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

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

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 $(x, v) \in X$.