

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

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **35 (1989)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.09.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

$$\begin{aligned} \text{RRES} &= \text{RES} \cap \mathbf{N} \times [8\mathbf{N} + 5] \\ &= \{(x, p) \in \mathbf{N} \times P : p \equiv 5 \pmod{8} \text{ et } x \text{ est r\u00e9sidu quadratique modulo } p\} \end{aligned}$$

L'int\u00e9r\u00eat de restreindre RES \u00e0  $8\mathbf{N} + 5$  tient \u00e0 ce que  $q - 1$  est de la forme  $4(2k + 1)$  lorsque  $q$  est lui-m\u00eame de la forme  $8k + 5$ .

Le Corollaire 7.3 pr\u00e9c\u00e9dent s'adapte simplement :

**TH\u00c9OR\u00c8ME.** *Les structures  $\langle \mathbf{N}; S; \perp, \text{RRES} \rangle$ ,  $\langle \mathbf{N}; \text{Pred}; \perp, \text{RRES} \rangle$  et  $\langle \mathbf{N}; +, \times; = \rangle$  d\u00e9finissent les m\u00eames relations et fonctions.*

*Preuve.* En changeant, dans la preuve du Lemme 2.13, l'\u00e9quation  $z \equiv 1 \pmod{4}$  en  $z \equiv 5 \pmod{8}$ , on peut supposer que l'entier premier  $q$  obtenu dans ce lemme satisfait l'\u00e9quation  $q \equiv 5 \pmod{8}$ .

Ceci permet alors de remplacer RES par RRES dans la traduction utilis\u00e9e dans la preuve de la Proposition 7.3.

## § 8. D\u00c9FINISSABILIT\u00c9 PAR SUCCESSEUR, COPRIMARIT\u00c9 ET LA RELATION BINAIRE « y EST UNE PUISSANCE DE x »

8.1. Nous consid\u00e9rons maintenant la relation binaire

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

Remarquons que la relation d'\u00e9galit\u00e9 se d\u00e9finit facilement dans le langage r\u00e9duit au seul pr\u00e9dicat PUIS par la formule  $\text{PUIS}(x, y) \wedge \text{PUIS}(y, x)$ . Les fonctions  $S$  et  $\text{Pred}$  sont donc d\u00e9finissables l'une \u00e0 partir de l'autre avec PUIS.

**TH\u00c9OR\u00c8ME.** *Les deux structures  $\langle \mathbf{N}; S; \perp, \text{PUIS} \rangle$  et  $\langle \mathbf{N}; +, \times; = \rangle$  d\u00e9finissent les m\u00eames relations et fonctions.*

*Remarque.* Bien s\u00fbr, le Th\u00e9or\u00e8me 6.2 n'est pas directement applicable car PUIS n'est pas — a priori — quasi-satur\u00e9 pour un  $\cong_A$ .

Ce Th\u00e9or\u00e8me est un corollaire imm\u00e9diat du Th\u00e9or\u00e8me 7.4 et de la Proposition suivante, dont la preuve est l'objet des alin\u00e9as 8.2 \u00e0 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  $\text{Pred}$  est exprimable avec  $S$  et  $\text{PUIS}$ , 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  $x^a = x^{\text{ORD}(x, p)}$  si et seulement si  $p$  est diviseur primitif de  $x^a - 1$ . 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  $\{(x, p): x \geq 2, p \text{ est premier et ne divise pas } x\}$  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:

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

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

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

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

$$\quad \quad \quad \text{si et seulement si} \quad \text{ORD}(x, p) \text{ divise } (p-1)/2.$$

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

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

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

(3)  $(x, p) \in \text{RES}$  si et seulement si  $\text{SUPP}(x^4 - 1) \not\subseteq \text{SUPP}[x^{\text{ORD}(x, p)} - 1]$ .

Ceci prouve l'égalité

(4)  $C \cap \text{RES} = \{(x, p) \in C : \text{SUPP}(x^4 - 1) \not\subseteq \text{SUPP}[x^{\text{ORD}(x, p)} - 1]\}$ .

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

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

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

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

Dans toute la suite, la première projection de  $X$  sera toujours égale à  $\mathbb{N}$  tout entier. La relation d'égalité se définit alors facilement dans le langage réduit au seul prédicat  $X\text{-ADD}$  (resp.  $X\text{-MULT}$ ):  $x = x'$  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  $\text{Pred}$  sont donc définissables l'une à partir de l'autre avec  $X\text{-ADD}$  ou  $X\text{-MULT}$ .

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

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