant à la question. Si $q \nmid x$ posons $z = z'$. Si $q \mid x$ et $q \mid y'$ posons $z = z' \cdot q$. Sinon posons $z = z' \cdot V(q,y)$. Alors ce z répond à la question.

o Le z ainsi associé à y est le z cherché dans l'énoncé. □

d5.- Pour un entier n on pose $x \equiv_n y$ ssi $\exists\, z\ (y = z^n . x)$

$P13^n$.- (Séparation) (Pour $n \in \mathbb{N}$:)

$\forall\, x\, \forall\, y\ (xy \neq 0 \to \exists\, z\, \forall\, p(\mathbb{P}(p) \to$

$$(((V(p,x) \equiv_n V(p,y) \wedge p \mid xy) \to V(p,z) = p)$$

$$\wedge\ ((V(p,x) \not\equiv_n V(p,y) \vee p \nmid xy) \to V(p,z) = 1))))$$

Démonstration.- Supposons x fixé non nul et posons :

$F(y) = (y \neq 0 \to \exists\, z(z \mid xy \wedge \forall\, p((p \mid xy \wedge \mathbb{P}(p)) \to$

$$((V(p,x) \equiv_n V(p,y) \to V(p,z) = p)$$

$$\wedge\ (V(p,x) \not\equiv_n V(p,y) \to V(p,z) = 1)))))$$

Alors, il suffit de montrer $\forall\, x\ F(y)$. Faisons-le par induction complète sur y. Supposons montré $\forall\, t\ (t < y \to F(t))$ et montrons F(y).
Si y = 1 il suffit de prendre z = 1.
Si $y \neq 1$ àlors il existe un nombre premier q divisant y. Posons $y' = \frac{y}{q}$.
Alors y' < y donc il existe un z' associé à y' répondant à la question, d'après l'hypothèse de récurrence.

- Si $q \nmid xy'$ alors on a : $V(q,x) = V(q,z') = 1$, $V(q,y) = q$.

Si n = 1 posons $z = q . z'$, sinon $z = z'$.

- Si $q \mid xy'$ alors $V(q,y) = q . V(q,y')$.

Si $V(q,x) \equiv_n V(q,y')$: si n = 1 posons $z = z'$, sinon $z = \frac{z'}{q}$.
Si $V(q,x) \not\equiv_n V(q,y')$: si $V(q,x) \equiv_n V(q,y)$ posons $z = qz'$, sinon $z = z'$.

Alors ce z répond à la question. □

T.- La théorie de la multiplication M est conséquence de la Σ_o-induction.

Démonstration.- Il suffit de montrer que les axiomes de M sont déduits

de $I\Sigma_o$. Or cela résulte du développement ci-dessus de la Σ_o-induction: l'associativité, l'existence de l'élément neutre, la commutativité, la régularité, la positivité (1 seul élement inversible) sont classiques ; on a démontré la non-torsion en $P3^n$, la divisibilité en P10, l'existence de nombres premiers en P4, | total sur PR(p,) en P5, l'existence des valuations en P6, la caractérisation d'un élément par ses valuations en P9, Corollaire 2, la linéarité de la valuation en P8, la division en P9, Corollaire 1, l'incrémentation en P11, Corollaire, le troncage en P12 et enfin la séparation en $P13^n$. □

E.- ELIMINATION DU QUANTIFICATEUR DE RAMSEY POUR LA MULTIPLICATION DES ENTIERS NATURELS NON NULS

INTRODUCTION.- Dans ce qui suit, nous ne considérons que le modèle standard $(\mathbb{N},+,.,0,1)$ de l'arithmétique. Le quantificateur de Ramsey Q^2 lie deux variables libres. Si ϕ est une formule du langage $(+,.,0,1,Q^2)$, on dit que $Q^2 x\, y\, \phi(x,y)$ est vraie si, et seulement si, il existe un ensemble infini d'entiers naturels X, dit ensemble témoin, tel que $\phi(a,b)$ est vrai pour tout a, b de X, avec $a \neq b$ (Cf. [SS] ou [MA]).

Schmerl et Simpson ([SS]) ont montré que le quantificateur de Ramsey peut être éliminé de la théorie de l'addition des entiers naturels avec ce quantificateur, i.e. de $(\mathbb{N},+,Q^2)$, en utilisant l'élimination des quantificateurs de la théorie des entiers naturels de Presburger. Autrement dit, ils ont démontré le théorème suivant :

"Etant donné une formule du langage $(+,Q^2)$, on peut trouver effectivement une formule du seul langage $(+)$, équivalente pour la structure $(\mathbb{N},+,Q^2)$."

Nous allons montrer que ce résultat est également vrai pour la théorie de la multiplication, en nous servant de ce résultat ainsi que de l'élimination des quantificateurs que nous venons de donner pour la théorie de la multiplication.

Théorème.- Toute formule du langage $(.,Q^2)$ est, modulo la théorie de $(\mathbb{N},.,Q^2)$, équivalente à une formule du seul langage $(.)$.

Démonstration.- o D'après le résultat que nous venons de rappeler et la mise sous forme normale, il suffit de montrer pour une formule du type :

$$Q^2 x\, y \bigvee \bigwedge \pm R_k(\theta).$$

De plus, d'après le théorème de Ramsey, on a :

$$Q^2 x\, y \bigvee\!\!\!\!\bigwedge \pm R_k(\theta) \longleftrightarrow \bigvee\!\!\!\!\bigwedge Q^2 x\, y \pm R_k(\theta).$$

On note $\underline{S_k(\theta)}$ pour : $R_k(\theta) \wedge \neg R_{k+1}(\theta)$.

Remarquons que : $\neg R_{k+1}(\theta) \leftrightarrow \neg R_1(\theta) \vee S_1(\theta) \vee \ldots \vee S_k(\theta)$,

$$\text{et : } \neg R_1(\theta_1) \wedge \ldots \wedge \neg R_1(\theta_n) \longleftrightarrow \neg R_1(\theta_1 \vee \ldots \vee \theta_n).$$

Aussi suffit-il de le montrer pour une formule du type :

$$Q^2 x\, y\Big(\bigwedge_{1\le i\le n} R_{k_i}(\theta_i) \wedge \bigwedge_{1\le j\le m} S_{L_j}(\theta'_j) \wedge \neg R_1(\theta)\Big).$$

De plus, on peut prendre les θ_i, θ'_j, θ indépendantes (i.e. la conjonction de deux d'entre elles est contradictoire).

Puisque : $Q^2 x\, y \bigwedge\!\!\!\!\bigwedge \phi \to \bigwedge\!\!\!\!\bigwedge Q^2 x\, y\, \phi$, nous allons commencer par éliminer Q^2 pour les formules du type : $R_k(\theta)$, $S_k(\theta)$ et $R_1(\theta)$.

o <u>Lemme 1</u>.- $Q^2 x\, y\, R_k(\theta) \leftrightarrow (R_1(\exists\, x\, \exists\, y\, \theta(x,y,\vec{\delta}))$

$$\vee\, R_k(\exists\, x\, \theta(x,x,\vec{z}) \vee Q^2 x\, y\, \theta(x,y,\vec{z})))$$

<u>Démonstration</u>. <u>CN</u>. Supposons $Q^2 x\, y\, R_k(\theta)$ et soit X un ensemble témoin associé. Soit P' l'ensemble des nombres premiers divisant le produit des paramètres. Pour $x,y \in X$, $x \neq y$, il existe k nombres premiers p tels que : $\mathcal{A}_p \models \theta(V(p,x),V(p,y),V(p,\vec{z}))$. D'après les conditions ces nombres premiers p sont parmi P' ou alors on a : $\theta^p(V(p,x),V(p,y),\vec{\delta})$. D'où, d'après le théorème de Ramsey, il existe un sous-ensemble infini Y de X tel que :

- soit pour tout x,y de Y, avec $x \neq y$, on a : $\theta^p(V(p,x),V(p,y)\vec{\delta})$;

- soit il existe k nombres premiers $p_1,\ldots,p_k$ de P' tel que pour x,y de Y, avec $x \neq y$, on a : $\theta^{p_i}(V(p_i,x),V(p_i,y),V(p_i,\vec{z}))$ pour $1 \le i \le k$.

Dans le deuxième cas et pour $i \in [1,k]$ on a :

+ soit il existe $x,y \in Y$, $x \neq y$, avec $V(p_i,x) = V(p_i,y)$, d'où on a : $(\exists\, x\, \theta(x,x,\vec{z}))^{p_i}$;

+ sinon on a : $(Q^2 x\, y\ \theta(x,y,\vec{z}))^{p_i}$.

Dans le premier cas on a : $(\exists x \exists y\ \theta(x,y,\vec{0}))^{p}$.

CS.- - Si on a $R_k(\exists x\ \theta(x,x,\vec{z}) \vee Q^2 x\, y\ \theta(x,y,\vec{z}))$, soient $p_1,\ldots,p_k$ k nombres premiers correspondants, et pour $i \in [1,k]$ soit Y_i le singleton $\{y_i\}$ si on a $(\theta(y_i,y_i,\vec{z}))^{p_i}$, un ensemble témoin (pour la théorie de l'addition) sinon (puisqu'on a $Q^2 x\, y\ \theta^{p_i}(x,y,\vec{z})$).
Soit p un nombre premier différent de $p_1,\ldots,p_k$. Posons :
$X = \{x_n^o / n \in \mathbb{N}\}$, avec x_n défini par : $V(p_o,x_n) = n$

$V(p_i,x_i) \in Y_i$ pour $1 \leq i \leq k$

$V(p,x_n) = 0$ sinon.

Alors X est un ensemble témoin et on a $Q^2 x\, y\ R_k(\theta)$.

- Si on a $R_1(\exists x \exists y\ \theta(x,y,\vec{0}))$, soit $x_o,y_o \in \mathbb{N}$ tels que $\theta(x_o,y_o,\vec{0})$ dans la théorie de l'addition, P' l'ensemble fini des nombres premiers divisant les paramètres et $(p_i)_{i\in\mathbb{N}}$ une énumération de $\mathbb{P}\setminus P'$. Soit $X = \{x_n / n \in \mathbb{N}^*\}$ défini par : $V(p_o,x_n) = n$ et pour $m \in \mathbb{N}$:
si $i \in [m.2k + 1,\ m.2k + k]$ $V(p_i,x_n) = 0$ si $n < m$

$V(p_i,x_m) = x_o$

$V(p_i,x_n) = y_o$ si $m < n$

si $i \in [m\,2k + k + 1, m\,2k + 2k]$ $V(p_i,x_n) = 0$ si $n < m$

$V(p_i,x_m) = y_o$

$V(p_i,x_n) = x_o$ si $m < n$.

Alors X est un ensemble témoin, car pour $n,m \in \mathbb{N}^*$, $n < m$, on a :

pour $i \in [n\,2k + 1, n\,2k + k]$ $V(p_i,x_n) = x_o$, $V(p_i,x_m) = y_o$

$i \in [n\,2k + k + 1, n\,2k + 2k]$ $V(p_i,x_n) = y_o$, $V(p_i,x_m) = x_o$

d'où $R_k(\theta(x_n,x_m,\vec{z}))$ et $R_k(\theta(x_m,x_n,\vec{z}))$. □

Remarque.- On élimine bien ainsi le quantificateur de Ramsey Q^2, d'après le résultat de Schmerl et Simpson cité ci-dessus, car ce qui est à l'intérieur d'un R_k ne concerne que la théorie de l'addition.

o Lemme 2 .- $Q^2 x\, y\ \neg R_1(\theta) \longleftrightarrow$

$(\neg R_1(\theta(O,O,\vec{O})) \wedge \neg R_1(\neg(\exists x\, \neg\theta(x,x,\vec{z}) \vee Q^2 x\, y\, \neg\theta(x,y,\vec{z})))$

$\wedge R_1(Q^2 x\, y\, \neg\theta(x,y,\vec{z}) \vee \exists x(x \neq O \wedge \neg\theta(x,O,\vec{O}) \wedge \neg\theta(O,x,\vec{O}))))$.

Démonstration.- CN. + la première condition est évidente : si on avait $\theta(O,O,\vec{O})$ pour la théorie de l'addition, alors, puisque pour x,y donnés il existe un nombre premier p qui ne divise ni x, ni y, ni le produit des paramètres, on aurait : $\exists\, p \in \mathbb{P}\ (\theta(V(p,x),V(p,y),V(p,\vec{z})))$, ce qui serait en contradiction avec l'hypothèse.

+ On a : $Q^2 x\, y \neg R_1(\theta) \longleftrightarrow Q^2 x\, y(\forall\, p \in \mathbb{P})(\neg\theta)$.

Soit X un ensemble témoin. Pour $x,y \in X$, $x \neq y$, et $p \in \mathbb{P}$, on a : $\neg\theta(V(p,x),V(p,y),V(p,\vec{z}))$. A p fixé :

- si $\exists\, x,y \in Y$, $x \neq y$ et $V(p,x) = V(p,y)$, alors on a $(\exists\, x\, \neg\theta(x,x,\vec{z}))^p$;

- sinon on a : $(Q^2 x\, y\, \neg\theta(x,x,\vec{z}))^p$;

d'où la deuxième condition.

+ Soient X un ensemble témoin, $x_o \in X$, P' l'ensemble des nombres premiers divisant le produit de x_o et des paramètres :

- si $\{V(p,x)/p \in P',\ x \in X\}$ est infini alors, d'après le théorème de Ramsey, il existe $p_o \in P'$ tel que $\{V(p_o,x)/x \in X\}$ soit infini et on a : $\neg\theta(V(p_o,x),V(p_o,y)V(p_o,\vec{z}))$ pour $x,y \in X$, $x \neq y$, d'où on a : $R_1(Q^2 x\, y\, \neg\theta(x,y,\vec{z}))$.

- sinon il existe x avec $V(p,x) \neq O$ pour un $p \notin P'$ et on a :

$$\neg\theta(O,V(p,x),\vec{O}) \wedge \neg\theta(V(p,x),O,\vec{O})$$

d'où : $R_1(\exists x(x \neq O \wedge \neg\theta(O,x,\vec{O}) \wedge \neg\theta(x,O,\vec{O}))$, d'où la dernière condition.

CS.- Si on a : $R_1(Q^2 x\, y \neg\theta(x,y,\vec{z}))$, soit p_o un nombre premier tel que $(Q^2 x\, y \neg\theta(x,y,\vec{z}))^{p_o}$ et Y un ensemble témoin correspondant. Soit P' l'ensemble des nombres premiers divisant les paramètres. Pour $p \in P'$, soit Y_p un ensemble témoin si on a $(Q^2 x\, y \neg\theta(x,y,\vec{z}))^p$, soit $\{x_p\}$ si on a : $\neg\theta(x_p,x_p,V(p,\vec{z}))$ dans la théorie de l'addition. Alors
$X = \{x/V(p,x) = 0$ si $p \notin P' \cup \{p_o\}$

$V(p,x) \in Y_p$ si $p \in P'\backslash\{p_o\}$

$V(p_o,x) \in Y\ \}$

est témoin.

- Sinon on a $R_1(\exists x(x \neq 0 \wedge \neg\theta(0,x,\vec{0}) \wedge \neg\theta(x,0,\vec{0})))$

et $\neg R_1(\neg\exists x \neg\theta(x,x,\vec{z}))$.

Soient P' l'ensemble des nombres premiers divisant les paramètres, $(p_i)_{i\in\mathbb{N}}$ une énumération de $\mathbb{P}\backslash P'$, x_o tel que $\neg\theta(0,x_o,\vec{0})$ et $\neg\theta(x_o,0,\vec{0})$ pour la théorie de l'addition, et pour $p \in P'$, x_p tel que $\neg\theta(x_p,x_p,V(p,\vec{z}))$ pour la théorie de l'addition. Alors l'ensemble $X = \{x_n/n \in \mathbb{N}\}$ défini de la façon suivante :

+ $V(p,x_n) = x_p$ pour $p \in P'$

+ $V(p_n,x_n) = x_o$

+ $V(p_i,x_n) = 0$ pour $i \neq n$

est un ensemble témoin. □

Lemme 3.- $Q^2 x\, y\ S_k(\theta) \longleftrightarrow (Q^2 x\, y\ R_k(\theta) \wedge \neg R_1(\theta(0,0,\vec{0}))$

$\wedge \neg R_{k+1}(\neg(\exists x \neg\theta(x,z,\vec{x}) \vee Q^2 x\, y \neg\theta(x,y,\vec{z})))$

$\wedge R_1(Q^2 x\, y\ \theta(x,y,\vec{z}) \vee Q^2 x\, y \neg\theta(x,y,\vec{z})$

$\vee \exists x\ (x \neq 0 \wedge (\theta(x,0,\vec{0}) \vee \neg\theta(x,0,\vec{0})))))$

Démonstration.- CN. + La première condition vient de ce que : $Q^2(A \wedge B) \rightarrow Q^2A$.

+ La deuxième condition se montre comme dans le lemme 2.

+ Pour la troisième condition, s'il existe au moins $k+1$ nombres premiers p tels que

$$(1) \qquad (\neg \exists x \neg\theta(x,x,\vec{z}) \wedge \neg Q^2 x y \neg\theta(x,y,\vec{z}))^p$$

alors, d'après le théorème de Ramsey, il existe un nombre premier p parmi ceux-là et Y infini tel que : $\forall x,y \in Y,\ x \neq y,\ (\neg\theta(x,y))^p$; d'où s'il existe $x,y \in Y$ avec $x \neq y$ et $V(p,x) = V(p,y)$ on a $\exists x \neg\theta$, et sinon $Q^2 x y \neg\theta$, ce qui est contradictoire avec (1).

+ Pour la dernière condition soit X un ensemble témoin, donc infini.

S'il existe $p_o \in \mathbb{P}$ tel que $\{V(p,x)/x \in X\}$ soit infini, alors, en utilisant le théorème de Ramsey, on obtient :

$$R_1(Q^2 x y\ \theta(x,y,\vec{z}) \vee Q^2 x y \neg\theta(x,y,\vec{z})).$$

Sinon soit $x_o \in X$, P' l'ensemble fini des nombres premiers divisant x_o et le produit des paramètres, alors il existe $y_o \in X$, $p_o \in \mathbb{P} \setminus P'$ tel que $V(p_o,y) \neq 0$, d'où on a :

$$R_1(\exists x(x \neq 0 \wedge (\theta(x,0,\vec{0}) \vee \neg\theta(x,0,\vec{0})))).$$

CS. + Soient $m \leq k$ tel que $S_m(\neg(\exists x \neg\theta(x,x,\vec{z}) \vee Q^2 x y \neg\theta(x,y,\vec{z})))$ et $p_1,\ldots,p_m$ les m nombres premiers concernés. On mettra : $V(p_i,x) = 0$. Dans la suite on peut donc considérer que :

$$\neg R_1(\neg(\exists x \neg\theta(x,x,\vec{z}) \vee Q^2 x y \neg\theta(x,y,\vec{z})))$$

en remplaçant k par $m-k$ dans $S_k(\theta)$.

+ Si on a $R_1(\exists x \exists y\ \theta(x,y,\vec{0}))$, distinguons les trois cas suivants :

- si on a : $R_1(\exists x\ \theta(x,x,\vec{0})) \wedge \neg R_1(\exists x(x \neq 0 \wedge (\theta(x,0,\vec{0}) \vee \theta(0,x,\vec{0}))))$ soit x_o tel que l'on ait $\theta(x_o,x_o,0)$ pour la théorie de l'addition, et $p_1,\ldots,p_k$ k nombres premiers ne divisent pas le produit des paramètres. On a aussi :

$$R_1(Q^2 x\ y\ \theta(x,y,\vec{z}) \vee Q^2 x\ y \neg\theta(x,y,\vec{z}) \vee \exists x(x \neq 0 \wedge \neg\theta(x,0,\vec{0})))$$

On comprend alors comment construire l'ensemble témoin ; on procède ainsi :

- si on a :

$$R_1(\exists x\ y\ (x \neq y \wedge \theta(x,y,\vec{0}) \wedge \neg\theta(y,x,\vec{0}) \wedge \neg\theta(x,x,\vec{0}) \wedge \neg\theta(y,y,\vec{0}))),$$

alors on construit l'ensemble témoin de façon analogue à celle utilisée dans le lemme 1.

- si on a

$$R_1(\exists x\ \exists\ y(x \neq y \wedge \theta(x,y,\vec{0}) \wedge \theta(y,x,\vec{0}) \wedge \neg\theta(x,x,\vec{0}) \wedge \neg\theta(y,y,\vec{0})))$$

alors soient (x_o,y_o) un tel couple d'entiers, P' l'ensemble des nombres premiers divisant les paramètres et $(p_i)_{i\in\mathbb{N}^*}$ une énumération de $\mathbb{P}\setminus P'$, on construit un ensemble témoin $X = \{x_n / n \in \mathbb{N}^*\}$, avec $V(p,x_n) \in Y_p$, Y_p ensemble témoin si on a $(Q^2 x\ y \neg\theta(x,x,\vec{z}))^p$, ou $V(p,x) = y_p$ tel que $(\neg\theta(y_p,y_p,\vec{z}))^p$ sinon, pour $p \in P'$, et

$$V(p_i,x_n) = y_o \qquad \text{pour } i \in [1,k(n-1)]$$

$$V(p_i,x_n) = x_o \qquad \text{pour } i \in [k(n-1)+1,k_n]$$

$$V(p_i,x_n) = 0 \qquad \text{sinon.}$$

+ Sinon on a : $R_k(\exists x\ \theta(x,x,\vec{z}) \vee Q^2 x\ y\ \theta(x,y,\vec{z}))$

$$\wedge R_1(Q^2 x\ y\ \theta(x,y,z) \vee Q^2 x\ y \neg\theta(x,y,\vec{z}) \wedge \exists x(x \neq y \wedge \neg\theta(x,0,\vec{0})$$

$$\wedge \neg\theta(0,x,\vec{0})))$$

et la construction de l'ensemble témoin ne pose pas de problème. □

o Dans le cas général, on se sert du fait que :

$$Q^2 x y \bigwedge_i \phi_i \to \bigwedge_i Q^2 x y \phi_i,$$

ce qui fait que l'on peut se servir des lemmes précédents pour établir la condition nécessaire ; pour la condition suffisante, on fera la construction effective d'un ensemble témoin. La difficulté est que l'on peut avoir des chevauchements c'est-à-dire que, malgré que les θ_j soient indépendants, pour un nombre premier on peut avoir, par exemple : $(Q^2 x y \theta_1 \wedge Q^2 x y \theta_2)^p$.

Disons d'abord, pour $l_1,\ldots,l_k$ entiers, $\theta_1,\ldots,\theta_k$ formules de (.), que $\Phi_k(l_1,\theta_1,\ldots,l_k,\theta_k)$ signifie:

"Il existe un sous-ensemble de nombres premiers admettant une partition en k classes, $(P_i)_{1\le i\le k}$, tel que pour $i \in [1,k]$, P_i contienne l_i éléments et pour $p \in P_i$ on ait :

$$(\exists x\ \theta_i(x,x,\vec{z}) \vee Q^2 x y\ \theta_i(x,y,\vec{z}))^p \text{ ".}$$

Ceci se dit, bien sûr, dans le langage de la multiplication. Dans la suite, on ne notera pas l'indice k.

Alors, je dis que, si $n+m \neq 0$:

$$Q^2 x y\Big(\bigwedge_{1\le i\le n} R_{k_i}(\theta_i) \wedge \bigwedge_{n+1\le i\le n+m} S_{k_i}(\theta_i) \wedge \neg R_l(\theta)\Big)$$

$$\leftrightarrow \Big[\neg R_l\Big(\bigvee_{n+1\le i\le n+m} \theta_i(0,0,\vec{0}) \vee \theta(0,0,\vec{0})\Big)$$

$$\wedge \bigwedge_{n+1\le i\le n+m} \neg R_{k_i+1}(\neg(\exists x \neg\theta_i(x,x,\vec{z}) \vee Q^2 x y \neg\theta_i(x,y,\vec{z})))$$

$$\wedge \neg R_l(\neg(\exists x \neg\theta(x,x,\vec{z}) \vee Q^2 x y \neg\theta(x,y,\vec{z})))$$

$$\wedge \bigvee_{I\subset[1,n+m]} (\Phi((k_i,\theta_i)_{i\notin I}) \wedge \bigwedge_{i\in I} R_l(\exists x \exists y(\theta_i(x,y,\vec{0})))$$

$$\wedge R_l\Big(\bigvee_{1\le i\le n+m} Q^2 x y\ \theta_i(x,y,\vec{z}) \vee \bigvee_{1\le i\le n} \exists x \exists y\ \theta_i(x,y,\vec{0})$$

$$\vee \bigvee_{n+1\le i\le n+m} \exists x \exists y(x \neq y \wedge \theta_i(x,y,\vec{0}))\Big)\Big]$$

d'où le résultat. □

Remarque.- Pour $n \geq 2$, le quantificateur de Ramsey Q^n est tel que $Q^n x_1 \ldots x_n \, \phi(x_1,\ldots,x_n)$ est vrai si, et seulement si, il existe un ensemble infini X tel que $\phi(a_1,\ldots,a_n)$ soit vrai pour tout n-ensemble $\{a_1,\ldots,a_n\}$ de X.

Schmerl et Simpson ([SS]) ont montré que les quantificateurs de Ramsey supérieurs Q^n s'éliminaient pour l'addition. Le résultat est encore vrai pour la multiplication. Il suffit de reprendre la démonstration précédente, que nous avons traitée seulement dans le cas n =2 pour simplifier.

REFERENCES

[CH] Zoé CHATZIDAKIS : "Théorie de la multiplication et faisceaux", ce volume.

[FV] S. FEFERMAN, R.L. VAUCHT : "The first order properties of products of algebraic systems", Fundamenta Mathematicae, 1959, pp. 57-103

[FR] R. FRAISSE : Cours de Logique mathématique, t. 2 (p. 45), 172 p., Gauthier -Villars, 1972.

[JE] DON JENSEN, A. EHRENFEUCHT : "Some problems in elementary arithmetic", Fundamenta Mathematicae, 1976, XCII, pp. 223-245.

[LE] H. LESSAN : Models of arithmetics (Thèse, Manchester, 1978).

[MA] A. MACINTYRE : "Ramsey quantifiers in arithmetic", Proceeding of logic symposium (Karpacz, 1979), Springer-Verlag SLN 834.

[Mc] K. Mc ALOON : "On the complexity of models of arithmetic" (à paraître dans JSL).

[ME] E. MENDELSON : Introduction to mathematical logic, 2nd. ed. 1979, 324 p. Van Nostrand.

[MO] A. MOSTOWSKI : "On direct products of theories", Journal of symbolic logic 17, 1952, pp. 1-31.

[NA] M.E. NADEL : "The completeness of Peano multiplication", Abstracts of the american mathematical society, vol.1 N° 2, Février 1980, p. 236

[PA] R. PARIKH : "Existence and feasibility in arithmetic", Journal of Symbolic Logic 36, 1971, pp. 494-503.

[PR] M. PRESBURGER : "Uber die Völlstandigkeit eines gewissen systems der arithmetik ganzer zahlen in welchem addition als einzige operation hervortritt",C.R. 1er Congr. des mathématiciens des Pays slaves, 1930, pp. 92-101, 395.

[RA] Ch. RACKOFF : "On the complexity of the theories of weak direct products", preprint de janvier 1974.

[SK] T. SKOLEM : "Uber einige satzfunktionen in der arithmetik" Skriften utgit av videnskasselskapet i Kristiana, 1 Klasse, N° 7, Oslo, 1930. Reproduit dans T. Skolem Selected works in logic, J.E. Fenstad ed., Universteds-forlaget, Oslo, 1970, pp. 281-306; avec une analyse en anglais de Hao Wang (p. 34).

[SS] J.H. SCHMERL, S.G. SIMPSON : "On the role of Ransey quantifier in first order atithmetic", à proposer au Journal of symbolic logic.

*
* *