§7. DÉFINISSABILITÉ PAR SUCCESSEUR, COPRIMARITÉ ET RÉSIDUATION QUADRATIQUE

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **27.04.2024**

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

où F_α est une formule ne faisant pas intervenir l'égalité.

Si K_α ou L_α contient plus d'un élément alors la clause associée à α est impossible et peut donc être supprimée. Si L_α n'est pas vide ou si K_α contient 0 alors la clause associée à α 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 α 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_α.
Puisque la clause associée à α 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 $x \cong_{\{0,\dots,k\}} y$, 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* ε *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:

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

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* $\langle \mathbf{N}; S; \perp, \text{RRES}\rangle$, $\langle \mathbf{N}; \text{Pred}; \perp, \text{RRES}\rangle$ *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

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

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

THÉORÈME. *Les deux structures* $\langle \mathbf{N}; S; \perp, \text{PUIS}\rangle$ *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.