Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 35 (1989)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: CONTRIBUTION À L'ÉTUDE D'UNE CONJECTURE DE THÉORIE DES NOMBRES PAR LE CODAGE ZBV
Autor: Grigorieff, Serge / Richard, Denis
Kapitel: §4. Autour du problème de J. Robinson
DOI: https://doi.org/10.5169/seals-57370

§ 4. Autour du problème de J. Robinson

4.1. Rappelons, avant d'en venir aux premiers résultats concernant le problème de JR, dans quelle problématique logique celui-ci s'est posé.

Ce problème relève de l'étude du pouvoir d'expression des langages faibles de l'arithmétique du premier ordre de **N** et de **Z**. Il s'agit de savoir ce qui peut s'exprimer dans les structures arithmétiques formées de prédicats et fonctions dont la portée est — a priori — réduite.

4.2. Le premier résultat spectaculaire dans ce domaine de la définissabilité remonte à la thèse du logicien K. Gödel:

Théorème (Gödel, 1931). *La classe des fonctions et relations qui sont définissables dans la structure* $\langle \mathbf{N}; +, \times; = \rangle$ *par des formules du premier ordre du langage associé* $(+, \times; =)$ *est stable par le procédé de construction par récurrence.*

Ce résultat permet de voir que toutes les fonctions et relations arithmétiques de la pratique mathématique sont définissables (au premier ordre) à partir de l'addition, la multiplication et l'égalité.

Ainsi,

La structure $\langle \mathbf{N}; +, \times; = \rangle$ *est la structure logique essentielle de l'arithmétique;* l'objet de l'étude des langages faibles est donc de déterminer la part de cette structure que l'on peut retrouver à partir d'eux.

Remarque. Pour saisir la portée du résultat de Gödel, il convient d'observer que le procédé de construction par récurrence

— n'est pas une définition explicite d'une fonction f à partir d'autres fonctions,

— mais une caractérisation d'une fonction f comme l'unique solution d'un système d'équations fonctionnelles.

Pour traduire une telle caractérisation en termes de formule logique il est nécessaire — a priori — d'utiliser des quantifications portant sur les fonctions et non sur les entiers seulement.

On pourra aussi se rendre compte de la force de ce résultat en essayant de définir directement l'exponentielle ou l'énumération des entiers premiers par des formules du premier ordre du langage $(+, \times; =)$.

4.3. Ce résultat de K. Gödel a reçu sa forme optimale dans la solution du 10-ième problème de Hilbert, achevée en 1972 (cf. [DM]) et due à

J. Robinson, M. Davis, H. Putnam et Y. Matijacevitch. Ils montrèrent que toute partie récursive (c'est-à-dire algorithmiquement reconnaissable) de $\mathbf{N}^k$ est diophantienne et peut donc être définie par une formule du type suivant:

$$\exists y_1 \ldots \exists y_n [P(y_1, \ldots, y_n, x_1, \ldots, x_k) = Q(y_1, \ldots, y_n, x_1, \ldots, x_k)]$$

où P et Q sont des polynômes à coefficients dans $\mathbf{N}$.

4.4. Bien entendu, des langages trop réduits ne permettent pas en général de retrouver toutes les relations et fonctions usuelles de l'arithmétique. Ainsi, comme il a été vu en 3.8,

— l'égalité et le successeur ne suffisent pas à définir l'ordre,

— l'égalité et l'ordre ne suffisent pas à définir l'addition,

— l'égalité et l'addition ne suffisent pas à définir la multiplication,

— l'égalité et la multiplication ne suffisent pas à définir l'addition (ni même l'ordre).

En revanche, l'équivalence:

$$(xz+1)(yz+1) = [z^2(xy+1)] + 1 \quad \text{si et seulement si} \quad z = 0 \text{ ou } x + y = z$$

montre que l'on peut définir l'addition avec le successeur en plus de l'égalité et de la multiplication, résultat observé par A. Tarski (cf. [TA]).

Une formule convenable du langage $(S, \times ; =)$ est

$$[\text{Zéro}(x) \cdot \text{Zéro}(y) \leftrightarrow \text{Zéro}(z)] \wedge [S(x \times z) \times S(y \times z) = S[(z \times z) \times S(x \times y)]]$$

où Zéro(x) est la formule $\forall u(x \times u = x)$.

4.5. Le premier résultat d'importance relatif aux langages plus réduits que le langage $(+, \times ; =)$ a été obtenu par J. Robinson dans sa thèse, publiée en 1949 (cf. [RJ]):

L'addition et la multiplication sont définissables dans la structure $\langle \mathbf{N}; S; | \rangle$.

Bien sûr, l'égalité est déjà définissable de façon triviale dans la structure $\langle \mathbf{N}; | \rangle$ par la formule $(x|y) \wedge (y|x)$. Ainsi,

THÉORÈME (J. Robinson, 1948). *Les structures* $\langle \mathbf{N}; S; | \rangle$ *et* $\langle \mathbf{N}; +, \times ; = \rangle$ *définissent les mêmes relations et fonctions.*

Preuve (esquissée). L'argument de J. Robinson est fondé sur l'équivalence suivante (elle-même conséquence simple du Théorème de Dirichlet, cf. 2.2): $z = xy$ si et seulement si pour tout premier p ne divisant ni x

ni y, il existe x' et y', premiers entre eux et premiers avec x et y et vérifiant les équations de congruence

$$xx' \equiv -1 \pmod{p}, \quad yy' \equiv -1 \pmod{p} \quad \text{et} \quad zx'y' \equiv 1 \pmod{p}.$$

Comme la fonction ppcm est définissable dans la structure $\langle \mathbf{N}; | \rangle$ et donne le produit de deux entiers premiers entre eux, on voit simplement que cette condition permet de définir la multiplication avec S et $|$. On conclut à l'aide de 4.4.

J. Robinson montre aussi que l'ensemble $\mathbf{N}$ est définissable en termes d'addition et de multiplication dans le corps $\mathbf{Q}$ des rationnels (c'est-à-dire que le fait, *pour un rationnel, d'être un entier naturel* est définissable au premier ordre dans le langage de l'arithmétique sur $\mathbf{Q}$). Ce dernier résultat est central dans l'étude des théories indécidables.

Dans ce même travail, et dans le but de trouver d'autres axiomatiques naturelles de l'arithmétique, J. Robinson pose la question qui nous intéresse ici :

PROBLÈME (J. Robinson). *Peut-on définir l'addition et la multiplication en termes d'égalité, successeur et coprimarité ?*

4.6. Les premiers résultats sur le problème de J. Robinson figurent dans la thèse d'A. Woods (cf. [WA]) soutenue en 1981. Celui-ci montre que

THÉORÈME (A. Woods, 1981). *Les structures* $\langle \mathbf{N}; <, \perp \rangle$ *et* $\langle \mathbf{N}; +, \times; = \rangle$ *définissent les mêmes relations et fonctions.*

On a vu (cf. 3.10) que l'égalité est définissable dans les structures $\langle \mathbf{N}; +; \perp \rangle$ et $\langle \mathbf{N}; S, \times; \perp \rangle$. Comme l'addition est définissable dans la structure $\langle \mathbf{N}; S, \times; = \rangle$ (cf. 4.4) et que la relation d'ordre $x < y$ est définissable dans la structure $\langle \mathbf{N}; +; = \rangle$ (par la formule $\exists i[(x+i)=y \wedge \neg(i+i=i)]$), on déduit le résultat suivant :

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

Remarque. 1°) En revanche, la structure $\langle \mathbf{N}; \times; =, \perp \rangle$ ne permet pas de définir l'addition. Ceci résulte de l'exemple 1 de 3.8 puisque la relation $\perp$ est déjà définissable dans la structure $\langle \mathbf{N}; \times; = \rangle$ et n'apporte donc rien de plus.

2°) Comme l'égalité est aussi définissable dans la structure $\langle \mathbf{N}; \text{Pred}, \times ; \perp \rangle$ — où Pred est la fonction prédécesseur, qui vaut 0 en 0 — (cf. 3.9), cette structure permet de définir S et est donc passible du même Corollaire ci-dessus.

4.7. Dans le même travail, A. Woods relie ces problèmes de définissabilité logique à des problèmes ouverts d'arithmétique.

Il prouve aussi que, dans le problème de J. Robinson, l'égalité est superfétatoire (cf. 4.12 pour une preuve de ces résultats).

THÉORÈME (A. Woods). *Les assertions suivantes sont équivalentes:*

i) *Le problème de J. Robinson admet une réponse positive: on peut définir l'addition et la multiplication en termes d'égalité, coprimarité et fonction successeur.*

i)′ *On peut définir l'ordre* ou *l'addition* ou *la multiplication en termes d'égalité, coprimarité et fonction successeur.*

ii) *On peut définir l'égalité, l'addition et la multiplication en termes de coprimarité et fonction successeur.*

ii)′ *On peut définir l'ordre* ou *l'addition* ou *la multiplication en termes de coprimarité et fonction successeur.*

iii) *On peut définir l'égalité en termes de coprimarité et fonction successeur.*

iv) *La conjecture d'Erdös-Woods.*

Remarque. Comme S est une injection, il est équivalent de dire que S et $\perp$ définissent l'égalité ou de dire qu'ils définissent le graphe de S: en effet, $x = y$ si et seulement s'il existe z tel que (x, z) et (y, z) soient tous deux dans $Gr(S)$.

4.8. Rappelons la différence — quant au pouvoir de définissabilité — entre une fonction et la relation constituée par son graphe. Ainsi,

— La relation d'égalité est trivialement définissable à partir de chacun des *graphes* $Gr(S)$ et $Gr(\text{Pred})$ des fonctions S et Pred par les formules suivantes:

$$\exists z[Gr(S)(x, z) \wedge Gr(S)(y, z)] \quad \text{et} \quad \exists z[Gr(\text{Pred})(z, x) \wedge Gr(\text{Pred})(z, y)] .$$

— La relation d'égalité n'est pas — a priori — définissable à partir de la relation $\perp$ et des *fonctions* S et Pred (cf. le Théorème ci-dessous).

— En présence de la relation d'égalité chacune des deux fonctions S et Pred permet de définir les deux graphes de S et de Pred.

Sans égalité il n'en est plus — a priori — de même.

Cependant, le Théorème de Woods reste valable en remplaçant la fonction S par Pred ou bien par S et Pred (cf. 4.12 pour une preuve).

THÉORÈME. *Les assertions du* Théorème 4.7 *sont également équivalentes aux suivantes :*

ii)bis *On peut définir l'égalité, l'addition et la multiplication en termes de coprimarité et fonction prédécesseur.*

ii)ter *On peut définir l'égalité, l'addition et la multiplication en termes de coprimarité et fonctions successeur et prédécesseur.*

Les versions ii)'bis, ii)'ter de ii)'.

iii)bis *On peut définir l'égalité en termes de coprimarité et fonction prédécesseur.*

iii)ter *On peut définir l'égalité en termes de coprimarité et fonctions successeur et prédécesseur.*

4.9. D'autres travaux récents sur le problème de J. Robinson figurent dans [RD1] :

THÉORÈME (D. Richard, 1985). *Toute relation définissable dans la structure* $\langle \mathbf{N}; +, \times, = \rangle$ et qui ne porte que sur les seuls entiers primaires *est également définissable dans la structure* $\langle \mathbf{N}; S; \perp \rangle$.

4.10. Le résultat suivant (dont la preuve est l'objet de 4.11 et du § 5 ci-dessous) est une version plus forte du Théorème 4.9, s'exprimant en termes des équivalences $\cong_A$ introduites en 2.10.

THÉORÈME. *Soit* ρ *une relation définissable dans la structure* $\langle \mathbf{N}; +, \times, = \rangle$.

1°) ρ *est définissable dans la structure* $\langle \mathbf{N}; S; \perp \rangle$ *si et seulement si elle est saturée par une relation* $\cong_A$, *où* A *est un ensemble* fini *d'entiers positifs ou nuls.*

2°) ρ *est définissable dans la structure* $\langle \mathbf{N}; \text{Pred}; \perp \rangle$ *si et seulement si elle est saturée par une relation* $\cong_A$, *où* A *est un ensemble* fini *d'entiers négatifs ou nuls.*

3°) ρ *est définissable dans la structure* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$ *si et seulement si elle est saturée par une relation* $\cong_A$, *où* A *est un ensemble* fini *d'entiers de* $\mathbf{Z}$.

N.B. Comme toute relation sur les primaires est saturée pour $\cong_{\{0,1,2\}}$ et $\cong_{\{-2,-1,0\}}$ (cf. le Théorème 2.12), le Théorème 4.9, et son analogue relatif au langage $(S, \mathrm{Pred}; \perp)$, apparaît comme un corollaire de celui-ci.

4.11. La Proposition suivante donne le sens le plus facile à établir des équivalences du Théorème 4.10.

PROPOSITION. *Soit* ρ *une relation définissable dans* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$ *(resp.* $\langle \mathbf{N}; S; \perp \rangle$, *resp.* $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$*); il existe une partie finie* A *de* $\mathbf{Z}$ *(resp. de* $\mathbf{N}$, *resp. de* $-\mathbf{N}$*) telle que* ρ *soit* $(\cong_A)$*-saturée.*

Preuve. Nous prouvons le cas de la définissabilité dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$, les deux autres sont analogues (en fait, plus simples).

Soit $\mathfrak{R}$ la famille des relations ρ pour lesquelles il existe une partie finie A de $\mathbf{Z}$ telle que ρ soit $(\cong_A)$-saturée. Il est clair que $\mathfrak{R}$ est stable par opérations booléennes et par projections (opérations qui correspondent aux connecteurs logiques et aux quantifications). Tout revient donc à montrer que $\mathfrak{R}$ contient les images réciproques de la relation $\perp$ par les fonctions composées des fonctions S et Pred avec les fonctions de brassage (cf. 3.6). (En termes logiques, ceci revient à montrer que $\mathfrak{R}$ contient les relations définies par les formules atomiques.) Comme $\mathrm{Pred} \circ S$ est l'identité, toute composée des fonctions S et Pred est de la forme $S^i \circ \mathrm{Pred}^j$. Il est à noter que $[S^i \circ \mathrm{Pred}^j](n) = i$ si $n \leqslant j$ et $[S^i \circ \mathrm{Pred}^j](n) = n + (i-j)$ si $n > j$; on ne peut donc pas simplifier cette fonction.

On voit facilement que, posant $A_{i,j} = \{-j, ..., 0\} \cup \{i-j\}$, si $x \cong_{A_{i,j}} y$ alors

— si $x \leqslant j$ ou $y \leqslant j$ alors $A_{i,j}$ contient $-x$ ou $-y$ et donc $x = y$ (cf. Fait 2.10, 3°)),

— $x + (i-j) \cong_{\{0\}} y + (i-j)$.

Il en résulte que $\mathrm{SUPP}[[S^i \circ \mathrm{Pred}^j](x)] = \mathrm{SUPP}[[S^i \circ \mathrm{Pred}^j](y)]$. Toute composée des fonctions S et Pred avec les fonctions de brassage (cf. 3.6) est de la forme $(x_1, ..., x_p) \mapsto (S^{i_1}[\mathrm{Pred}^{j_1}(x_{\sigma(1)})], ..., S^{i_q}[\mathrm{Pred}^{j_q}(x_{\sigma(q)})])$, où $\sigma : \{1, ..., q\} \mapsto \{1, ..., p\}$.

Il est clair que l'image réciproque de la relation $\perp$ par une telle fonction (nécessairement à valeurs dans $\mathbf{N}^2$, i.e. $q = 2$) est une relation $\cong_A$ saturée, où $A = A_{i_1, j_1} \cup A_{i_2, j_2}$.

Remarque. La preuve précédente montre, en fait, que si $p \geqslant 0$, $q \geqslant 0$ et si les termes figurant dans une formule $F(x, x_1, ..., x_k)$ et dans lesquels intervient effectivement la variable x sont tous de la forme $S^i[\mathrm{Pred}^j(x)]$ avec $j \leqslant p$ et $i - j \leqslant q$, alors la relation définie dans la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$ par la formule $F(x, x_1, ..., x_k)$ est saturée en sa première variable pour la relation $\cong_{\{-p, ..., 0, ..., q\}}$ (i.e. si $\mathrm{SUPP}(a+i) = \mathrm{SUPP}(b+i)$ pour tout i dans $\{-p, ..., 0, ..., q\}$, alors, pour tout p-uplet $(c_1, ..., c_k)$, la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$ satisfait la formule F au point $(a, c_1, ..., c_k)$ si et seulement si elle la satisfait au point $(b, c_1, ..., c_k)$).

4.12. *Preuve des Théorèmes 4.7 et 4.8*

Les résultats de Woods mentionnés en 4.6 (qui, ici, sont obtenus au § 9) montrent l'équivalence de i), ii), ii)bis, ii)ter) avec leurs versions primées.

On montre les implications

$$\begin{array}{ccccccc} & & & & \text{iii)} & \leftarrow & \text{ii)} \quad \rightarrow \text{ii)ter} \\ & & & & \downarrow & & \Uparrow \\ \text{ii)ter} & \rightarrow & \text{i)} & \Rightarrow & \text{iii)ter} & \Rightarrow & \text{iv)} \\ & & & & \uparrow & & \Downarrow \\ & & & & \text{iii)bis} & \leftarrow & \text{ii)bis} \quad \rightarrow \text{ii)ter} \end{array}$$

1°) Les implications notées par des flèches simples sont triviales.

2°) i) $\Rightarrow$ iii)ter est prouvée plus loin, c'est le Corollaire 6.6.

3°) iv) $\Rightarrow$ ii) et iv) $\Rightarrow$ ii)bis se prouve à l'aide du Théorème 4.10 (dont la preuve est donnée au § 5).

Appliquant la Remarque 2.10, la conjecture d'Erdös-Woods montre l'existence de k tel que les restrictions à $\mathbf{N}$ de $\cong_{\{0, ..., k\}}$ et $\cong_{\{-k, ..., 0\}}$ coïncident avec l'égalité. Toute relation sur $\mathbf{N}$ est alors — trivialement — saturée à la fois pour $\cong_{\{0, ..., k\}}$ et $\cong_{\{-k, ..., 0\}}$. Le Théorème 4.10 montre donc que toute relation est définissable avec S et $\perp$ ou bien Pred et $\perp$; c'est en particulier le cas de $=$, $+$ et $\times$.

4°) iii)ter $\Rightarrow$ iv) est une autre application du Théorème 4.10 (en fait, de sa partie facile qu'est la Propriété 4.11): si l'égalité est $(S, \mathrm{Pred}; \perp)$-définissable alors elle est saturée pour un certain $\cong_{\{-k, ..., k\}}$, ce qui implique (cf. Remarque 2.10) la conjecture d'Erdös-Woods.

Remarque. L'implication iv) ⇒ iii) peut se voir directement (sans passer par le Théorème 4.10). La conjecture d'Erdös-Woods, si elle est vraie, fournit la définition simple suivante de l'égalité dans le langage $(S; \perp)$:

$$\forall z[[z \perp x \leftrightarrow z \perp y] \wedge [z \perp S(x) \leftrightarrow z \perp S(y)] \wedge \ldots \wedge [z \perp S^k(x) \leftrightarrow z \perp S^k(y)]] .$$

Cette conjecture d'Erdös-Woods montre l'équivalence de l'égalité $x = y$ avec la condition suivante:

$x \geqslant k$ et $y \geqslant k$ et $\mathrm{SUPP}(x-i) = \mathrm{SUPP}(y-i)$ pour tout $i \in \{0, 1, \ldots, k\}$, ou bien x et y sont tous deux inférieurs à k et égaux.

Désignant par $\mathrm{Egal}_n(x)$ une formule qui définit $\{n\}$ dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$, on déduit alors de la condition précédente une définition simple de l'égalité dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$:

$$[\mathrm{Egal}_1(x) \leftrightarrow \mathrm{Egal}_1(y)] \wedge \ldots \wedge [\mathrm{Egal}_k(x) \leftrightarrow \mathrm{Egal}_k(y)]$$
$$\wedge \forall z[[z \perp x \leftrightarrow z \perp y] \wedge \ldots \wedge [z \perp \mathrm{Pred}^k(x) \leftrightarrow z \perp \mathrm{Pred}^k(y)]] .$$

4.13. Mentionnons enfin le résultat suivant qui étend à **Z** le Théorème 4.9 ci-dessus:

THÉORÈME. *Toute relation ou fonction arithmétique définie sur l'ensemble* ZPP *des primaires de* **Z** *et de leurs opposés est* $(S; \perp)$*-définissable.*

Remarquons que contrairement à ce qui peut sembler à première vue, le passage de **N** à **Z** n'a rien d'automatique. La preuve de ce résultat constitue d'ailleurs l'objet principal de l'article [RD2].

La difficulté principale est ici de reconnaître le signe d'un élément de ZPP. En particulier, on ne sait pas distinguer avec le langage $(S; \perp)$ si un diviseur premier de $x - 1$ divise $|x| - 1$ ou $|x| + 1$.

On peut voir (cf. [RD2]) que le Théorème précédent implique le Théorème 4.9. Il a aussi les Corollaires suivants.

1°) Une généralisation du Théorème de Woods:

L'arithmétique de **Z** (i.e. l'addition et la multiplication) est $(S; \perp)$-définissable sur **Z** si et seulement s'il existe un entier k (nécessairement $\geqslant 2$) tel que tout entier x de **Z** soit uniquement déterminé par les supports des entiers $x + 1, x + 2, \ldots, x + k$.

2°) La définissabilité de l'arithmétique de **Z** par successeur et divisibilité (question posée par J. Robinson dans l'article où elle prouve le résultat analogue sur **N**). Une preuve directe du même résultat se trouve aussi en [RD3].

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