3°) Des résultats nouveaux de définissabilité de l'addition et de la multiplication à partir de $(S, +; \perp)$ ou de $(<, \perp)$ sur $\mathbf{Z}$.

Il est à noter que $S$ n'est pas définissable par addition et coprimarité sur $\mathbf{Z}$: en effet, $x \mapsto (-x)$ est un automorphisme de $\mathbf{Z}$ qui respecte $+$ et $\perp$ mais pas $S$.

## § 5. La méthode de codage ZBV et le problème de J. Robinson

### 5.1. *La méthode de codage* ZBV

Les Théorèmes ZBV et LC (cf. 2.2 et 2.3) et leur Corollaire 2.4 permettent des codages qui s'avèrent particulièrement performants dans l'étude du pouvoir de définissabilité des langages $(S; \perp)$ et $(\mathrm{Pred}; \perp)$.

*La méthode de codage* ZBV *consiste à considérer comme codes d'un entier $x$ les supports ou bien les diviseurs primitifs des formes du type $p^x \pm 1$, où $p$ est premier.*

*On ramène ainsi certaines questions arithmétiques à la* théorie des ensembles finis *de nombres premiers; en particulier, à des questions sur leur combinatoire.*

*Par ailleurs, chaque ensemble fini de nombres premiers (ou fonction de domaine fini entre nombres premiers) est lui-même codable (de multiples façons) par un seul nombre premier via la méthode indiquée en 2.1 combinant le Théorème de Dirichlet et le Théorème des restes chinois. Un tel code joue alors le rôle de mémoire dans laquelle est stocké l'ensemble fini de premiers (ou la fonction) considéré(e).*

5.2. Avant de passer à des applications de la méthode ZBV, nous montrons quelques résultats simples sur la mise en place dans la structure $\langle \mathbf{N}; \perp \rangle$ d'éléments d'une théorie des ensembles finis par le biais des supports d'entiers: l'ensemble de base est $P$, *chaque partie finie $X$ de $P$ est codée par les entiers ayant $X$ pour support.*

La relation d'inclusion entre parties finies de $P$ se traduit sur leurs codes par la relation $\mathrm{SUPP}(x) \subseteq \mathrm{SUPP}(y)$.
Comme cette inclusion entre supports a lieu si et seulement si tout entier premier avec $y$ est premier avec $x$, on voit qu'elle se traduit dans la structure $\langle \mathbf{N}; \perp \rangle$ par la formule $\forall z[(z \perp y) \rightarrow (z \perp x)]$, notée $\mathrm{SUPP}(x) \subseteq \mathrm{SUPP}(y)$.

A partir de cette relation, on peut définir la relation d'égalité entre supports et les opérations ensemblistes d'union, intersection et différence des

supports. On obtient ainsi l'algèbre ensembliste élémentaire sur les parties finies de $P$.

5.3. On remarque ensuite qu'un entier $x$ est primaire si et seulement si son support est inclus dans celui de tout entier non premier avec lui.

On en déduit alors des formules qui définissent dans $\langle \mathbf{N}; \perp \rangle$ l'ensemble $PP$ des primaires et la relation $\{(x, y) : x$ et $y$ sont des puissances d'un même premier$\}$. Notées respectivement $PP(x)$ et $PP(x, y)$, ce sont

$$\forall y\{[\neg(y \perp x)] \to \mathrm{SUPP}(x) \subseteq \mathrm{SUPP}(y)\} \quad \text{et} \quad PP(x) \wedge PP(y) \wedge \neg(x \perp y) \ .$$

On observe enfin que les ensembles $\{1\}$ et $\{0\}$ sont $\langle \mathbf{N}; \perp \rangle$-définis par les formules suivantes, notées respectivement $\mathrm{Egal}_1(x)$ et $\mathrm{Egal}_0(x)$:

$$\forall y(y \perp x) \quad \text{et} \quad \forall y[(y \perp x) \to \mathrm{Egal}_1(y)] \ .$$

On utilisera donc (cf. la Proposition 3.10) les constantes 0 et 1 dans le cadre de tout langage contenant $\perp$.

*Remarque.* L'exemple 1 de 3.8 permet de voir que les singletons $\{0\}$ et $\{1\}$ sont les seuls à pouvoir être définis dans $\langle \mathbf{N}; \perp \rangle$.

5.4. On peut définir très simplement le singleton $\{n\}$, $n \geqslant 2$, (et donc aussi toute relation finie) dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$ par la formule $\mathrm{Egal}_1[\mathrm{Pred}^{n-1}(x)]$, notée $\mathrm{Egal}_n(x)$.

On utilisera donc toutes les constantes entières dans le cadre du langage $\langle \mathrm{Pred}; \perp \rangle$.

5.5. Nous montrons maintenant des applications simples — et fondamentales — de la méthode ZBV.

Le Théorème 2.12 montre que pour des entiers primaires $x$ et $y$, les trois conditions $x = y$, $x \cong_{\{0,1,2\}} y$, $x \cong_{\{-2,-1,0\}} y$ sont équivalentes.
On en déduit des définitions de l'égalité restreinte au domaine $PP$ dans les structures $\langle \mathbf{N}; S; \perp \rangle$ et $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$, notées toutes deux $x =_{PP} y$:

$$PP(x, y) \wedge \mathrm{SUPP}[S(x)] = \mathrm{SUPP}[S(y)] \wedge \mathrm{SUPP}[S^2(x))] = \mathrm{SUPP}[S^2(y))] \ ,$$

$$PP(x, y) \wedge \mathrm{SUPP}[\mathrm{Pred}(x)] = \mathrm{SUPP}[\mathrm{Pred}(y)] \wedge \mathrm{SUPP}[\mathrm{Pred}^2(x))]$$
$$= \mathrm{SUPP}[\mathrm{Pred}^2(y))] \ .$$

A partir de ces formules, on obtient une définition dans $\langle \mathbf{N}; S; \perp \rangle$ de la restriction à $PP$ de la fonction prédécesseur par la formule, notée $\mathrm{Pred}_{PP}(x, y)$:

$$[\mathrm{Egal}_0(x) \to \mathrm{Egal}_0(y)] \wedge \{[\neg(\mathrm{Egal}_0(x)] \to [x =_{PP} S(y)]\}$$

On obtient aussi une définition dans $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$ de la restriction à $PP$ de la fonction successeur par la formule, notée $S_{PP}(x, y)$: $\neg(\mathrm{Egal}_0(y)] \wedge [x =_{PP} \mathrm{Pred}(y)]\}$.

*Remarques.* 1°) Soit $n > 0$. La formule

$$PP(x) \vee PP[S(x)] \vee \ldots \vee PP[S^n(x)]$$

définit l'ensemble $PP + [-n, 0]$ dans $\langle \mathbf{N}; S; \perp \rangle$. L'application du Corollaire 2.12 montre — comme plus haut — que l'égalité et la fonction prédécesseur restreintes à cet ensemble sont définissables avec $S$ et $\perp$.

2°) De façon analogue, avec Pred et $\perp$, c'est l'ensemble $PP + [0, n]$ qui est définissable, ainsi que l'égalité et la fonction successeur restreintes à celui-ci.

5.6. On peut maintenant définir les singletons dans $\langle \mathbf{N}; S; \perp \rangle$.
Soit $n \geqslant 2$ et soit $p$ un premier plus grand que $n$. La condition $x = n$ équivaut à

$$(p-n)\text{-ième successeur de } x = (p-1)\text{-ième successeur de } 1\,,$$

relation qui ne fait intervenir que la seule restriction de l'égalité à $PP$.

Ainsi, l'ensemble $\{n\}$ est défini dans $\langle \mathbf{N}; S; \perp \rangle$ par la formule $S^{p-n}(x) =_{PP} S^{p-1}(1)$, notée $\mathrm{Egal}_n(x)$. On utilisera donc toutes les constantes entières dans le cadre du langage $(S; \perp)$.

5.7. Nous définissons maintenant (à la suite de [RD1]) *l'ensemble $P$ des nombres premiers* dans chacun des langages $(S; \perp)$ et $(\mathrm{Pred}; \perp)$.

Le point ii) du Corollaire 2.4 montre que l'ensemble $X$ des primaires $x$ tels que $\mathrm{SUPP}(x-1) \subseteq \mathrm{SUPP}(y-1)$ pour tout primaire $y$ de même base que $x$ est égal à

$$X = P \cup \{(2^u-1)^2 : u \geqslant 2 \text{ et l'entier } 2^u - 1 \text{ est premier}\}\,.$$

Cet ensemble $X$ se définit dans $\langle \mathbf{N}; S; \perp \rangle$ par la formule $X(x)$ suivante:

$$PP(x) \wedge \forall y \forall u \forall v \{[PP(x, y) \wedge \mathrm{Pred}_{PP}(x, u) \wedge \mathrm{Pred}_{PP}(y, v)] \to \mathrm{SUPP}(u) \subseteq \mathrm{SUPP}(v)\}$$

Comme $(2^u-1)^2 + 1 = 2[2^u(2^{u-1}-1)+1]$, l'entier $(2^u-1) + 1$ est une puissance de 2 mais pas $(2^u-1)^2 + 1$. On voit ainsi que $P$ se définit à

partir de $X$ comme suit: $P = \{x \in X$: s'il existe $y \in X$, $y$ de même base que $x$ et $y \neq x$ alors $x + 1$ est une puissance de $2\}$
On en déduit alors une définition, notée $P(x)$, dans $\langle \mathbf{N}; S; \perp \rangle$ de l'ensemble $P$:

$$X(x) \wedge \{[\exists z[X(z) \wedge (z \neq_{PP} x) \wedge PP(x, z)]] \rightarrow PP(S(x), 2)]\} .$$

Grâce au prédicat $S_{PP}$, ces définitions se transfèrent simplement de la structure $\langle \mathbf{N}; S; \perp \rangle$ à la structure $\langle \mathbf{N}; \text{Pred}; \perp \rangle$ donnant les formules, notées également $X(x)$ et $P(x)$:

$$PP(x) \wedge \forall y\{PP(x, y) \rightarrow \text{SUPP}\,[\text{Pred}(x)] \subseteq \text{SUPP}\,[\text{Pred}(u)]\} .$$

$$X(x) \wedge \{[\exists z[X(z) \wedge (z \neq_{PP} x) \wedge PP(x, z)]] \rightarrow \exists t\,[S_{PP}(x, t) \wedge PP(t, 2)]\} .$$

5.8. La possibilité de définir $P$ par l'adjonction à $\perp$ de $S$ ou bien Pred permet de développer considérablement la théorie des parties finies de $P$ mise en place en 5.2 par le biais des supports d'entiers:

*Toute la combinatoire ensembliste sur les supports s'exprime dans chacun des langages* $(S; \perp)$ *et* $(\text{Pred}; \perp)$.

La relation d'appartenance, traduite sur les codes par la relation $p \in \text{SUPP}\,(x)$, est définie dans chacune des structures $\langle \mathbf{N}; S; \perp \rangle$ et $\langle \mathbf{N}; \text{Pred}; \perp \rangle$ par la formule $P(p) \wedge \neg(p \perp x)$.

Nous montrons ci-dessous comment élargir le codage des parties finies de $P$ à un *codage des relations et fonctions sur ces parties finies.*

Pour $k \geqslant 1$ fixé, on note $(A_\alpha)_{1 \leqslant \alpha \leqslant K}$ une énumération des suites de $k + 1$ parties de $\{1, 2, ..., k\}$. Soit $\pi$ un entier premier plus grand que $K$. Soient $x_1, ..., x_k$ des entiers.
A tout $(p_1, ..., p_k) \in \text{SUPP}\,(x_1) \times ... \times \text{SUPP}\,(x_k)$ on associe — à l'aide du Théorème de Dirichlet (cf. 2.1) — l'ensemble infini $X_{p_1, ..., p_k}$ des entiers premiers $z > \pi$ qui vérifient les équations de congruences:

$z \equiv i \pmod{p_i}$ pour les $i$ tels que $p_i > k + 1$, $p_i \neq \pi$ et $p_i \neq p_j$ pour tous les $j < i$,

$z \equiv k + 1 \pmod{q}$ si $q \in [\text{SUPP}(x_1) \cup ... \cup \text{SUPP}(x_k)] \setminus \{1, ..., k+1, p_1, ..., p_k, \pi\}$,

$z \equiv \alpha \pmod{\pi}$ si $A_\alpha$ est $(\{i: p_i = 2\}, ..., \{i: p_i = k + 1\}, \{i: p_i = \pi\})$.

On voit simplement que les $X_{p_1, ..., p_k}$ sont deux à deux disjoints.

Les Pred-codes d'une relation $\rho$ sur $\text{SUPP}\,(x_1) \times ... \times \text{SUPP}\,(x_k)$ sont alors les entiers dont les supports coupent les seuls $X_{p_1, ..., p_k}$ tels que $(p_1, ..., p_k) \in \rho$. Les Pred-codes d'une fonction sont ceux de son graphe.

Les $S$-codes d'une relation sont définis de façon similaire avec les ensembles $Y_{p_1, ..., p_k}$ obtenus en remplaçant dans la définition de $X_{p_1, ..., p_k}$ les restes de congruences par leurs opposés.

PROPOSITION. *Les relations*

« $(p_1, ..., p_k)$ appartient à la relation $S$-codée par $x$ sur $\mathrm{SUPP}(x_1) \times ... \times \mathrm{SUPP}(x_k)$ »,

« $(p_1, ..., p_k)$ appartient à la relation Pred-codée par $x$ sur $\mathrm{SUPP}(x_1) \times ... \times \mathrm{SUPP}(x_k)$ »

*sont respectivement définissables dans les structures* $\langle \mathbf{N}; S; \perp \rangle$ *et* $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

*Preuve.* La définition des $X_{p_1, ..., p_k}$ se traduit simplement en une définition avec Pred et $\perp$ de la relation $\{(x_1, ..., x_k, p_1, ..., p_k, z): z \in X_{p_1, ..., p_k}\}$. D'où l'assertion relative aux Pred-codes. Celle pour les $S$-codes se déduit de même.

Les notions ensemblistes usuelles se traduisent alors en propriétés sur les $S$-codes ou Pred-codes définissables avec $S$ et $\perp$, ou Pred et $\perp$.

En particulier, la notion d'injection entre supports d'entiers conduit à la définissabilité de toute l'arithmétique sur les cardinalités des supports.

Notant $|X|$ le nombre d'éléments de $X$, on retrouve ainsi un résultat de Woods:

COROLLAIRE (Woods). 1°) *Les images réciproques par la surjection* $x \mapsto |\mathrm{SUPP}(x)|$ *de* $\mathbf{N}\backslash\{0\}$ *sur* $\mathbf{N}$ *des relations* $\leqslant$, $=$ *et des graphes de l'addition et de la multiplication sont définissables dans les structures* $\langle \mathbf{N}; S; \perp \rangle$ *et* $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

2°) *La théorie* $Th(\mathbf{N}; S; \perp)$ (ensemble des énoncés s'écrivant avec le successeur et la coprimarité pour seuls symboles de fonction et prédicat) *est indécidable.*

*Remarque.* La partie 2°) de ce Corollaire signifie que la vérité arithmétique des énoncés avec successeur et coprimarité est aussi compliquée que celle de tous les énoncés de l'arithmétique. C'est une condition évidemment nécessaire à une réponse positive à la conjecture d'Erdös-Woods d'après le théorème cité en 4.7.

5.9. Une autre application simple du Théorème ZBV permet de définir une fraction de la fonction exponentielle.

La caractérisation donnée par le point iii) du Corollaire 2.4 de la notion de diviseur primitif se traduit directement par des formules des langages $(S; \perp)$ et (Pred; $\perp$), notées toutes deux PRIMITIF $(p, u)$.

Si $p$ et $q$ sont des nombres premiers distincts, l'entier $q^{\mathrm{ORD}(q, p)}$ est la seule puissance $u$ de $q$ telles que $p$ soit diviseur primitif de $u - 1$. Cette condition s'exprime immédiatement avec la formule PRIMITIF $(p, u)$, d'où le résultat suivant.

PROPOSITION. *On peut définir avec* $S$ *et* $\perp$, *ou bien* Pred *et* $\perp$, *la relation ternaire*

$$\{(p, q, u) : p \text{ et } q \text{ sont premiers distincts et } u = q^{\mathrm{ORD}(q, p)}\} .$$

5.10. Les deux propositions qui suivent sont des résultats techniques utiles en 5.11. Soient $p^\alpha$ un primaire de base $p$ et $x$ un entier tels que :

— $\mathrm{SUPP}(x) \subseteq \mathrm{SUPP}(p^\alpha - 1)$,

— l'ensemble $\mathrm{SUPP}(x)$ contient exactement un diviseur primitif de tout $p^\beta - 1$ qui admet un diviseur primitif et vérifie l'inclusion $\mathrm{SUPP}(p^\beta - 1) \subseteq \mathrm{SUPP}(p^\alpha - 1)$.

Le point ii) du Corollaire 2.5 montre que

— si $p^\alpha$ n'est pas le carré d'un premier de Mersenne $p = 2^u - 1$ et si $p \neq 2$ ou bien $p = 2$ mais $\mathrm{SUPP}(2^6 - 1) = \{3, 7\} \nsubseteq \mathrm{SUPP}(p^\alpha - 1)$, alors le cardinal de $\mathrm{SUPP}(x)$ est le nombre des diviseurs de $\alpha$,

— si $p = 2$ et $\mathrm{SUPP}(2^6 - 1) = \{3, 7\} \subseteq \mathrm{SUPP}(p^\alpha - 1)$, alors le cardinal de $\mathrm{SUPP}(x)$ est le nombre des diviseurs de $\alpha$ diminué de 1,

— si $p$ est de la forme $2^u - 1$ et $p^\alpha = p^2$, alors $|\mathrm{SUPP}(x)| = 1$ tandis que le nombre des diviseurs de $\alpha$ est 2.

Toutes les clauses précédentes sont exprimables avec $S$ et $\perp$, ou Pred et $\perp$. A l'aide du Corollaire 5.8, ceci conduit à :

PROPOSITION 1. *On peut définir avec* $S$ *et* $\perp$, *ou bien* Pred *et* $\perp$, *la relation*

$$\{(u, x) : u \text{ est primaire et } |\mathrm{SUPP}(x)| \text{ est le nombre des diviseurs de la valuation de } u\} .$$

*En particulier, on peut aussi exprimer dans ces langages la relation*

$$\{(u, v) : u \text{ et } v \text{ sont primaires et leurs valuations ont le même nombre des diviseurs}\} .$$

On peut alors montrer la Proposition suivante.

PROPOSITION 2. *On peut définir avec* $S$ *et* $\perp$, *ou bien* Pred *et* $\perp$, *la relation*

$$\{(p, q,) : p \text{ et } q \text{ sont premiers et distincts et } \mathrm{ORD}(q, p) = p - 1\}.$$

*Preuve.* Comme pour tout $r$ l'entier $\mathrm{ORD}(r, p)$ est toujours un diviseur de $p - 1$, on voit que l'égalité $\mathrm{ORD}(q, p) = p - 1$ équivaut à la condition « *pour tout premier* $r$ *l'entier* $\mathrm{ORD}(r, p)$ *n'a pas plus de diviseurs que* $\mathrm{ORD}(q, p)$ ».

Cette dernière condition peut aussi s'écrire

« *pour tout premier* $r$ *la valuation de* $r^{\mathrm{ORD}(r, p)}$ *n'a pas plus de diviseurs que celle de* $q^{\mathrm{ORD}(q, p)}$ ».

Sous cette forme, la traduction dans les langages avec $S$ ou Pred est une application immédiate de la Proposition 1 et de celle de 5.9.

5.11. La Proposition 2 précédente permet de définir maintenant une partie importante de la fonction exponentielle. La preuve qui suit reprend et simplifie celle de [RD1].

PROPOSITION. *On peut définir avec* $S$ *et* $\perp$, *ou bien* Pred *et* $\perp$, *la restriction de la fonction* $(p, q) \mapsto q^{p-1}$ *à l'ensemble* $\{(p, q,) : p$ *et* $q$ sont premiers et distincts$\}$.

*Preuve.* Compte tenu de la Proposition 2 de 5.10, il suffit de définir $q^{p-1}$ lorsque $p$ et $q$ sont des premiers distincts tels que $\mathrm{ORD}(q, p) < p - 1$.

Soit $w$ une puissance de $q$ telle que $\mathrm{SUPP}(q^{\mathrm{ORD}(q, p)} - 1) \subseteq \mathrm{SUPP}(w - 1)$ (c'est-à-dire de la forme $q^{k \times \mathrm{ORD}(q, p)}$). On pose

$$X_w = \{q^\alpha : \mathrm{SUPP}(q^{\mathrm{ORD}(q, p)} - 1) \subseteq \mathrm{SUPP}(q^\alpha - 1) \subseteq \mathrm{SUPP}(w - 1)\},$$

$$D(X_w) = \{r : r \neq p \text{ et } r \text{ est diviseur primitif d'un } q^\alpha - 1 \text{ où } q^\alpha \in X\},$$

$$\Sigma(X_w) = \{z : z \text{ est premier, } \mathrm{ORD}(z, p) = p - 1 \text{ et } z \equiv q \pmod r \text{ pour tout } r \in D(X_w)\}.$$

Le théorème de Dirichlet (cf. 2.2) (et le fait que la condition $\mathrm{ORD}(z, p) = p - 1$ soit impliquée par toute équation de congruence $z \equiv g \pmod p$, où $g$ est un entier tel que $\mathrm{ORD}(g, p) = p - 1$) montre que l'ensemble $\Sigma(X_w)$ est infini.

La définition de $\Sigma(X_w)$ montre que si $z \in \Sigma(X_w)$ alors $\mathrm{ORD}(z, p) = \mathrm{ORD}(g, p) = p - 1$ et $\mathrm{ORD}(z, r) = \mathrm{ORD}(q, r)$. Ainsi, $p$ est diviseur primitif de $z^{p-1}$ et tout diviseur primitif de $q^\alpha - 1$ qui est différent de $p$ est aussi primitif pour $z^\alpha - 1$ (et donc non primitif pour les $z^\beta - 1$ où $\alpha \neq \beta$). En particulier,

— si $\alpha \neq p - 1$ alors $q^\alpha - 1$ n'a aucun diviseur primitif différent de $p$ et qui soit primitif pour $z^{p-1} - 1$;

— si $q^{p-1} \in X$ et s'il existe un diviseur primitif de $q^{p-1} - 1$ alors celui-ci est différent de $q$ et tel que $\mathrm{SUPP}(u-1) = \mathrm{SUPP}(q-1)$;

3°) il existe un primaire $w$ de base $q$ tel que $\mathrm{SUPP}(q^{\mathrm{ORD}(q,p)}-1) \subseteq \mathrm{SUPP}(w-1)$ et $u$ admet un diviseur primitif différent de $p$ en commun avec $z^{p-1} - 1$ pour tout $z$ de $\Sigma(X_w)$.

On conclut la preuve en observant que ces conditions sont simplement exprimables dans les langages $(S; \perp)$ et $(\mathrm{Pred}; \perp)$.

COROLLAIRE. *La restriction de la fonction* $x \mapsto 5^x$ *à l'ensemble* $P$ *est définissable dans la structure* $\langle \mathbf{N}; S; \perp \rangle$.

*Preuve.* Le Corollaire 2.4 montre que $5^{n+1}$ est le seul primaire $5^\alpha$ tel que $\mathrm{SUPP}(5^\alpha - 5) = \{5\} \cup \mathrm{SUPP}(5^n - 1)$.

Cette condition permet donc de définir la fonction $5^n \mapsto 5^{n+1}$ de domaine $5^{\mathbf{N}}$ dans la structure $\langle \mathbf{N}; S; \perp \rangle$. On conclut avec la Proposition précédente, appliquée à $q = 5$.

5.12. PROPOSITION. *La fonction* $x \mapsto 5^x$ *transforme la structure*

$$\langle \mathbf{N}; +; \times, = \rangle$$

*en une structure* $\langle 5^{\mathbf{N}}; \mathrm{NA}, \mathrm{NM}; =_{PP} \rangle$ *qui est entièrement définissable dans la structure* $\langle \mathbf{N}; S; \perp \rangle$.

*En particulier, les structures* $\langle \mathbf{N}; S, x \mapsto 5^x; \perp \rangle$ *et* $\langle \mathbf{N}; +, \times; = \rangle$ *définissent les mêmes relations et fonctions.*

*Preuve.* On a déjà vu que la fonction $5^n \mapsto 5^{n+1}$ de domaine $5^{\mathbf{N}}$, notée NS (pour Nouveau Successeur) est $(S, \perp)$-définissable.

Le même Corollaire 2.4 définit aussi directement la relation NDIV (pour Nouvelle DIVisibilité) formée des couples $(5^n, 5^m)$ tels que $n$ divise $m$.

Cette fonction et cette relation sont les images, par l'application $x \mapsto 5^x$, de la fonction successeur et de la relation de divisibilité.

Ainsi, on peut définir, au sein de la structure $\langle \mathbf{N}; S; \perp \rangle$, une nouvelle structure $\langle 5^{\mathbf{N}}; \mathrm{NS}; \mathrm{NDIV} \rangle$ qui est isomorphe, via $x \mapsto 5^x$, à la structure $\langle \mathbf{N}; S; | \rangle$.

Le Théorème de J. Robinson (cf. 4.5) assure que l'addition et la multiplication sont définissables dans $\langle \mathbf{N}; S; | \rangle$. Les formules qui définissent l'addition et la multiplication usuelles sur les entiers à partir de $S$ et $|$ permettent alors de définir dans la structure $\langle 5^{\mathbf{N}}; \mathrm{NS}; \mathrm{NDIV} \rangle$, et donc à fortiori dans $\langle \mathbf{N}; S; \perp \rangle$, les fonctions, notées NA et NM (pour nouvelles addition et multiplication), qui sont les images des fonctions $+$ et $\times$ par l'isomorphisme $x \mapsto 5^x$.

*Remarques.* 1°) Le choix de la base 5 (plutôt que 2 ou 3) permet d'éviter les exceptions au Théorème ZBV et à son Corollaire 3.4, lesquelles ne concernent en effet que les bases 2 et $2^u - 1$.

2°) J. P. Jones nous a signalé l'article [RR] dans lequel R. M. Robinson utilise également les modèles internes sur les puissances d'un premier fixé. Il démontre que ceux-ci sont $(S; |)$-définissables.

3°) La $(S; \perp)$-définissabilité de la fonction $x \mapsto 5^x$, de domaine $\mathbf{N}$, reste un problème ouvert (car équivalent à la conjecture E-W).

5.13. On peut maintenant prouver une partie essentielle du Théorème annoncé en 4.10.

PROPOSITION. *Soit* $\rho$ *une relation définissable dans la structure* $\langle \mathbf{N}; +, \times, = \rangle$. *La relation* $\mathrm{Sat}(\rho)$ *obtenue en saturant* $\rho$ *par la relation* $\cong_{\{0\}}$, *(où* $x \cong_{\{0\}} y$ *signifie* $\mathrm{SUPP}(x) = \mathrm{SUPP}(y)$*) est définissable dans les structures* $\langle \mathbf{N}; S; \perp \rangle$ *et* $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

*Preuve.* Soit $F(x_1, ..., x_k)$ une formule qui définit $\rho$ dans $\langle \mathbf{N}; +; \times, = \rangle$. L'isomorphisme $\mathrm{Exp}_5 : x \mapsto 5^x$ entre $\langle \mathbf{N}; +; \times, = \rangle$ et $\langle 5^{\mathbf{N}}; \mathrm{NA}, \mathrm{NM}; =_{PP} \rangle$ transforme $\rho$ en l'ensemble $5^\rho = \{(5^{x_1}, ..., 5^{x_k}) : (x_1, ..., x_k) \in \rho\}$, et cette image est la partie de $5^{\mathbf{N}^k}$ définie dans la structure $\langle 5^{\mathbf{N}}; \mathrm{NA}, \mathrm{NM}; =_{PP} \rangle$ par la même formule $F(x_1, ..., x_k)$. Comme cette structure est définissable dans $\langle \mathbf{N}; S; \perp \rangle$ et $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$, on voit que $5^\rho$ est aussi définissable avec $\perp$ et $S$ ou Pred. Notons SUPP la fonction support, qui envoie $\mathbf{N} \backslash \{0\}$ dans l'ensemble $\mathscr{P}_f(P)$ des parties finies de $P$. L'isomorphisme $\mathrm{Exp}_5$ transforme SUPP en la fonction NSUPP (nouveau support) qui envoie $5^{\mathbf{N} \backslash \{0\}}$ dans l'ensemble $\mathscr{P}_f(5^P)$ des parties finies de $5^P$ de sorte que, notant $\mathrm{EXP}_5$ la restriction à $\mathscr{P}_f(P)$ de l'extension de $\mathrm{Exp}_5$ aux parties, le diagramme (1) soit commutatif:

Diagramme (1)

$$\begin{array}{ccc} \mathscr{P}_f(P) & \xrightarrow[\mathrm{EXP}_5]{} & \mathscr{P}_f(5^P) \\ {\scriptstyle \mathrm{SUPP}}\uparrow & & \uparrow{\scriptstyle \mathrm{NSUPP}} \\ \mathbf{N}\backslash\{0\} & \xrightarrow[\mathrm{Exp}_5]{} & 5^{\mathbf{N}}\backslash\{1\} \end{array}$$

On observe que

$$\begin{aligned} \mathrm{Sat}(\rho) &= \mathrm{SUPP}^{-1}[\mathrm{SUPP}(\rho)] \\ &= [\mathrm{EXP}_5 \circ \mathrm{SUPP}]^{-1}[\mathrm{EXP}_5 \circ \mathrm{SUPP}](\rho) \\ &= [\mathrm{EXP}_5 \circ \mathrm{SUPP}]^{-1}[\mathrm{NSUPP} \circ \mathrm{Exp}_5](\rho) \\ &= [\mathrm{EXP}_5 \circ \mathrm{SUPP}]^{-1}[\mathrm{NSUPP}](5^\rho) \end{aligned}$$

Chacune des fonctions intervenant dans cette dernière égalité est $(S; \perp)$ et (Pred; $\perp$) définissable:

— c'est évident pour la fonction SUPP,

— ceci résulte de la Proposition 5.12 pour $\mathrm{EXP}_5$ (extension aux parties de la *restriction aux premiers* de $\mathrm{Exp}_5$),

— la fonction NSUPP, définissable dans $\langle 5^{\mathbf{N}}; \mathrm{NA}, \mathrm{NM}; =_{PP}\rangle$ l'est aussi avec $(S; \perp)$ ou (Pred; $\perp$).

La définissabilité de Sat($\rho$) avec $(S; \perp)$ ou (Pred; $\perp$) résulte alors de celle de $5^\rho$.

5.14. On peut enfin prouver le Théorème annoncé en 4.10.

THÉORÈME. *Soit $A$ un ensemble d'entiers de $\mathbf{Z}$. Soit $\rho$ une relation définissable dans la structure $\langle \mathbf{N}; +, \times, =\rangle$, incluse dans $\mathbf{N}^k$, et saturée par la restriction à $\mathbf{N}$ de la relation d'équivalence $\cong_A$ (où $x \cong_A y$ signifie $\mathrm{SUPP}(|x+i|) = \mathrm{SUPP}(|y+i|)$ pour tout $i \in A$, cf. 2.11).*

i) *Si $A$ est fini alors $\rho$ est définissable dans la structure $\langle \mathbf{N}; S, \mathrm{PRED}; \perp\rangle$.*

ii) *Si $A$ est fini et formé d'entiers tous positifs ou nuls, alors $\rho$ est définissable dans la structure $\langle \mathbf{N}; S; \perp\rangle$.*

iii) *Si $A$ est fini et formé d'entiers tous négatifs ou nuls, alors $\rho$ est définissable dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp\rangle$.*

*Preuve.* 1°) Le cas $A = \{0\}$ est réglé par la Proposition 5.13. Le cas où $A$ est vide est trivial car $\rho$ est alors égal à $\mathbf{N}^k$ tout entier.

Si $a \in \mathbf{Z}$ on désigne par $T_a$ la translation $x \mapsto \mathrm{Sup}(x+a, 0)$ de $\mathbf{N}$ dans $\mathbf{N}$. Si $A = \{a_1, ..., a_n\}$, on note $T_A$ l'application $x \mapsto (T_{a_1}(x), ..., T_{a_n}(x))$ de $\mathbf{N}$ dans $\mathbf{N}^n$.

Si $B \subseteq \mathbf{Z}$, (la trace de) l'équivalence $\cong_B$ sur $\mathbf{N}$ s'étend de façon évidente sur $\mathbf{N}^n$. Pour toute relation $\tau$ sur $\mathbf{N}$ on note $\mathrm{Sat}_{\cong_B}(X)$ la relation obtenue en saturant $\tau$ pour (la restriction à $\mathbf{N}$ de) l'équivalence $\cong_B$.
Nous considérons d'abord le cas où $A = \{a_1, ..., a_n\} \subseteq \mathbf{N}$.

2°) Remarquons que si $x$ et $y$ sont dans $\mathbf{N}$ alors $T_A(x) \cong_B T_A(y)$ si et seulement si $x \cong_{A+B} y$, où $A + B = \{a + b : a \in A \text{ et } b \in B\}$. En particulier, $T_A(x) \cong_{\{0\}} T_A(y)$ si et seulement si $x \cong_A y$.

On observe enfin que, pour toute partie $\rho$ de $\mathbf{N}^k$, on a

$$\begin{aligned}\mathrm{Sat}_{\cong_A}(\rho) &= \{(y_1, ..., y_k) : \text{il existe } (x_1, ..., x_k) \in \rho \text{ tel que } y_i \cong_A x_i \\ &\qquad \text{pour } 1 \leqslant i \leqslant k\} \\ &= \{(y_1, ..., y_k) : \text{il existe } (x_1, ..., x_k) \in \rho \text{ tel que } T_A(y_i) \cong_{\{0\}} T_A(x_i) \\ &\qquad \text{pour } 1 \leqslant i \leqslant k\} \\ &= [(T_A, ..., T_A)]^{-1}[\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)(\rho)]] \\ &\qquad (\text{où } (T_A, ..., T_A)(\rho) \text{ est incluse dans } \mathbf{N}^{n \times k}).\end{aligned}$$

3°) Si $\rho$ est définissable dans la structure $\langle \mathbf{N}; +, \times; = \rangle$ alors la relation $\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)(\rho)]$ l'est aussi; étant $\cong_{\{0\}}$ saturée, elle est également (d'après la Proposition 5.13) définissable dans la structure $\langle \mathbf{N}; S; \perp \rangle$.

Par ailleurs, si $a \in \mathbf{N}$, l'application $T_a$ n'est autre que l'itérée d'ordre $a$ de la fonction $S$. La fonction $T_A$ est donc une composée d'itérées de la fonction $S$ avec la fonction de brassage $x \mapsto (x, ..., x)$ de $\mathbf{N}$ dans $\mathbf{N}^n$.

D'après la Proposition 3.6, la famille des relations définissables dans $\langle \mathbf{N}; S; ... \rangle$ est stable par image réciproque par $T_A$ (en termes logiques, si $F(x_1, ..., x_n)$ définit $\tau$ dans $\langle \mathbf{N}; S; ... \rangle$ alors $[(T_A, ..., T_A)]^{-1}(\tau)\, y$ est défini par la formule $F[S^{a_1}(x), ..., S^{a_n}(x)]$).

*Remarque.* Rappelons que l'application $S$ n'est pas — à priori — $(S; \perp)$-définissable (cf. 3.5), il en est donc de même de $T_A$.

Il en résulte que l'ensemble $[(T_A, ..., T_A)]^{-1}[\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)(\rho)]]$, c'est-à-dire $\mathrm{Sat}_{\cong_A}(\rho)$, est définissable dans la structure $\langle \mathbf{N}; S; \perp \rangle$. Si $\rho$ est saturée pour $\cong_A$ alors $\rho = \mathrm{Sat}_{\cong_A}(\rho)$ et est donc $(S; \perp)$-définissable. Ceci achève la preuve de l'assertion ii) du Théorème.

4°) Considérons maintenant le cas où $A = \{a_1, ..., a_n\}$ est formé d'éléments tous négatifs ou nuls. Soit $m$ le plus grand entier positif ou nul tel que $-m$ soit dans $A$. On note $M$ le saturé de $\{0, ..., m\}$ pour $\cong_A$:

$$M = \{x \in \mathbf{N} : \text{il existe } i \in \{0, ..., m\} \text{ tel que } x \cong_A i\}.$$

Si $a \leqslant 0$ alors la fonction $T_a$ est constante de valeur 0 sur $\{0, ..., a\}$ et sa restriction à $\mathbf{N}\backslash\{0, ..., a\}$ est injective et d'image $\mathbf{N}\backslash\{0\}$. On voit ainsi que si $x > m$ alors $T_A^{-1}(x)] = \{x\}$.

De même, si $x > m$ et $y > m$ (en particulier si $x$ et $y$ sont dans $\mathbf{N}\backslash M$) alors, comme plus haut, $T_A(x) \cong_{\{0\}} T_A(y)$ si et seulement si $x \cong_A y$.

On remarque que pour toute partie $\tau$ de $\mathbf{N}^p$ on a

$$\begin{aligned}(\mathbf{N}\backslash M)^p \cap \mathrm{Sat}_{\cong_A}(\tau) &= \mathrm{Sat}_{\cong_A}[(\mathbf{N}\backslash M)^p \cap \tau] \\ &= \{(y_1, ..., y_p) \in (\mathbf{N}\backslash M)^p : \text{il existe } (x_1, ..., x_p) \in (\mathbf{N}\backslash M)^p \cap \tau \\ &\quad \text{tel que } y_i \cong_A x_i \text{ pour } 1 \leqslant i \leqslant p\} \\ &= \{(y_1, ..., y_p) \in (\mathbf{N}\backslash M)^p : \text{il existe } (x_1, ..., x_p) \in (\mathbf{N}\backslash M)^p \cap \tau \\ &\quad \text{tel que } T_A(y_i) \cong_{\{0\}} T_A(x_i) \text{ pour } 1 \leqslant i \leqslant p\} \\ &= [(T_A, ..., T_A)]^{-1}[\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)((\mathbf{N}\backslash M)^p \cap \tau)]] .\end{aligned}$$

5°) Si $\tau$ est définissable dans $\langle \mathbf{N}; +, \times; = \rangle$ alors la relation

$$\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)((\mathbf{N}\backslash M)^p \cap \tau)]$$

(qui est incluse dans $\mathbf{N}^{n \times k}$) l'est aussi. Etant $\cong_{\{0\}}$ saturée, elle est également (d'après la Proposition 5.13) définissable dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

D'autre part, si $a \leqslant 0$, l'application $T_a$ n'est autre que l'itérée d'ordre $|a|$ de la fonction Pred. Comme en 3°), on voit que la famille des relations définissables dans $\langle \mathbf{N}; \mathrm{Pred}; ... \rangle$ est stable par image réciproque par $T_A$.

Ainsi,

$$[(T_A, ..., T_A)]^{-1}[\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)((\mathbf{N}\backslash M)^p \cap \tau)]] ,$$

c'est-à-dire $(\mathbf{N}\backslash M)^p \cap \mathrm{Sat}_{\cong_A}(\tau)$, est définissable dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

Ceci prouve que

*si* $\tau \subseteq \mathbf{N}^p$ *est saturée pour* $\cong_A$ *alors* $(\mathbf{N}\backslash M)^p \cap \tau$ *est* (Pred; $\perp$)-*définissable.*

6°) Soit $\rho$ une partie de $\mathbf{N}^k$.

Si $I = \{i_1, ..., i_t\}$, où $i_1 < ... < i_t$, est incluse dans $\{1, ..., k\}$, on note $\mathrm{Proj}_I$ la fonction $(x_1, ..., x_k) \mapsto (x_{i_1}, ..., x_{i_t})$ de $\mathbf{N}^k$ sur $\mathbf{N}$.

Si $\tau \subseteq \mathbf{N}^t$, on note $\mathrm{Ext}_I(\tau)$ l'ensemble

$$\begin{aligned}\mathrm{Ext}_I(\tau) = \{(x_1, ..., x_k) : \mathrm{Proj}_I[(x_1, ..., x_k)] \in \tau \quad \text{et} \quad x_i \in M \\ \text{pour tout } i \in \{1, ..., k\}\backslash I\} .\end{aligned}$$

Comme $M$ est saturée pour $\cong_A$, on voit que pour toute partie $\rho$ de $\mathbf{N}^k$ on a

$$(*) \qquad \mathrm{Sat}_{\cong_A}(\rho) = \bigcup_{I \subseteq \{1,\ldots,k\},\, p=|I|} \mathrm{Ext}_I[(\mathbf{N}\backslash M)^p \cap \mathrm{Proj}_I[\mathrm{Sat}_{\cong_A}(\rho)]] .$$

On note $K_{i,a}$ l'ensemble $K_{i,a} = \{x > m : \mathrm{SUPP}(x+a) = \mathrm{SUPP}(|i+a|)\}$. Il est clair que si $-m \leqslant a \leqslant 0$ l'ensemble $K_{i,a}$ est (Pred; $\perp$)-définissable. Comme $M = [M \cap \{0, 1, ..., m\}] \cup [\bigcup_{1 \leqslant i \leqslant m} \bigcap_{a \in A} K_{i,a}]$, on en déduit que $M$ est (Pred; $\perp$)-définissable.

Il en résulte que si $X$ est (Pred; $\perp$)-définissable alors il en est de même des $\mathrm{Ext}_I(X)$.

7°) On peut maintenant achever la preuve du point iii) du Théorème. Si $\rho$ est saturée pour $\cong_A$ alors les $\mathrm{Proj}_I[\mathrm{Sat}_{\cong_A}(\rho)]$ le sont aussi. Le point 5°) montre que les $(\mathbf{N}\backslash M)^p \cap \mathrm{Proj}_I[\mathrm{Sat}_{\cong_A}(\rho)]$ sont (Pred; $\perp$)-définissables, il en résulte que les $\mathrm{Ext}_I[(\mathbf{N}\backslash M)^p \cap \mathrm{Proj}_I[\mathrm{Sat}_{\cong_A}(\rho)]]$ le sont aussi, et donc également $\rho$.

8°) Dans le cas général où $A$ comprend des éléments positifs et d'autres négatifs, on raisonne comme dans les points 4°) à 7°). Cependant, la fonction $T_A$ est, dans ce cas, une composée d'itérées des deux fonctions $S$ et Pred avec la fonction de brassage $x \mapsto (x, ..., x)$ de $\mathbf{N}$ dans $\mathbf{N}^n$. C'est donc alors la famille des relations définissables dans $\langle \mathbf{N}; S, \mathrm{Pred}; ... \rangle$ qui est stable par image réciproque par $T_A$. D'où la nécessité (à priori) d'introduire le langage ($S$, Pred; $\perp$).

## § 6. L'ÉGALITÉ ET LE PROBLÈME DE J. ROBINSON

6.1. Le résultat ci-dessous — à priori technique — s'avère être un outil performant dans l'étude du rôle de l'égalité en face de $S$ et $\perp$.

*Définition.* Soit $A$ une partie finie de $\mathbf{Z}$. Une relation $\rho$, incluse dans $\mathbf{N}^{k+1}$, est dite *quasi-saturée* pour $\cong_A$ si elle est saturée en toutes ses variables sauf peut-être la première, c'est-à-dire que lorsque $x_i \cong_A y_i$ pour $1 \leqslant i \leqslant k$, alors les $(k+1)$-uplets $(z, x_1, ..., x_k)$ et $(z, y_1, ..., y_k)$ sont simultanément dans $\rho$ ou hors de $\rho$.

*Exemple.* D'après la Proposition 2.13, toutes les parties de $\mathbf{N} \times PP^k$ (où $PP$ est l'ensemble des primaires) sont quasi-saturées pour $\cong_A$ si $A$ contient $\{0, 1, 2\}$ ou $\{-2, -1, 0\}$.

LEMME. *Soit $A$ une partie finie de $\mathbf{Z}$. Soient $\rho_1, ..., \rho_p, \theta$ des relations définissables dans la structure $\langle \mathbf{N}; +, \times; = \rangle$ et chacune quasi-*

*saturée pour* $\cong_A$. *On suppose que* $\theta$ *est incluse dans* $\mathbf{N}^2$ *et que la deuxième projection* $\Delta$ *de* $\theta$ *(i.e.* $\Delta = \{x_0$: il existe $x$ tel que $(x, x_0) \in \theta\}$*) est une partie de* $\mathbf{N}$ *définissable dans* $\langle \mathbf{N}; S, \mathrm{Pred}; \bot \rangle$.

*Si* $\tau$ *est une relation définissable dans* $\langle \mathbf{N}; S, \mathrm{Pred}; \bot, \rho_1, ..., \rho_p \rangle$ *et incluse dans* $\mathbf{N}^n$, *alors les relations*

$$\tau' = \{(x_0, x_1, ..., x_{n-1}) : \text{ il existe } x \text{ tel que } (x, x_0) \in \theta \text{ et } (x, x_1, ..., x_{n-1}) \in \tau\},$$

$$\tau'' = \{(x_0, x_1, ..., x_{n-1}) : x_0 \in \Delta \text{ et, pour tout } x, \text{ si } (x, x_0) \in \theta \text{ alors } (x, x_1, ..., x_{n-1}) \in \tau\}$$

*sont également définissables dans la structure* $\langle \mathbf{N}; S, \mathrm{Pred}; \bot, \rho_1, ..., \rho_p \rangle$ *(c'est-à-dire sans faire intervenir la relation* $\theta$*).*

*Preuve.* 1°) Le fait que $\Delta$ soit la deuxième projection de $\theta$ et la quasi-saturation de $\theta$ pour $\cong_A$ montrent que $\Delta$ est $(\cong_A)$-saturé. Comme, relativement à $\tau'$ et $\tau''$, la variable $x_0$ varie dans $\Delta$, on voit que $\tau'$ et $\tau''$ sont $(\cong_A)$-saturées par rapport à $x_0$.

2°) Si $X$ est une partie de $\mathbf{Z}$, posons $T_{i,j}(X) = \{-j, ..., 0\} \cup [X + \{i-j\}]$. Si $u \cong_{T_{i,j}(X)} v$ alors (cf. la preuve de 4.11) on voit facilement que

— si $x \leqslant j$ ou $y \leqslant j$ alors $T_{i,j}(X)$ contient $-x$ ou $-y$ et donc $x = y$,

— $x + (i-j) \cong_X y + (i-j)$.

Il en résulte que $S^i[\mathrm{Pred}^j(u)] \cong_X S^i[\mathrm{Pred}^j(v)]$.

3°) Par récurrence sur la complexité de la formule $F(x_0, x_1, ..., x_{n-1})$ qui définit $\tau$ dans $\langle \mathbf{N}; S, \mathrm{Pred}; \bot, \rho_1, ..., \rho_p \rangle$, on construit des formules $F'$ et $F''$ qui définissent $\tau'$ et $\tau''$ dans cette même structure.

L'étape d'induction, c'est-à-dire l'introduction des connecteurs et quantificateurs (qui, en termes ensemblistes (cf. 3.6), correspond aux opérations booléennes et aux projections) est évidente: si $D(x_0)$ définit $\Delta$ avec $S$, Pred et $\bot$, alors

$$(\exists x_i F)' \text{ est } \exists x_i(F'), (F \vee G)' \text{ est } F' \vee G', (\neg F)' \text{ est } \neg(F'') \wedge D(x_0);$$

$$(\forall x_i F)'' \text{ est } \forall x_i(F''), (F \wedge G)'' \text{ est } F'' \wedge G'', (\neg F)'' \text{ est } \neg(F') \wedge D(x_0).$$

L'étape initiale de la récurrence concerne les formules atomiques, c'est-à-dire les relations $\tau$ qui sont images réciproques des relations $\bot, R_1, ..., R_p$ par les composées des fonctions $S$ et Pred avec les fonctions de brassage. Les termes du langage $(S, \mathrm{Pred}; \bot, R_1, ..., R_p)$ se ramènent (après simplification des $\mathrm{Pred} \circ S$) à ceux de la forme $t(x) = S^i[\mathrm{Pred}^j(x)]$ où $x$ est une variable. D'où les différents cas considérés ci-dessous.

4°) *Cas où* $F$ *est* $t(x_0) \perp u(x_0)$

Dans ce cas $\tau'$ et $\tau''$ ne comportent qu'un seul argument et le point 1°) montre qu'elles sont $(\cong_A)$-saturées et donc, d'après le Théorème 4.10, définissables dans la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$.

5°) *Cas où* $F$ *est* $t_0(x_0) \perp t_1(x_1)$

Si le terme $t_1(x_1)$ est $S^i[\mathrm{Pred}^j(x_1)]$ alors la $(\cong_{\{0\}})$-saturation de $\perp$ implique la $(\cong_{T_{i,j}(\{0\})})$-saturation par rapport à $x_1$ de la relation $\tau$ et donc aussi de $\tau'$ et $\tau''$. Compte tenu de 1°), les relations $\tau'$ et $\tau''$ sont $(\cong_{T_{i,j}(\{0\})A})$-saturées, et donc (Théorème 4.10) définissables dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$.

6°) *Cas où* $F(x_0, x_1, ..., x_{n-1})$ *est* $R_\alpha(t_1[x_{\sigma(1)}], ..., t_{k_\alpha}[x_{\sigma(k_\alpha)}])$, *où* $1 \leqslant \alpha \leqslant p - 1$, $\sigma: \{1, ..., k_\alpha\} \to \{0, ..., n-1\}$ *et* $\sigma(1) = 0$.

Si $t_{i_r, j_r}(x_{\sigma(r)})$ est $S^{i_r}[\mathrm{Pred}^{j_r}(x_{\sigma(i)})]$, on pose $B = T_{i_1, j_1}(A) \cup ... \cup T_{i_{k_\alpha}, j_{k_\alpha}}(A)$. De la $(\cong_A)$-quasi-saturation de l'interprétation $\rho_\alpha$ de $R_\alpha$, on déduit la $(\cong_B)$-saturation de $\tau$ par rapport aux variables $x_i$ telles que $i \neq \sigma(1) = 0$, et donc aussi le même résultat relatif à $\tau'$ et $\tau''$. Le point 1°) assure alors que $\tau'$ et $\tau''$ sont $(\cong_{B \cup A})$-saturées et donc (Théorème 4.10) définissables dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$.

7°) *Cas où* $F(x_0, x_1, ..., x_{n-1})$ *est* $R_\alpha(t_1[x_{\sigma(1)}], ..., t_{k_\alpha}[x_{\sigma(k_\alpha)}])$, *où* $1 \leqslant \alpha \leqslant p - 1$, $\sigma: \{1, ..., k_\alpha\} \to \{0, ..., n-1\}$ *et* $\sigma(1) \neq 0$.

Soit $B$ défini comme au point 6°). On pose

$$\lambda = \{(z, x_0): \text{il existe } x \text{ tel que } z \cong_B x \text{ et } (x, x_0) \in \theta\}.$$

Comme $\theta$ est $(\cong_A)$-quasi-saturée, $\lambda$ est $(\cong_{B \cup A})$-saturée et donc (Théorème 4.10) définissable dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$. La $(\cong_A)$-quasi-saturation de $\rho_\alpha$ montre la $(\cong_B)$-saturation de $\tau$ par rapport aux variables $x_i$ telles que $i \neq \sigma(1)$, en particulier celles telles que $\sigma(i) = 0$ (car $\sigma(1) \neq 0$). On a donc

$$\begin{aligned}
\tau' &= \{(x_0, x_1, ..., x_{n-1}): \text{il existe } x \text{ tel que } (x, x_0) \in \theta \text{ et } (y_1, ..., y_{k_\alpha}) \in \rho_\alpha \text{ où} \\
&\qquad y_i \text{ vaut } t_i[x_{\sigma(i)}] \text{ si } \sigma(i) \neq 0 \text{ et vaut } t_i[x] \text{ si } \sigma(i) = 0\}, \\
&= \{(x_0, x_1, ..., x_{n-1}): \text{il existe } z \text{ tel que } (z, x_0) \in \lambda \text{ et } (y_1, ..., y_{k_\alpha}) \in \rho_\alpha \text{ où} \\
&\qquad y_i \text{ vaut } t_i[x_{\sigma(i)}] \text{ si } \sigma(i) \neq 0 \text{ et vaut } t_i[z] \text{ si } \sigma(i) = 0\}. \\
\tau'' &= \{(x_0, x_1, ..., x_{n-1}): x_0 \in \Delta \text{ et pour tout } x, \text{ si } (x, x_0) \in \theta \text{ alors} \\
&\qquad (y_1, ..., y_{k_\alpha}) \in \rho_\alpha \text{ où } y_i \text{ vaut } t_i[x_{\sigma(i)}] \text{ si } \sigma(i) \neq 0 \text{ et vaut} \\
&\qquad t_i[x] \text{ si } \sigma(i) = 0\}, \\
&= \{(x_0, x_1, ..., x_{n-1}): x_0 \in \Delta \text{ et pour tout } z, \text{ si } (z, x_0) \in \lambda \text{ alors} \\
&\qquad (y_1, ..., y_{k_\alpha}) \in \rho_\alpha \text{ où } y_i \text{ vaut } t_i[x_{\sigma(i)}] \text{ si } \sigma(i) \neq 0 \text{ et vaut} \\
&\qquad t_i[z] \text{ si } \sigma(i) = 0\}.
\end{aligned}$$

Ces égalités donnent des définitions de $\tau'$ et $\tau''$ à partir de $\Delta$, $\lambda$ et $\rho_\alpha$, et donc (puisque $\Delta$ et $\lambda$ sont définissables avec $S$, Pred et $\perp$) des définitions de $\tau'$ et $\tau''$ dans $\langle \mathbf{N}; S, \text{Pred}; \perp, \rho_\alpha \rangle$.

6.2. Le résultat suivant est une extension du Théorème de Woods sur l'équivalence du Problème de Robinson et de la $(S; \perp)$-définissabilité de l'égalité.

THÉORÈME. *Soient* $\rho_1, ..., \rho_p, \varphi_1, ..., \varphi_q$ *des relations et fonctions définissables dans* $\langle \mathbf{N}; +, \times; = \rangle$. *On suppose que* $\rho_1, ..., \rho_p$ *et les graphes de* $\varphi_1, ..., \varphi_q$ *sont quasi-saturés pour* $\cong_A$ *où* $A$ *est une partie finie de* $\mathbf{Z}$ *(c'est le cas, en particulier, si ces relations et graphes sont inclus dans un produit* $\mathbf{N} \times [PP^k + B]$ *où* $B$ *est une partie finie de* $\mathbf{Z}$*).*

*Si l'égalité est définissable dans* $\langle \mathbf{N}; S, \text{Pred}, \varphi_1, ..., \varphi_q; \perp, \rho_1, ..., \rho_p \rangle$ *(resp.* $\langle \mathbf{N}; S, \varphi_1, ..., \varphi_q; \perp, \rho_1, ..., \rho_p \rangle$, *resp.* $\langle \mathbf{N}; \text{Pred}, \varphi_1, ..., \varphi_q; \perp, \rho_1, ..., \rho_p \rangle$*) alors cette structure définit les mêmes relations et fonctions que* $\langle \mathbf{N}; +, \times; = \rangle$.

*Preuve.* Appliquons le Lemme 6.1 avec les relations $\rho_i$ et les graphes des $\varphi_j$, et, pour $\tau$ la relation d'égalité, pour $\theta$ le graphe de la fonction $x \mapsto 5^x$ (graphe qui est bien quasi-saturé puisque son second argument est toujours un primaire). On observe que $\tau'$ est l'image de $\theta$ par la fonction de brassage $(x, y) \mapsto (y, x)$. La $\langle \mathbf{N}; S, \text{Pred}; \perp, \rho_1, ..., \rho_p, Gr(\varphi_1), ... Gr(\varphi_q) \rangle$-définissabilité de $\tau'$, et donc de $\theta$, permet de conclure à celle de $+$ et $\times$, grâce à la Proposition 5.12.

On achève la preuve en observant que la définissabilité de l'égalité dans la structure $\langle \mathbf{N}; S, \text{Pred}, \varphi_1, ..., \varphi_q; \perp, \rho_1, ..., \rho_p \rangle$ montre l'équivalence de cette structure et de $\langle \mathbf{N}; S, \text{Pred}; \perp, \rho_1, ..., \rho_p, Gr(\varphi_1), ... Gr(\varphi_q) \rangle$.

On remarque enfin que si l'égalité est définissable avec les $\rho_i$, $\varphi_j$, $\perp$ et $S$ sans l'aide de Pred (resp. avec Pred sans l'aide de $S$) alors la fonction Pred (resp. $S$) l'est aussi.

*Remarque.* Considérant pour $\rho$ la relation d'égalité, on voit que la condition de quasi-saturation des $\rho_\alpha$ ne peut pas être levée dans le Lemma 6.1 ni dans le présent Théorème (sauf si la conjecture d'Erdös-Woods est vraie!).

6.3. Une application simple du Théorème 6.2 est la suivante:

THÉORÈME. *Soit* $J$ *une injection de domaine* $\mathbf{N}$ *à valeurs dans les primaires et définissable dans* $\langle \mathbf{N}; +, \times; = \rangle$.

*Les trois structures* $\langle \mathbf{N}; S, J; \perp \rangle$, $\langle \mathbf{N}; \mathrm{Pred}, J; \perp \rangle$ *et* $\langle \mathbf{N}; +, \times; = \rangle$ *définissent les mêmes relations et fonctions.*

*Preuve.* La relation d'égalité est définissable dans la structure $\langle \mathbf{N}; S, J; \perp \rangle$ par la formule $J(x) =_{PP} J(y)$ (cf. 5.5 pour la définition de $=_{PP}$). On conclut en appliquant le Théorème 6.2 avec pour $\rho$ le graphe de $J$ (qui est quasi-saturé car à valeurs dans les primaires).

6.4. Une autre application simple du Théorème 6.2 est la suivante:

Soit EXP la relation binaire $\mathrm{EXP} = \{(x, y)$: il existe $a \geqslant 0$ tel que $y = a^x\}$.

THÉORÈME. *Les trois structures* $\langle \mathbf{N}; S; \perp, \mathrm{EXP} \rangle$, $\langle \mathbf{N}; S; \perp, \mathrm{EXP} \rangle$ *et* $\langle \mathbf{N}; +, \times; = \rangle$ *définissent les mêmes relations et fonctions.*

*Preuve.* On considère seulement le cas $(S; \perp, \mathrm{EXP})$. Soit $A$ l'ensemble $A = \mathrm{EXP} \cap [\mathbf{N} \times PP] = \{(x, p^x)$: $x \in \mathbf{N}$ et $p \in P\}$. On observe que l'égalité $x = y$ équivaut à l'existence d'un $z$ tel que $(x, z)$ et $(y, z)$ soient dans $A$. L'égalité est donc définissable dans la structure $\langle \mathbf{N}; S; \perp, A \rangle$.

Comme $A$ est incluse dans $\mathbf{N} \times PP$, elle est quasi-saturée pour $\cong_{\{0,1,2\}}$, et le Théorème 6.2 montre que $+$ et $\times$ sont définissables dans la structure $\langle \mathbf{N}; S; \perp, A \rangle$. On conclut en remarquant que la relation $A$ est elle-même définissable dans la structure $\langle \mathbf{N}; S; \perp, \mathrm{EXP} \rangle$ par la formule $PP(y) \wedge \mathrm{EXP}(x, y)$.

6.5. Le Théorème ci-dessous est un fait curieux que l'on peut énoncer ainsi:

*bien qu'il apparaisse difficile de la définir avec successeur et coprimarité, la relation d'égalité n'a pourtant pas un pouvoir de définissabilité important, sa contribution — en face de* $S$ *et* $\perp$ *— se limite à se définir elle-même ainsi que le graphe des itérés de* $S$ *et elle n'est pas en mesure d'utiliser la puissance des quantifications!*

THÉORÈME. *Toute formule du langage* $(S, \mathrm{Pred}; =, \perp)$ *équivaut à une combinaison booléenne de formules du langage* $(S, \mathrm{Pred}; \perp)$ *— formules sans égalité — et de formules du type* $x = S^i(y)$ *(resp.* $x = \mathrm{Pred}^i(y)$*) — formules sans quantificateur —.*

*En termes ensemblistes, la classe des relations* $\langle \mathbf{N}; S, \mathrm{Pred}; =, \perp \rangle$*-définissables coïncide avec la classe des relations obtenues par combinaisons booléennes*

— *des relations définissables dans la structure* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$,

— *des graphes des itérées de la fonction successeur (resp. prédécesseur) et leurs images réciproques par les fonctions* $f_{p,\alpha,\beta}: (x_1, ..., x_p) \mapsto (x_\alpha, x_\beta)$ *où* $1 \leqslant \alpha \leqslant p, 1 \leqslant \beta \leqslant p, \alpha \neq \beta$.

*Preuve.* 1°) On commence par montrer que toute formule du langage $(S, \mathrm{Pred}; =, \perp)$ équivaut à une formule de ce même langage dont les sous-formules atomiques sont particulièrement simples. C'est l'objet des points 2°) à 4°).

2°) Si $t_1$ et $t_2$ sont des termes, les formules $t_1 \perp t_2$ et $t_1 = t_2$ sont équivalentes à

$$\exists z_1 \exists z_2 [(z_1 = t_1) \wedge (z_2 = t_2) \wedge (z_1 \perp z_2)] \quad \text{et} \quad \exists z_1 \exists z_2 [(z_1 = t_1) \wedge (z_2 = t_2) \wedge (z_1 = z_2)] .$$

Toute formule est donc équivalente à une autre dans laquelle les sous-formules atomiques sont toutes de la forme $t = x$ ou $x \perp y$ où $t$ est un terme et $x, y$ sont des variables.

3°) Comme $\mathrm{Pred} \circ S$ est l'identité, on peut se ramener au cas où tous les termes sont de la forme $S^i[\mathrm{Pred}^j(z)]$ où $z$ est une variable.

4°) On a déjà vu (cf. 5.3) que tout singleton, et donc toute relation finie ou cofinie, est définissable avec $\perp$ et $S$ ou Pred.

Comme $S^i[\mathrm{Pred}^j(z)]$ vaut $i$ si $z \leqslant j$ et vaut $z + i - j$ si $z \geqslant j$, la formule $S^i[\mathrm{Pred}^j(z)] = x$ est équivalente à :

$$\begin{aligned}
&[(x = z) \wedge (z \geqslant j)] \vee [(x = i) \wedge (z \leqslant j)] && \text{si} \quad i = j , \\
&[(x = \mathrm{Pred}^{j-1}(z)) \wedge (z \geqslant j)] \vee [(x = i) \wedge (z \leqslant j)] && \text{si} \quad i < j , \\
&[(x = S^{i-j}(z)) \wedge (z \geqslant j)] \vee [(x = i) \wedge (z \leqslant j)] && \text{si} \quad i > j .
\end{aligned}$$

Ces formules sont de la forme $[(t = x) \wedge A(x)] \vee B(x, z)$ où $A$ et $B$ sont écrites avec Pred et $\perp$, et $t$ est un terme du type $S^k(z)$ ou $\mathrm{Pred}^k(z)$.

Notons enfin que la formule $x = x$ est toujours vraie et équivaut à $\neg(x \perp x)$; si $k \neq 0$, la formule $x = S^k(x)$ est toujours fausse et équivaut à $(x \perp x) \wedge \neg(x \perp x)$, la formule $x = \mathrm{Pred}^k(x)$ équivaut à $x = 0$.

On voit donc que

(*) *Toute formule est équivalente à une formule dont les sous-formules atomiques sont toutes de la forme* $x = S^k(y)$ *ou* $x = \mathrm{Pred}^k(y)$ *ou encore* $x \perp z$, *où* $x, y$ *sont des variables distinctes,* $z$ *une variable et* $k \geqslant 0$.

5°) Notons enfin que la formule $x = S^k(y)$ est équivalente à $(y = \mathrm{Pred}^k(x)) \wedge (x \geqslant k)$, laquelle est de la forme $(y = \mathrm{Pred}^k(x)) \wedge A(x)$, où $A$ est écrite avec Pred et $\perp$ (et sans égalité).

De même, la formule $x = \mathrm{Pred}^k(y)$ est équivalente à $(y = S^k(x)) \vee [(x = 0) \wedge (y \leqslant k)]$, de la forme $(y = \mathrm{Pred}^k(x)) \wedge B(x, y)$ où $B$ est écrite sans égalité. Ainsi, on peut donc échanger les sous-formules $x = \mathrm{Pred}^k(y)$ et $y = S^k(x)$, modulo l'introduction d'autres sous-formules du langage (Pred, $\perp$) ou ($S$, $\perp$).

6°) Le point 5°) montre qu'il suffit, pour prouver le Théorème, de pouvoir associer à toute formule $F(x_1, ..., x_p)$ du langage ($S$, Pred; $=$, $\perp$) une formule *équivalente* $F'(x_1, ..., x_p)$ qui est combinaison booléenne de formules du langage ($S$, Pred, $\perp$) et de formules du type $S^i(x) = y$ ou $\mathrm{Pred}^i(x) = y$, où $x, y$ sont des variables. Les points 2°) à 4°) montrent que l'on peut se restreindre aux formules $F(x_1, ..., x_p)$ du langage ($S$, Pred; $=$, $\perp$) qui ont la propriété (*).

La construction procède alors par récurrence sur la complexité de $F$.

7°) L'initialisation de la récurrence indiquée en 6°) est l'étude du cas des formules atomiques. Puisque $F$ vérifie (*), les seuls cas à étudier sont $x = S^k(y)$, $x = \mathrm{Pred}^k(y)$ et $x \perp y$; il est évident qu'il suffit de prendre alors $F'$ égale à $F$.

8°) L'étape d'induction de cette récurrence concerne l'introduction des connecteurs et du quantificateur existentiel.

Le passage aux connecteurs est évident: $(\neg F)'$ est $\neg(F')$, etc.

Le passage au quantificateur existentiel est l'objet des points ci-dessous.

9°) Soit $F(x_1, ..., x_p, x_{p+1})$ une formule du langage ($S$, Pred, $=$, $\perp$) pour laquelle est déjà construite la formule équivalente $F'$ de la forme indiquée en 6°). On cherche à construire $[\exists x_{p+1} F(x_1, ..., x_p, x_{p+1})]'$.

Utilisant 5°) pour les sous-formules $\mathrm{Pred}^k(x_i) = x_j$, $S^k(x_{p+1}) = x_j$ et $\mathrm{Pred}^k(x_{p+1}) = x_j$ de $F'$, on voit que $F'$, et donc aussi $F$, équivaut à une combinaison booléenne de formules du langage ($S$, Pred, $\perp$) et de formules des types $S^k(x_i) = x_j$, $S^k(x_i) = x_{p+1}$ et $\mathrm{Pred}^k(x_i) = x_{p+1}$, où $i \leqslant p$ et $j \leqslant p$.

Rappelons que toute combinaison booléenne de formules se ramène à une disjonction de conjonctions de ces formules et de leurs négations. D'autre part, toute conjonction $(t_1 = x_{p+1}) \wedge R(t_2, x_{p+1})$ équivaut à

$$(t_1 = x_{p+1}) \wedge R(t_2, t_1).$$

Enfin, toute conjonction $(t_1 \neq x_{p+1}) \wedge (t_2 \neq x_{p+1})$ équivaut à

$$[(t_1 \neq x_{p+1}) \wedge (t_1 = t_2)] \vee [(t_1 \neq x_{p+1}) \wedge (t_2 \neq x_{p+1}) \wedge (t_1 \neq t_2)].$$

Ceci montre que *la formule* $F'$, et donc aussi $F$, *équivaut à la disjonction d'une famille de formules* $H_\alpha(x_1, ..., x_p) \wedge F_\alpha(x_1, ..., x_p, x_{p+1})$, $\alpha \in A$ ($A$ *fini*),

*où* $H_\alpha$ *est une conjonction de formules* $S^k(x_i) = x_j, i \leqslant p, j \leqslant p$, *et de leurs négations, et chacune des* $F_\alpha$ *est de l'une des deux formes suivantes:*

$$G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge [(s_\alpha = x_{p+1})]$$

*ou* $$G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge [\bigwedge_{u \in U_\alpha} (t_u \neq x_{p+1})] \wedge [\bigwedge_{u \in U_\alpha, v \in U_\alpha, u \neq v} (t_u \neq t_u)]$$

*où* $G_\alpha$ *est une formule du langage* $(S, \mathrm{Pred}, \perp)$, $s_\alpha$ *et* $t_u$ *sont des termes de la forme* $S^k(x_i)$ *ou* $\mathrm{Pred}^k(x_i)$, *avec* $i \leqslant p$.

10°) Comme la quantification existentielle commute avec la disjonction, la formule $\exists x_{p+1} F$ équivaut à la disjonction des $\exists x_{p+1}(H_\alpha \wedge F_\alpha)$. La construction de $[\exists x_{p+1} F]'$ peut ainsi être ramenée à celle des $[\exists x_{p+1}(H_\alpha \wedge F_\alpha)]'$ (dont ce sera la disjonction).

Comme $H_\alpha(x_1, ..., x_p)$ ne dépend pas de $x_{p+1}$, la formule $\exists x_{p+1}(H_\alpha \wedge F_\alpha)$ équivaut à $H_\alpha(x_1, ..., x_p) \wedge \exists x_{p+1} F_\alpha$. La construction de $[\exists x_{p+1}(H_\alpha \wedge F_\alpha)]'$ peut ainsi être ramenée à celle de $[\exists x_{p+1} F_\alpha]'$ (dont ce sera la conjonction avec $H_\alpha$).

11°) Le cas où $F_\alpha$ est de la forme $G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge [(s_\alpha = x_{p+1})]$ est trivial: la formule $\exists x_{p+1} F_\alpha$ équivaut alors à $G_\alpha(x_1, ..., x_p, s_\alpha)$, laquelle est de la forme demandée en 6°) et peut être prise pour $[\exists x_{p+1} F_\alpha]'$.

12°) Etudions maintenant le cas où $F_\alpha$ est de la forme

$$G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge [\bigwedge_{u \in U_\alpha} (t_u \neq x_{p+1})] \wedge [\bigwedge_{u \in U_\alpha, v \in U_\alpha, u \neq v} (t_u \neq t_u)]$$

D'après la Proposition 4.11 il existe une partie finie $A$ de $\mathbf{Z}$ telle que la relation définie par la formule $G_\alpha$ soit $(\cong_A)$-saturée. La relation $\cong_A$ est évidemment définissable dans le langage $(S, \mathrm{Pred}, \perp)$. Pour tout entier $k \geqslant 1$, l'ensemble $\{x \in \mathbf{N}$: la classe de $x$ pour $\cong_A$ contient exactement $k$ éléments$\}$ est $(\cong_A)$-saturé. Le Théorème 4.10 assure donc qu'il est définissable par une formule, notée $EQ_k(x)$, du langage $(S, \mathrm{Pred}, \perp)$. Si $X$ est un ensemble fini nous notons $|X|$ le nombre de ses éléments. On considère les formules $\theta$, $\varphi_{u,X}$ et $\psi_{u,X}$ suivantes, où $u \in U_\alpha$ et $X \subseteq U_\alpha$:

$$\bigwedge_{v \in U_\alpha} (x_{p+1} \ncong_A t_v), (x_{p+1} \cong_A t_u)] \wedge [\bigwedge_{v \in X} (t_v \cong_A t_u)] \wedge [\bigwedge_{w \notin X} (t_w \ncong_A t_u)] \wedge EQ_{|X|}(t_u)$$

et

$$(x_{p+1} \cong_A t_u)] \wedge [\bigwedge_{v \in X} (t_v \cong_A t_u)] \wedge [\bigwedge_{w \notin X} (t_w \ncong_A t_u)] \wedge \neg EQ_{|X|}(t_u).$$

La disjonction de ces formules, quand $u$ varie dans $U_\alpha$ et $X$ dans les parties de $U_\alpha$, est une tautologie.

La construction de $[\exists x_{p+1} F_\alpha]'$ peut ainsi être ramenée à celle des $[\exists x_{p+1}(F_\alpha \wedge \theta)]'$, $[\exists x_{p+1}(F_\alpha \wedge \varphi_{u,X})]'$, $[\exists x_{p+1}(F_\alpha \wedge \psi_{u,X})]'$ (dont ce sera la disjonction).

13°) On observe que les clauses $t_u \neq x_{p+1}$ de $F_\alpha$ sont trivialement impliquées par $\theta$ et peuvent donc être supprimées dans la formule $F_\alpha \wedge \theta$. Cette dernière équivaut donc à $G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge L_\alpha$ où $L_\alpha$ est la conjonction des $t_u \neq t_v$ (où ne figure pas $x_{p+1}$). Ainsi, $\exists x_{p+1}(F_\alpha \wedge \theta)$ équivaut à $L_\alpha \wedge \exists x_{p+1} G_\alpha$. Il est clair que cette dernière formule est de la forme demandée en 6°) et peut être prise pour $[\exists x_{p+1}(F_\alpha \wedge \theta)]'$.

14°) On observe que la formule $F_\alpha \wedge \varphi_{u,X}$ est toujours fausse car $\varphi_{u,X}$ implique que la classe de $t_u$ pour $\cong_A$ est l'ensemble des $t_v$, $v \in X$, et donc que $x_{p+1}$ est égal à l'un d'eux, ce qui contredit une des clauses de $F_\alpha$. On peut donc prendre pour $[\exists x_{p+1}(F_\alpha \wedge \varphi_{u,X})]'$ une formule comme $x_1 \neq x_1$.

15°) La relation définie par $G_\alpha$ étant $(\cong_A)$-saturée et $\psi_{u,X}$ impliquant $x_{p+1} \cong_A t_u$, les formules $G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge \psi_{u,X}$ et $G_\alpha(x_1, ..., x_p, t_u) \wedge \psi_{u,X}$ sont équivalentes. Notons $\rho_{u,X}$ la conjonction des clauses $t_v \cong_A t_u$, $t_w \ncong_A t_u$ et $\neg EQ_{|X|}(t_u)$ de $\psi_{u,X}$ ($v \in X$ et $w \notin X$). Cette formule assure que la classe de $t_u$ pour $\cong_A$ contient un élément $z$ différent des $t_v$, $v \in X$. Un tel élément $z$ est nécessairement également différent des $t_w$, $w \notin X$ (lesquels ne sont pas dans la classe de $t_u$). Ainsi, $\rho_{u,X}$ implique $\exists z[(z \cong_A t_u) \wedge \bigwedge_{v \in U_\alpha} (t_v \neq z)]$.

Observons que $F_\alpha \wedge \psi_{u,X}$ est équivalente à une formule de la forme

$$M_\alpha(x_1, ..., x_p) \wedge [(x_{p+1} \cong_A t_u)] \wedge \bigwedge_{v \in U_\alpha} (t_v \neq x_{p+1})],$$

où $M_\alpha$, qui contient $\rho_{u,X}$, est la conjonction d'une formule du langage $(S, \text{Pred}, \perp)$ et des $t_u \neq t_v$ (où ne figure pas $x_{p+1}$).

On voit donc que $\exists x_{p+1}(F_\alpha \wedge \psi_{u,X})$ équivaut à $M_\alpha(x_1, ..., x_p)$, laquelle peut donc être prise pour $[\exists x_{p+1}(F_\alpha \wedge \psi_{u,X})]'$.

*Fin de la preuve du Théorème 6.5.*

6.6. Une application du Théorème 6.5 permet d'obtenir l'implication i) ⇒ iii)ter du Théorème 4.8 (et ce, de façon tout à fait constructive).

COROLLAIRE. *Si* $+$ *et* $\times$ *sont définissables dans la structure* $\langle \mathbf{N}; S, \text{Pred}; =, \perp \rangle$ *alors l'égalité l'est dans* $\langle \mathbf{N}; S, \text{Pred}; \perp \rangle$.

*Preuve.* Le Théorème 6.5 montre que si la relation d'ordre $x < y$ est définissable avec $S$, Pred, $=$ et $\perp$, elle l'est par une formule qui, mise sous forme de disjonction de conjonctions, a la forme suivante

$$\bigvee_{\alpha\in A}[F_\alpha(x,y)\wedge[\bigwedge_{i\in I_\alpha}(y\neq x+i)]\wedge[\bigwedge_{j\in J_\alpha}(x\neq y+j)]\wedge[\bigwedge_{k\in K_\alpha}(y=x+k)]\wedge[\bigwedge_{I\in L_\alpha}(x=y+1)]]$$

où $F_\alpha$ est une formule ne faisant pas intervenir l'égalité.

Si $K_\alpha$ ou $L_\alpha$ contient plus d'un élément alors la clause associée à $\alpha$ est impossible et peut donc être supprimée. Si $L_\alpha$ n'est pas vide ou si $K_\alpha$ contient 0 alors la clause associée à $\alpha$ contredit la condition $x < y$ et peut donc être supprimée. Si $K_\alpha = \{k\}, k \geqslant 1$, alors la sous-formule $y = x + k$ implique $x < y$; ainsi, la clause associée à $\alpha$ peut, toute entière, être remplacée par $y = x + k$.

Ceci permet de définir $x < y$ sous la forme suivante:

$$[\bigvee_{k\in K}y=x+k]\vee\bigvee_{\alpha\in A}[F_\alpha(x,y)\wedge[\bigwedge_{i\in I_\alpha}(y\neq x+i)]\wedge[\bigwedge_{j\in J_\alpha}(x\neq y+j)]].$$

Soit $M$ le supremum des éléments des $J_\alpha$.
Puisque la clause associée à $\alpha$ implique $x < y$, on voit que $F_\alpha(x, y)$ implique $(x<y)\vee[\bigvee_{i\in I_\alpha}(y=x+i)]\vee[\bigvee_{j\in J_\alpha}(x=y+j)]]$, qui implique aussi $x \leqslant y + M$.
Si $F(x, y)$ est la disjonction des $F_\alpha(x, y)$, on voit donc que

$$x < y \Rightarrow F(x,y) \Rightarrow x \leqslant y + M,$$

d'où $x = y \Rightarrow F(x, y+1) \wedge F(y, x+1) \Rightarrow |x - y| \leqslant M + 1$.

Le point iii) du Théorème 2.11 permet alors de conclure que l'égalité $x = y$ est définie par la formule $F(x, y+1) \wedge F(y, x+1) \wedge E(x, y)$ où $E(x, y)$ est la formule, écrite avec $S$ et $\perp$ qui définit la relation $x \cong_{\{0,\ldots,k\}} y$, où $k$ est un premier supérieur à $M$.

## § 7. Définissabilité par successeur, coprimarité et résiduation quadratique

7.1. Désignons par RES et $T$ les relations binaires

RES $= \{(x, p) \in \mathbf{N} \times P$: $x$ est résidu quadratique modulo le premier $p\}$,

$T = \{(x, p) \in \mathbf{N} \times P$: $x$ est impair et l'exposant (peut-être nul) du premier $p$ dans la décomposition primaire de $x$ est pair$\}$.

Le Théorème de Størmer (cf. Corollaire 2.5, point ii) se traduit par le lemme suivant:

LEMME. *L'égalité des entiers impairs* $x$ *et* $y$ *équivaut à la condition suivante (où* $\varepsilon$ *vaut, au choix,* $1$ *ou bien* $-1$*):*

$\mathrm{SUPP}(x) = \mathrm{SUPP}(y)$ *et* $\mathrm{SUPP}(x+2\varepsilon) = \mathrm{SUPP}(y+2\varepsilon)$ *et, pour tout* $p$ *premier et tout* $i \in \{0, 2\}$, *les couples* $(x+\varepsilon i, p)$ *et* $(y+\varepsilon i, p)$ *sont simultanément dans* $T$ *ou hors de* $T$.

7.2. THÉORÈME. *Les structures* $\langle \mathbf{N}; S; \perp, T\rangle$, $\langle \mathbf{N}; \mathrm{Pred}; \perp, T\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

*Preuve.* Le Lemme 7.1 fournit des définitions dans les langages $(\mathrm{Pred}; \perp, T\rangle$ et $(S; \perp, T)$ de la relation d'égalité restreinte aux entiers impairs. On en déduit simplement des définitions dans ces langages de la relation d'égalité tout entière. On conclut enfin en appliquant le Théorème 6.2 puisque, la seconde variable de $T$ variant dans $P$, la relation $T$ est quasi-saturé (cf. Exemple 6.1).

7.3. Nous allons maintenant définir la relation $T$ dans le langage $(S; \perp, \mathrm{RES})$.

PROPOSITION. *La relation* $T$ *est définissable dans les structures* $\langle \mathbf{N}; S; \perp, \mathrm{RES}\rangle$ *et* $\langle \mathbf{N}; \mathrm{Pred}; \perp, \mathrm{RES}\rangle$.

*Preuve.* Soient $x$ un entier impair différent de 1 et $p$ un diviseur premier de $x$. Le Lemme 2.13 montre que l'exposant de $p$ dans $x$ est pair si et seulement s'il existe un entier premier $q$ ne divisant pas $x$ et tel que les conditions suivantes soient simultanément satisfaites:

$$\left(\frac{x}{q}\right) = +1 \quad \text{et} \quad \left(\frac{p}{q}\right) = -1 \quad \text{et} \quad \left(\frac{p'}{q}\right) = +1$$

$$\text{pour tout} \quad p' \in \mathrm{SUPP}(x)\backslash\{p\}\,.$$

Comme l'égalité sur les premiers s'exprime dans les langages $(\mathrm{Pred}; \perp)$ et $(S; \perp)$ (cf. 5.5) cette caractérisation s'écrit dans $(\mathrm{Pred}; \perp, T, \mathrm{RES})$ et dans $(S; \perp, T, \mathrm{RES})$.

COROLLAIRE. *Les structures* $\langle \mathbf{N}; S; \perp, \mathrm{RES}\rangle$, $\langle \mathbf{N}; \mathrm{Pred}; \perp, \mathrm{RES}\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

7.4. L'analyse de la preuve précédente et de celle du Lemme 2.3 suggère qu'on peut remplacer RES par diverses restrictions. Nous utiliserons au § 8 la restriction suivante de la relation RES:

$$\mathrm{RRES} = \mathrm{RES} \cap \mathbf{N} \times [8\mathbf{N}+5]$$
$$= \{(x, p) \in \mathbf{N} \times P : p \equiv 5 \pmod 8 \text{ et } x \text{ est résidu quadratique modulo } p\}$$

L'intérêt de restreindre RES à $8\mathbf{N} + 5$ tient à ce que $q - 1$ est de la forme $4(2k+1)$ lorsque $q$ est lui-même de la forme $8k + 5$.

Le Corollaire 7.3 précédent s'adapte simplement :

THÉORÈME. *Les structures* $\langle \mathbf{N}; S; \perp, \mathrm{RRES}\rangle$, $\langle \mathbf{N}; \mathrm{Pred}; \perp, \mathrm{RRES}\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

*Preuve.* En changeant, dans la preuve du Lemme 2.13, l'équation $z \equiv 1 \pmod 4$ en $z \equiv 5 \pmod 8$, on peut supposer que l'entier premier $q$ obtenu dans ce lemme satisfait l'équation $q \equiv 5 \pmod 8$.

Ceci permet alors de remplacer RES par RRES dans la traduction utilisée dans la preuve de la Proposition 7.3.

## § 8. DÉFINISSABILITÉ PAR SUCCESSEUR, COPRIMARITÉ ET LA RELATION BINAIRE « $y$ EST UNE PUISSANCE DE $x$ »

8.1. Nous considérons maintenant la relation binaire

$$\mathrm{PUIS} = \{(x, y) : \text{il existe } n \geqslant 1 \text{ tel que } y = x^n\}.$$

Remarquons que la relation d'égalité se définit facilement dans le langage réduit au seul prédicat PUIS par la formule $\mathrm{PUIS}(x, y) \wedge \mathrm{PUIS}(y, x)$. Les fonctions $S$ et Pred sont donc définissables l'une à partir de l'autre avec PUIS.

THÉORÈME. *Les deux structures* $\langle \mathbf{N}; S; \perp, \mathrm{PUIS}\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

*Remarque.* Bien sûr, le Théorème 6.2 n'est pas directement applicable car PUIS n'est pas — a priori — quasi-saturé pour un $\cong_A$.

Ce Théorème est un corollaire immédiat du Théorème 7.4 et de la Proposition suivante, dont la preuve est l'objet des alinéas 8.2 à 8.5 ci-dessous.

PROPOSITION. *La relation* RRES *est définissable dans* $\langle \mathbf{N}; S; \perp, \text{PUIS}\rangle$.

8.2. Le Corollaire 2.4 (point ii) du Théorème ZBV montre que l'égalité $y = x^2$ équivaut à la condition

(*) $x = y = 0$ ou $x = y = 1$ ou bien $y$ est une puissance de $x$ et $y \neq x$ et $\text{SUPP}(y-1) = \text{SUPP}(x^2-1)$.

Comme $\text{SUPP}(x^2-1) = \text{SUPP}(x+1) \cup \text{SUPP}(x-1)$, on peut exprimer dans le langage $(S, \text{Pred}; \perp)$ la relation $\text{SUPP}(y-1) = \text{SUPP}(x^2-1)$.

Comme Pred est exprimable avec $S$ et PUIS, on voit que (*) donne une définition de la fonction $x \mapsto x^2$ dans le langage $(S; \perp, \text{PUIS})$.

8.3. Si $p$ est premier et ne divise pas $x$, nous notons $\text{ORD}(x, p)$ l'ordre de $x$ modulo $p$.

Rappelons que $x^\alpha = x^{\text{ORD}(x,p)}$ si et seulement si $p$ est diviseur primitif de $x^\alpha - 1$. La caractérisation donnée par le point iii) du Corollaire 2.4 de la notion de diviseur primitif donne alors une définition de la fonction $(x, p) \mapsto x^{\text{ORD}(x,p)}$ sur le domaine $\{(x, p): x \geqslant 2,\ p$ est premier et ne divise pas $x\}$ dans le langage $(\text{Pred}; =, \perp, \text{PUIS})$ et donc aussi dans $(S; \perp, \text{PUIS})$.

8.4. Soient $A$ et $B$ les relations suivantes:

$A = \{(x, p): p$ est premier et divise $x$, ou $x \leqslant 1\}$,

$B = \{(x, p): x \geqslant 2,\ p$ est premier et ne divise pas $x$, et $p \equiv 5 \pmod 8\}$.

On observe que l'on a l'égalité

$$\text{RRES} = [A \cap [\mathbf{N} \times (P \cap 8\mathbf{N}+5)]] \cup [B \cap \text{RES}].$$

La relation $A$ est évidemment $(S; \perp)$-définissable, l'ensemble $P \cap 8\mathbf{N} + 5$, inclus dans $P$, l'est aussi (Théorème 4.8 ou 4.9). Ainsi, le premier terme de cette union est $(S; \perp)$-définissable.

Le même argument montre que la relation $B$ est $(S; \perp)$-définissable.

8.5. Nous montrons que $B \cap \text{RES}$ est $(S; \perp, \text{PUIS})$-définissable.
Soit $(x, p)$ dans $B$, le critère d'Euler sur les résidus quadratiques montre que

(1) $(x, p) \in \text{RES}$ si et seulement si $x^{(p-1)/2} \equiv 1 \pmod p$
si et seulement si $\text{ORD}(x, p)$ divise $(p-1)/2$.

Puisque $p \equiv 5 \pmod 8$, l'entier $p-1$ est de la forme $p-1 = 4(2k+1)$. Puisque $\mathrm{ORD}(x, p)$ divise toujours $p-1$, l'équivalence (1) devient alors

(2) $(x, p) \in \mathrm{RES}$ si et seulement si 4 ne divise pas $\mathrm{ORD}(x, p)$.

Le point ii) du Corollaire 2.4 du Théorème ZBV montre que (2) peut aussi s'écrire

(3) $(x, p) \in \mathrm{RES}$ si et seulement si $\mathrm{SUPP}(x^4-1) \nsubseteq \mathrm{SUPP}[x^{\mathrm{ORD}(x, p)}-1]$.

Ceci prouve l'égalité

(4) $C \cap \mathrm{RES} = \{(x, p) \in C : \mathrm{SUPP}(x^4-1) \nsubseteq \mathrm{SUPP}[x^{\mathrm{ORD}(x, p)}-1]\}$.

Les résultats de 8.2 et 8.3 permettent alors de traduire cette égalité en une définition de la relation $C \cap \mathrm{RES}$ dans le langage $(S; \perp, \mathrm{PUIS})$.

Ceci achève la preuve de la Proposition 8.1 et donc du Théorème 8.1.

8.6. *Problème ouvert.* Peut-on remplacer dans le Théorème 8.1 le prédicat PUIS par la relation $y = x^2$ ?

## § 9. Définissabilité par successeur, coprimarité et restrictions de l'addition, de la multiplication ou de la division

9.1. Nous allons maintenant donner les prédicats les plus faibles que nous connaissions qui, joints au successeur et à la coprimarité, permettent de définir toute l'arithmétique.

Si $X \subseteq \mathbf{N}^2$, on note $X$-ADD et $X$-MULT les graphes des restrictions de l'addition et de la multiplication à $X$ :

$$X\text{-ADD} = \{(x, y, z) : (x, y) \in X \quad \text{et} \quad z = x + y\} .$$

$$X\text{-MULT} = \{(x, y, z) : (x, y) \in X \quad \text{et} \quad z = xy\} .$$

*Dans toute la suite, la première projection de $X$ sera toujours égale à $\mathbf{N}$ tout entier.* La relation d'égalité se définit alors facilement dans le langage réduit au seul prédicat $X$-ADD (resp. $X$-MULT) : $x = x'$ si et seulement si

$$\{(p, y) : (x, p, y) \in X\text{-ADD}\} = \{(p, y) : (x', p, y) \in X\text{-ADD}\} .$$

Les fonctions $S$ et Pred sont donc définissables l'une à partir de l'autre avec $X$-ADD ou $X$-MULT.

Théorème. *Soit $X \subseteq \mathbf{N}^2$ une relation définissable dans la structure $\langle \mathbf{N}; +, \times; = \rangle$ et vérifiant la condition :*

(*) pour tout $x$ il existe une infinité d'entiers primaires $v$ tels que $(x, v) \in X$.

*Les trois structures* $\langle \mathbf{N}; S; \perp, X\text{-ADD}\rangle$, $\langle \mathbf{N}; S; \perp, X\text{-MULT}\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent alors les mêmes relations et fonctions.*

*Preuve.* Soit $\sigma = \{(x, v, p): (x, v) \in X,\ v$ est primaire, $p$ premier, $p$ divise $x + v\}$. Le Corollaire 2.8 assure que l'égalité $x = y$ équivaut à la condition

$$\mathrm{SUPP}(x+t) = \mathrm{SUPP}(y+t) \text{ pour une infinité d'entiers } t\,.$$

L'hypothèse faite sur $X$ permet donc d'assurer que $x = y$ équivaut à

$$\{p: (x, v, p) \in \sigma\} = \{p: (y, v, p) \in \sigma\}\,.$$

Ceci donne une définition de la relation d'égalité dans la structure $\langle \mathbf{N}; \perp, \sigma\rangle$. Comme $\sigma$ est incluse dans $\mathbf{N} \times PP \times P$, le Théorème 6.2 montre alors que $+$ et $\times$ sont aussi définissables dans la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \sigma\rangle$.

Par ailleurs, l'égalité

$$\sigma = \{(x, v, p): \text{il existe } s \text{ tel que } (x, v, s) \in X\text{-ADD} \quad \text{et} \quad q \in \mathrm{SUPP}(s)\}$$

montre que la relation $\sigma$ est définissable dans $\langle \mathbf{N}; S; \perp, X\text{-ADD}\rangle$. Comme Pred est définissable à partir de $S$ et $X$-ADD, ceci prouve que $+$ et $\times$ sont aussi définissables dans $\langle \mathbf{N}; S; \perp, X\text{-ADD}\rangle$.

En ce qui concerne la structure $\langle \mathbf{N}; S; \perp, X\text{-MULT}\rangle$, on introduit la relation

$$\pi = \{(x, v, p): (x, v) \in X,\ v \text{ est primaire, } p \text{ premier, } p \text{ divise } xv + 1\}\,.$$

On raisonne alors de façon analogue en se servant du Corollaire 2 de 2.6 qui assure l'équivalence entre l'égalité $x = y$ et la condition

$$\mathrm{SUPP}(x) = \mathrm{SUPP}(y) \text{ et, pour une infinité d'entiers } t,$$
$$\mathrm{SUPP}(tx+1) = \mathrm{SUPP}(ty+1)\,.$$

*Remarque.* Considérons le cas où $X = \perp = \{(x, y): x$ et $y$ sont premiers entre eux$\}$. On observe que l'ensemble $\{1\}$ et la relation $\perp$ se définissent très simplement dans la structure $\langle \mathbf{N}; |\rangle$ (où $|$ est le prédicat de divisibilité) par les formules

$$\forall t\ (x|t) \text{ et } \forall z\ [[(z|x) \wedge (z|y)] \to (z=1)]\,.$$

Par ailleurs, la relation $\perp$-MULT se confond avec le graphe de la fonction ppcm restreinte à cet ensemble $\perp$ et se définit donc aussi dans la structure $\langle \mathbf{N}; |\rangle$. On voit ainsi que le Théorème précédent contient le résultat de J. Robinson (cf. 4.5) selon lequel addition et multiplication sont $(S; |)$-définissables.

9.2. On obtient ci-dessous un renforcement important du Théorème 9.1.

THÉORÈME. *Il existe une fonction $f$, définissable dans la structure $\langle \mathbf{N}; S; \perp \rangle$ (resp. $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$), de domaine $\mathbf{N}$ et à valeurs dans l'ensemble des entiers premiers, et pour laquelle la propriété suivante est vraie. Si $X \subseteq \mathbf{N}^2$ est définissable dans la structure $\langle \mathbf{N}; +, \times; = \rangle$ et telle que*

(**) pour tout $x$ il existe un entier primaire $v$ tel que $v \geqslant f(x)$ et $(x, v) \in X$

*alors les trois structures $\langle \mathbf{N}; S; \perp, X\text{-ADD} \rangle$, $\langle \mathbf{N}; S; \perp, X\text{-MULT} \rangle$ et $\langle \mathbf{N}; +, \times; = \rangle$ définissent les mêmes relations et fonctions.*

*Preuve.* 1°) L'argument développé ci-dessous reprend la preuve du Corollaire 1 du Théorème de Størmer (cf. 2.6) en montrant que les notions introduites sont définissables dans les langages $(S; \perp)$ et $(\mathrm{Pred}; \perp)$.

Notons $E$ et $E'$ les ensembles

$$E = \{(x, q) \in \mathbf{N} \times P : \text{il existe } u, v \text{ tels que } u \cong_{\{0,1\}} x \quad \text{et} \quad v \cong_{\{0,1\}} x \quad \text{et} \quad u \neq v \quad \text{et} \quad q \in \mathrm{SUPP}(|u-v|)\},$$

$$E' = \{(x, y) \in \mathbf{N}^2 : \mathrm{SUPP}[y(y+1)] \subseteq \{q : (x, q) \in E\}\}.$$

D'après le Théorème de Størmer (cf. 2.6), l'ensemble $\{y : (x, y) \in E'\}$ est fini pour tout entier $x$. Soit $N(x)$ le plus grand élément de $\{y : (x, y) \in E'\}$. On définit la fonction $f$ comme suit :

$$f(x) = \text{le plus petit entier premier supérieur à } N(x).$$

Les relations $E$, $E'$ sont clairement saturées pour l'équivalence $\cong_{\{0,1\}}$. La définition de la fonction $f$ à partir de $E'$, et le fait qu'elle soit à valeurs dans les premiers, montre que son graphe est aussi saturé pour $\cong_{\{0,1\}}$. Le Théorème 4.10 assure alors que $f$ est définissable dans $\langle \mathbf{N}; S; \perp \rangle$.

2°) La preuve du Corollaire 1 de 2.6 (appliquée avec l'ensemble fini $\{u : u \cong_{\{0,1\}} x\}$ comme ensemble $A$) montre que les trois conditions suivantes sont équivalentes :

i) $x = y$,

ii) $x \cong_{\{0,1\}} y$ et $\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m)$ et $\mathrm{SUPP}(x+m+1) = \mathrm{SUPP}(y+m+1)\}$ pour un $m \geqslant f(x)$,

iii) $x \cong_{\{0,1\}} y$ et $\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1)$ pour un $m \geqslant f(x)$.

Posons, de façon semblable à ce qui a été fait plus haut,

$$\sigma = \{(x, v, p) : (x, v) \in X, v \text{ est primaire, } p \text{ premier, } p \text{ divise } x + v\},$$

$$\sigma' = \{(x, v, p) : (x, v) \in X,\ v \text{ est primaire, } p \text{ premier, } p \text{ divise } x + v + 1\},$$

$$\pi = \{(x, v, p) : (x, v) \in X,\ v \text{ est primaire, } p \text{ premier, } p \text{ divise } xv + 1\}.$$

L'hypothèse faite sur $X$ permet de traduire les conditions ii) et iii) en des définitions de la relation d'égalité dans les structures $\langle \mathbf{N}; \perp, \sigma, \sigma' \rangle$ et $\langle \mathbf{N}; \perp, \pi \rangle$. Commme $\sigma$, $\sigma'$ et $\pi$ sont incluses dans $\mathbf{N} \times PP \times P$, le Théorème 6.2 montre que $+$ et $\times$ sont aussi définissables dans $\langle \mathbf{N}; S, \text{Pred}; \perp, \sigma, \sigma' \rangle$ et $\langle \mathbf{N}; S, \text{Pred}; \perp, \pi \rangle$. On achève la preuve, commme précédemment, en observant $\sigma$ et $\sigma'$ sont définissables à partir de $S$ et $X$-ADD, et que $\pi$ l'est à partir de $S$ et $X$-MULT.

3°) Pour obtenir une fonction $f$ ayant la même propriété et définissable avec Pred et $\perp$, on remplace $\cong_{\{0,1\}}$ par $\cong_{\{-1,0\}}$ dans la définition de $E$, et le produit $y(y+1)$ par $y(y-1)$ dans la définition de $E'$.

On raisonne enfin à l'aide de la condition iii)bis suivante du Corollaire 1 de 2.6:

iii)bis $x \cong_{\{-1,0\}} y$ et $\text{SUPP}(mx-1) = \text{SUPP}(my-1)$ pour un $m \geqslant f(x)$.

9.3. Nous considérons maintenant des prédicats qui sont des affaiblissements de la division euclidienne.

Avant de prouver le Théorème 9.4 ci-dessous, dont le Théorème de Woods cité en 4.6 est corollaire, nous mentionnons d'abord un fait simple.

PROPOSITION. *Pour tout entier premier* $\pi$, *la fonction* $z \mapsto \text{Reste}(z, \pi)$, *de domaine* $\mathbf{N}$ *est définissable dans les structures*

$$\langle \mathbf{N}; S; \perp \rangle \quad \textit{et} \quad \langle \mathbf{N}; \text{Pred}; \perp \rangle.$$

*Preuve.* La relation $y = \text{Reste}(x, \pi)$ est équivalente à chacune des conditions:

$$[y=0 \text{ et } \pi|x] \text{ ou } [y=1 \text{ et } \pi|S^{\pi-1}(x)] \text{ ou } \ldots \text{ ou } [y=\pi-1 \text{ et } \pi|S(x)],$$

et

$$[y=0 \text{ et } \pi|x] \text{ ou } [y=1 \text{ et } x \geqslant 1 \text{ et } \pi|\text{Pred}(x)] \text{ ou } \ldots$$
$$\text{ou } [y=\pi-1 \text{ et } x \geqslant \pi-1 \text{ et } \pi|\text{Pred}^{\pi-1}(x)].$$

Comme $\pi \mid z$ s'écrit $\neg(\pi \perp z)$ et que les singletons sont définissables dans les langages $(S, \perp)$ et $(\text{Pred}, \perp)$ (cf. 5.4 et 5.6), ces conditions se traduisent dans ces langages.

9.4. Rappelons que Quot et Reste désignent les fonnctions quotient et reste de la division euclidienne.

Soit $\alpha \geqslant 2$; on note $\text{Quot}_\alpha$ et $\text{Reste}_\alpha$ les graphes des fonctions partielles

$$(x, p) \mapsto \text{Reste}\big(\text{Quot}(x, p), \alpha\big) \quad \text{et} \quad (x, p) \mapsto \text{Reste}\big(\text{Reste}(x, p), \alpha\big)$$

de domaine $[\mathbf{N}\backslash\{0\}] \times [P\backslash\{\alpha\}]$.

*Remarque.* 1°) Ces fonctions sont une vue modulo un entier fixé de la restriction de la division au cas des diviseurs premiers; elles sont évidemment définissables à partir des fonctions Quot et Reste.

2°) En contraste avec le théorème ci-dessous, les graphes des fonctions $(x, y) \mapsto \text{Reste}(x+y, \alpha)$ et $(x, y) \mapsto \text{Reste}(xy, \alpha)$, de domaine $\mathbf{N}\backslash\{0\}] \times \mathbf{N}$, sont définissables dans les langages $(S, \perp)$ et $(\text{Pred}, \perp)$.

Ceci résulte de la Proposition 9.3, du calcul évident du reste de la somme et d'un produit, et de ce que les graphes de $+$ et $\times$ restreintes à $\{0, ..., \alpha - 1\}^2$ sont définissables dans $(S, \perp)$ et $(\text{Pred}, \perp)$.

THÉORÈME. *Soit* $\alpha \geqslant 3$. *Les structures*

$$\langle \mathbf{N}; S; \perp, \text{Quot}_\alpha\rangle, \quad \langle \mathbf{N}; \text{Pred}; \perp, \text{Quot}_\alpha\rangle, \quad \langle \mathbf{N}; \text{Pred}; \perp, \text{Reste}_\alpha\rangle$$
$$\textit{et} \quad \langle \mathbf{N}; +, \times; =\rangle$$

*définissent les mêmes relations et fonctions.*

*Preuve.* Les conditions $\text{ii})_\alpha$ et $\text{iii})_\alpha$ de la Proposition 2.14 montrent que l'égalité $x = y$ équivaut à chacune des conditions

(*) $x$ et $y$ ont même parité et $\text{Reste}_\alpha(x, p) = \text{Reste}_\alpha(y, p)$ pour tout premier $p \neq \alpha$;

(**) $x$ et $y$ ont même parité et $\text{Quot}_\alpha(x, p) = \text{Quot}_\alpha(y, p)$ pour tout premier $p \neq \alpha$.

Comme l'égalité restreinte à l'ensemble fini fixé $\{0, ... \alpha - 1\}$ (dans lequel les fonctions $\text{Quot}_\alpha$ et $\text{Reste}_\alpha$ prennent leurs valeurs) est définissable dans chacun des langages $(S, \perp)$ et $(\text{Pred}, \perp)$ (cf. Remarque 5.5), on voit que la condition (*) (resp. (**)) se traduit dans les langages $(S; \perp, \text{Quot}_\alpha)$ et $(S; \perp, \text{Reste}_\alpha)$ (resp. $(\text{Pred}; \perp, \text{Quot}_\alpha)$ et $(\text{Pred}; \perp, \text{Reste}_\alpha)$).

Comme $\text{Quot}_\alpha$ et $\text{Reste}_\alpha$ sont inclus dans $\mathbf{N} \times P \times \{0, ..., \alpha - 1\}$, on conclut grâce au Théorème 6.2.

COROLLAIRE (Woods). *Les structures* $\langle \mathbf{N}; <, \perp\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

*Preuve.* Si $p$ est premier et $x \neq 0$, le nombre $p\mathrm{Quot}(x, p)$ est le plus grand entier divisible par $p$ et inférieur ou égal à $x$. Ainsi, la fonction $(x, p) \mapsto p\mathrm{Quot}(x, p)$, de domaine $[\mathbf{N}\backslash\{0\}] \times P$ est définissable dans la structure $\langle \mathbf{N}; S, <, \perp \rangle$. Par ailleurs, pour $p \neq 3$, $\mathrm{Quot}_3(x, p)$ vaut

$$\mathrm{Reste}\,(p\mathrm{Quot}\,(x, p), 3) \quad \text{si} \quad 3 \text{ divise } p - 1\,,$$

$$\mathrm{Reste}\,[2 \times \mathrm{Reste}\,(p\mathrm{Quot}\,(x, p), 3), 3] \quad \text{si} \quad 3 \text{ divise } p - 2\,.$$

La Proposition 9.3 montre alors que la fonction $\mathrm{Quot}_3$ est définissable avec $<, S$ et $\perp$.

Comme $<$ définit trivialement $S$ et l'égalité, le langage $(S, \mathrm{Pred}, <, \perp)$ se ramène au langage $(<, \perp)$.

*Problèmes.* 1°) Le Théorème 9.4 est-il vrai pour $\alpha = 2$?

2°) La restriction de l'ordre $<$ à $\mathbf{N} \times P$ suffit-elle, avec $S$ et $\perp$, à définir $+$ et $\times$ ? Une réponse positive est conséquence (par réduction immédiate au Corollaire ci-dessus) de la conjecture suivante d'Erdös: si $x < y$ et $x \cong_{\{0,1\}} y$ alors il existe un premier entre $x$ et $y$.

## § 10. Conclusion

### 10.1. *Quelques perspectives*

Une stratégie possible pour résoudre la conjecture d'Erdös-Woods pourrait être de définir la fonction exponentielle dans le langage avec $S, \perp$ et la fonction carré, puis de définir la fonction carré avec $S$ et $\perp$.

Une autre voie pourrait consister à déterminer, pour chaque entier $x$ le support d'un entier $x + v$ éloigné de $x$.

On voit bien que la difficulté réside dans les liens cachés entre l'addition et le produit (ici la coprimarité). C'est ce qu'avaient remarqué certains théoriciens des modèles (par exemple, A. Ehrenfeucht et D. Jensen (cf. [EA & JD]) à propos de la reconstruction des modèles de l'arithmétique par amalgamation de structures additives et multiplicatives. Ce n'est d'ailleurs pas sans raison que ces derniers auteurs sont demandeurs de langages formés de deux ou trois prédicats (à l'exclusion de l'addition et la multiplication, bien évidemment) qui permettent de redéfinir l'arithmétique du premier ordre.

10.2. *Quelques remarques sur le caractère désespéré de certaines conjectures de théorie des nombres.*

On sait depuis les travaux de K. Gödel (1931) que la vérité arithmétique est au-delà du pouvoir démonstratif de toute théorie axiomatique:

*L'ensemble des théorèmes de toute théorie non contradictoire qui contient l'arithmétique — et dont les axiomes sont « effectivement donnés » — ne recouvre pas l'ensemble des énoncés vrais de la structure* $\langle \mathbf{N}; =, +, \times \rangle$.

A l'heure actuelle (plus précisément depuis les travaux de P. Cohen en 1963) ce résultat de Gödel n'a trouvé sa pleine concrétisation qu'en théorie des ensembles. Dans ce sujet, il y a maintenant pléthore de résultats logiques (aussi optimaux que déconcertants) des types (*) et (**) décrits ci-dessous:

Rappelons que si $T$ est une théorie logique dans laquelle on peut interpréter l'arithmétique (par exemple toutes les formalisations classiques de la théorie des ensembles: Zermelo, Zermelo et Fraenkel, Gödel et Bernays, ...), il est possible de trouver un énoncé, que nous désignons par $\mathrm{NC}(T)$, exprimant le caractère non contradictoire de la théorie $T$.

Certains des résultats d'indépendance trouvés en théorie des ensembles sont du type suivant:

(*) Si la théorie des ensembles $T$ n'est pas contradictoire, alors

— $T$ ne prouve ni l'énoncé $A$ ni l'énoncé $\neg A$ (négation de $A$);

— de plus, la théorie $T + \mathrm{NC}(T)$ prouve $\mathrm{NC}(T+A)$ et $\mathrm{NC}(T+\neg A)$.

Des exemples de tels énoncés $A$ sont

— l'hypothèse du continu,

— l'assertion de la mesurabilité Lebesgue de tout ensemble de réels qui est PCA, c'est-à-dire projection du complémentaire de la projection d'un borélien, etc.

D'autres résultats d'indépendance sont du type plus subtil suivant:

(**) — La théorie $T + \mathrm{NC}(T)$ prouve $\mathrm{NC}(T+\neg A)$,

— si la théorie $T + \mathrm{NC}(T)$ n'est pas contradictoire alors elle ne prouve pas $\mathrm{NC}(T+A)$,

— ou bien $T$ prouve $\neg A$, et, a fortiori, $T$ prouve alors $\neg \mathrm{NC}(T+A)$), ou bien $T$ ne prouve ni $A$ ni $\neg A$.

Des exemples de tels énoncés $A$ sont

— le problème d'Ulam sur l'existence d'un ensemble infini admettant un ultrafiltre non principal stable par intersections dénombrables,

— l'assertion de la mesurabilité Lebesgue de tout ensemble de réels qui est PCPCA, c'est-à-dire projection du complémentaire de la projection du complémentaire de la projection (sic) d'un borélien, etc.

10.3. Le pessimisme de spécialistes de théorie des nombres devant certaines conjectures qu'ils jugent désespérées (comme l'est la conjecture d'Erdös-Woods pour certains mathématiciens) pourrait être l'expression de leur intuition de résultats du type (*) ou (**).

Un argument logique montre que tout énoncé arithmétique de type universel, tel que le problème de Fermat $\forall n \forall x \forall y \forall z [n \leqslant 2 \vee x^n + y^n \neq z^n]$, qui n'est pas réfutable dans une théorie axiomatique $T$ comme l'arithmétique du premier ordre de Peano est, en fait, vrai dans la structure **N**. En effet, $A$ est alors vrai dans un modèle (standard ou non) de $T$ et, comme **N** est isomorphe à un segment initial de ce modèle, l'énoncé $A$ est également vrai dans **N**.

Il serait bien surprenant que la vérité d'un énoncé arithmétique soit établie par de telles méthodes, aussi est-ce plutôt à des résultats du type (**) (ou pire...) auxquels il faut s'attendre.

## RÉFÉRENCES BIBLIOGRAPHIQUES


[BE] BETH, E. W. On Padoa's method in the theory of definition. *Indag. Math. 15* (1953), 330-339.

[BG & VH] BIRKHOFF, G. D. and H. S. VANDIVER. On the integral divisors of $a^n - b^n$. *Ann. of Math. 5* (1904), 173-180.

[CP] CEGIELSKI, P. Axiomatisation de l'arithmétique avec l'ordre naturel et la divisibilité. *Communication personnelle.*

[CR] CARMICHAEL, R. C. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. 15 (2)* (1913-1914), 30-69.

[DM] DAVIS, M. Hilbert's tenth problem is unsolvable. *American Math. Monthly 80* (1973), 233-269.

[EA & JD] EHRENFEUCHT, A. and D. JENSEN. Some problems in elementary arithmetics. *Fundamenta Mathematicae XCII* (1976), 223-245.

[EP] ERDÖS, P. How many pairs of products of consecutive integers have the same prime factors? *American Math. Monthly 87* (1982), 392-393.

[GR] GUY, R. K. Unsolved problems in Number Theory. *Problem book in mathematics, vol. 1.* Springer-Verlag (1981), 25-28.

[LM1] LANGEVIN, M. Plus grand facteur premier d'entiers voisins. *Comptes Rendus Acad. Sc. Paris 280* (1975), 1567-1570.

[LM2] —— Autour d'un problème d'Erdös et Woods. *Preprint.*