§6. L'ÉGALITÉ ET LE PROBLEME DE J. ROBINSON

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **23.09.2024**

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

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 $M = [M \cap \{0, 1, \ldots, m\}] \cup [\bigcup_{1 \leqslant i \leqslant m} \bigcap_{a \in A} K_{i,a}]$, 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 ρ 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 ρ.

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 $x \mapsto (x, \ldots, x)$ de $\mathbf{N}$ dans $\mathbf{N}^n$. C'est donc alors la famille des relations définissables dans $\langle \mathbf{N}; S, \mathrm{Pred}; \ldots \rangle$ 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 ρ, 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 $(z, x_1, \ldots, x_k)$ et $(z, y_1, \ldots, y_k)$ sont simultanément dans ρ ou hors de ρ.

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 $\rho_1, \ldots, \rho_p, \theta$ des relations définissables dans la structure $\langle \mathbf{N}; +, \times; = \rangle$ et chacune quasi-*

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

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

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

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

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

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

2°) Si X est une partie de $\mathbf{Z}$, posons $T_{i,j}(X) = \{-j, \ldots, 0\} \cup [X + \{i-j\}]$. 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 $F(x_0, x_1, \ldots, x_{n-1})$ qui définit τ dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \rho_1, \ldots, \rho_p \rangle$, on construit des formules F' et F'' qui définissent τ' et τ'' 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 Δ avec S, Pred et $\perp$, 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 τ qui sont images réciproques des relations $\perp, R_1, \ldots, R_p$ par les composées des fonctions S et Pred avec les fonctions de brassage. Les termes du langage $(S, \mathrm{Pred}; \perp, R_1, \ldots, R_p)$ 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 τ' et τ'' 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 τ et donc aussi de τ' et τ''. Compte tenu de 1°), les relations τ' et τ'' 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 ρ_α de R_α, on déduit la $(\cong_B)$-saturation de τ par rapport aux variables x_i telles que $i \neq \sigma(1) = 0$, et donc aussi le même résultat relatif à τ' et τ''. Le point 1°) assure alors que τ' et τ'' 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 θ est $(\cong_A)$-quasi-saturée, λ 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 ρ_α montre la $(\cong_B)$-saturation de τ 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 τ' et τ'' à partir de Δ, λ et ρ_α, et donc (puisque Δ et λ sont définissables avec S, Pred et $\perp$) des définitions de τ' et τ'' dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \rho_\alpha \rangle$.

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* $\rho_1, \ldots, \rho_p, \varphi_1, \ldots, \varphi_q$ *des relations et fonctions définissables dans* $\langle \mathbf{N}; +, \times; = \rangle$. *On suppose que* $\rho_1, \ldots, \rho_p$ *et les graphes de* $\varphi_1, \ldots, \varphi_q$ *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 $\langle \mathbf{N}; S, \mathrm{Pred}, \varphi_1, \ldots, \varphi_q; \perp, \rho_1, \ldots, \rho_p \rangle$ *(resp.* $\langle \mathbf{N}; S, \varphi_1, \ldots, \varphi_q; \perp, \rho_1, \ldots, \rho_p \rangle$, *resp.* $\langle \mathbf{N}; \mathrm{Pred}, \varphi_1, \ldots, \varphi_q; \perp, \rho_1, \ldots, \rho_p \rangle$*) alors cette structure définit les mêmes relations et fonctions que* $\langle \mathbf{N}; +, \times; = \rangle$.

Preuve. Appliquons le Lemme 6.1 avec les relations ρ_i et les graphes des φ_j, et, pour τ la relation d'égalité, pour θ 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 τ' est l'image de θ par la fonction de brassage $(x, y) \mapsto (y, x)$. La $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \rho_1, \ldots, \rho_p, Gr(\varphi_1), \ldots Gr(\varphi_q) \rangle$-définissabilité de τ', et donc de θ, 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 $\langle \mathbf{N}; S, \mathrm{Pred}, \varphi_1, \ldots, \varphi_q; \perp, \rho_1, \ldots, \rho_p \rangle$ montre l'équivalence de cette structure et de $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \rho_1, \ldots, \rho_p, Gr(\varphi_1), \ldots Gr(\varphi_q) \rangle$.

On remarque enfin que si l'égalité est définissable avec les ρ_i, φ_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 ρ la relation d'égalité, on voit que la condition de quasi-saturation des ρ_α 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 ρ 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 $\mathrm{EXP} = \{(x, y)\colon$ 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 $A = \mathrm{EXP} \cap [\mathbf{N} \times PP] = \{(x, p^x)\colon x \in \mathbf{N}$ 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* $f_{p,\alpha,\beta}: (x_1, \dots, x_p) \mapsto (x_\alpha, x_\beta)$ *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 :

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

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 $(\mathrm{Pred}, \perp)$ 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 $(S, \mathrm{Pred}; =, \perp)$ une formule *équivalente* $F'(x_1, ..., x_p)$ qui est combinaison booléenne de formules du langage $(S, \mathrm{Pred}, \perp)$ 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 $(S, \mathrm{Pred}; =, \perp)$ 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 $(S, \mathrm{Pred}, =, \perp)$ 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 $(S, \mathrm{Pred}, \perp)$ 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_α *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_α *est de l'une des deux formes suivantes:*

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

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

où G_α *est une formule du langage* $(S, \text{Pred}, \perp)$, s_α *et* t_u *sont des termes de la forme* $S^k(x_i)$ *ou* $\text{Pred}^k(x_i)$, *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 $H_\alpha(x_1, \ldots, x_p)$ ne dépend pas de x_{p+1}, la formule $\exists x_{p+1}(H_\alpha \wedge F_\alpha)$ équivaut à $H_\alpha(x_1, \ldots, x_p) \wedge \exists x_{p+1} F_\alpha$. 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_α).

11°) Le cas où F_α est de la forme $G_\alpha(x_1, \ldots, x_p, x_{p+1}) \wedge [(s_\alpha = x_{p+1})]$ est trivial: la formule $\exists x_{p+1} F_\alpha$ équivaut alors à $G_\alpha(x_1, \ldots, x_p, s_\alpha)$, 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_α est de la forme

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

D'après la Proposition 4.11 il existe une partie finie A de $\mathbf{Z}$ telle que la relation définie par la formule G_α soit $(\cong_A)$-saturée. La relation $\cong_A$ est évidemment définissable dans le langage $(S, \text{Pred}, \perp)$. 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 $(S, \text{Pred}, \perp)$. Si X est un ensemble fini nous notons $|X|$ le nombre de ses éléments. On considère les formules θ, $\varphi_{u,X}$ et $\psi_{u,X}$ suivantes, où $u \in U_\alpha$ et $X \subseteq U_\alpha$:

$$\bigwedge_{v \in U_\alpha} (x_{p+1} \not\cong_A t_v),\ (x_{p+1} \cong_A t_u)] \wedge [\bigwedge_{v \in X} (t_v \cong_A t_u)] \wedge [\bigwedge_{w \notin X} (t_w \not\cong_A t_u)] \wedge EQ_{|X|}(t_u)$$

et

$$(x_{p+1} \cong_A t_u)] \wedge [\bigwedge_{v \in X} (t_v \cong_A t_u)] \wedge [\bigwedge_{w \notin X} (t_w \not\cong_A t_u)] \wedge \neg EQ_{|X|}(t_u).$$

La disjonction de ces formules, quand u varie dans U_α et X dans les parties de U_α, 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_α sont trivialement impliquées par θ 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_α 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_α. 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_α 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_α, qui contient $\rho_{u,X}$, est la conjonction d'une formule du langage $(S, \mathrm{Pred}, \perp)$ 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) $\Rightarrow$ iii)ter du Théorème 4.8 (et ce, de façon tout à fait constructive).

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

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

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

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: