Zeitschrift: 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
Kapitel: §3. Préliminaires de logique
Autor: Grigorieff, Serge / Richard, Denis
DOI: https://doi.org/10.5169/seals-57370

Remarques. 1°) La restriction $|y - x| \neq 1$, triviale dans ii)$_\alpha$, ne peut être omise dans iii)$_\alpha$. En fait, les conditions suivantes sont équivalentes:

A) $y = x + 1$ et $p\mathrm{Quot}(x, p) \equiv p\mathrm{Quot}(y, p) \pmod{\alpha}$ pour tout premier $p \neq \alpha$;

B) $(x, y) = (0, 1)$ ou bien α est premier et $(x, y) = (\alpha^k - 1, \alpha^k)$ pour un $k \geqslant 1$.

2°) Le statut des assertions ii)$_2$, iii)$_2$ et iv)$_2$ reste ouvert. On note cependant qu'elles ne sont équivalentes à i) puisque

$$\mathrm{Quot}(0, p) = \mathrm{Quot}(2, p) = 0 \text{ pour tout premier } p \neq 2 .$$

$$\mathrm{Reste}(0, p) \equiv \mathrm{Reste}(2, p) \pmod{2} \text{ pour tout premier } p .$$

§ 3. Préliminaires de logique

3.1. Les *langages formels logiques* que nous considérerons sont ceux, dits *du premier ordre*, qui ne comportent qu'un seul type de variables. Dans le cadre arithmétique auquel nous nous intéressons, ces variables sont alors destinées à varier sur l'ensemble **N** des seuls entiers naturels et non sur les ensembles, relations ou fonctions sur **N**.

Ainsi, les formules ne permettent de traduire que les seules quantifications sur les entiers et non sur les relations ou fonctions comme il est usuel et tacite de le faire en mathématiques (en particulier dans les définitions par induction).

Un langage logique du premier ordre L est caractérisé par une liste de symboles spécifiques à chacun desquels est attaché un caractère relationnel ou fonctionnel ainsi qu'une arité (i.e. le nombre des arguments). En pratique, on désignera un langage L par la simple liste de ses symboles spécifiques fonctionnels puis relationnels, omettant d'expliciter les arités (rendues évidentes par le contexte).

A partir des variables on construit les termes de L par « composition » des symboles fonctionnels. Par « application » des symboles relationnels aux termes, on obtient les formules atomiques. Les opérations de négation, conjonction, implication et quantifications appliquées aux formules atomiques donnent enfin les formules de L.

3.2. Soit $L = (f_1, ..., f_m; R_1, ..., R_n)$ un langage du premier ordre.

Une *structure* $\Omega = \langle X; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n \rangle$ du langage L est la donnée

— d'un ensemble de base X,

— de fonctions $\varphi_1, ..., \varphi_m$ sur X qui interprètent les symboles fonctionnels du langage L (en respectant le nombre d'arguments de ces symboles),

— de relations $\rho_1, ..., \rho_n$ sur X qui interprètent les symboles relationnels du langage L (en respectant le nombre d'arguments de ces symboles).

Une relation ρ à k arguments sur X est dite Ω-*définissable* lorsqu'il existe une formule $F(x_1, ..., x_k)$ du langage L pour laquelle on a l'équivalence suivante :

un k-uplet $(a_1, ..., a_k)$ *d'éléments de* X *est dans* ρ *si structure* Ω *satisfait la formule* F *au point* $(a_1, ..., a_k)$.

Une fonction est dite Ω-*définissable* lorsque son graphe est une relation Ω-*définissable*.

3.3. *Remarque.* Par un abus commode et usuel, on confond souvent une structure de base $\mathbf{N}$ avec le langage associé $L = (f_1, ..., f_m; R_1, ..., R_n)$.

En particulier, les symboles du langage logique pour les prédicats et fonctions *(syntaxe)* d'une telle structure sont alors confondus avec ceux désignant les relations et fonctions qui les interprètent dans $\mathbf{N}$ *(sémantique)*.

Ainsi, les lettres S, $+$, $\times$, $=$, $\perp$, $|$ désignent tant les fonctions successeur, addition et multiplication, les relations d'égalité, de coprimarité et de divisibilité que les symboles de fonctions et de relations associés dans un langage formel logique.

Les expressions « *le langage* $(\varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n)$ *définit...* » et « *la structure* $\langle \mathbf{N}; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n \rangle$ *définit...* » sont donc synonymes.

3.4. *Remarques.* 1°) Il est important d'observer que nous considérons aussi des structures qui peuvent ne pas contenir la relation d'égalité (et donc des langages sans symbole d'égalité). C'est le cas de la structure $\langle \mathbf{N}; S; \perp \rangle$, notée aussi $(S; \perp)$, qui est le sujet principal d'intérêt de ce travail.

2°) Toute structure doit cependant contenir au moins une relation afin qu'il y puisse être défini quelque chose. En termes de langage, on voit que, sans symbole relationnel, le discours logique ne permet pas d'exprimer des propriétés et de décrire des relations et fonctions sur une structure mais ne peut que se borner à nommer des objets de celle-ci. Autrement dit, sans symbole relationnel il n'y a que des termes et pas de formules.

3.5. Une fonction φ et la relation $Gr(\varphi)$ constituée par son graphe ne sont pas, en général, équivalentes quant au pouvoir de définissabilité. Tout ce qui

est définissable dans la structure $\langle X ; \varphi_1, ..., \varphi_m ; \rho_1, ..., \rho_n, Gr(\varphi)\rangle$ l'est aussi dans la structure $\langle X ; \varphi_1, ..., \varphi_m, \varphi ; \rho_1, ..., \rho_n\rangle$. Si cette dernière structure permet de définir la relation d'égalité alors la réciproque est vraie. Dans le cas général, elle est fausse. Par exemple, considérant le graphe de la multiplication, on voit que :

— l'égalité est définissable dans toute structure $\langle \mathbf{N} ; Gr(\times), ...\rangle$ par la formule

$$\forall u \forall v [Gr(\times)(x, u, v) \leftrightarrow Gr(\times)(y, u, v)] .$$

— mais elle ne l'est pas dans la structure $\langle \mathbf{N} ; \times ; \perp\rangle$ (cf. l'exemple 3.9 ci-dessous).

3.6. La classe des relations définissables dans une structure peut aussi se définir en termes ensemblistes à l'aide des notions introduites ci-dessous.

On note $\mathrm{Proj}_{p,\{i_1,...,i_q\}}$ la fonction projection $(x_1, ..., x_p) \mapsto (x_{i_1}, ..., x_{i_q})$ de X^p dans X^q, où $1 \leqslant i_1 < ... < i_q \leqslant p$.

Si σ est une fonction de $\{1, 2, ..., q\}$ dans $\{1, 2, ..., p\}$, on appelle fonction de brassage la fonction $f_\sigma : (x_1, ..., x_p) \mapsto (x_{\sigma(1)}, ..., x_{\sigma(q)})$ qui envoie X^p dans X^q. Ces fonctions de brassage permettent d'ajouter de nouvelles variables (cas où $q \leqslant p$ et σ est l'injection canonique de $\{1, 2, ..., q\}$ dans $\{1, 2, ..., p\}$), de démultiplier certaines variables (cas où $q > p$), de permuter les variables (cas où $p = q$ et σ est une permutation de $\{1, 2, ..., p\}$), ou encore d'identifier certaines variables (cas où σ n'est pas injective).

PROPOSITION. 1°) *La classe des relations définissables dans une structure* Ω *de base* X *est la plus petite classe* $\mathfrak{R}$ *de relations sur* X *telle que :*

i) *Les relations* $\rho_1, ..., \rho_n$ *sont dans* $\mathfrak{R}$, *ainsi que toutes leurs images réciproques par les fonctions qui sont des composées des fonctions* $\varphi_1, ..., \varphi_m$ *et des fonctions de brassage.*

ii) *La classe* $\mathfrak{R}$ *est stable par les opérations booléennes.*

iii) *La classe* $\mathfrak{R}$ *est stable par image directe des fonctions projections.*

2°) *Cette classe* $\mathfrak{R}$ *est stable par image réciproque des fonctions qui sont des composées des fonctions* $\varphi_1, ..., \varphi_m$ *et des fonctions de brassage.*

Les conditions i) à iii) traduisent la construction des formules du langage L :

— les formules atomiques correspondent à la condition i),

— les connecteurs des formules correspondent aux opérations booléennes,

— toute quantification existentielle correspond à une projection.

3.7. *Remarque.* Cette caractérisation ensembliste de la notion de définissabilité dans une structure Ω se simplifie dans le cas où la relation d'égalité sur X est Ω-définissable; on peut alors remplacer la condition i) par la condition plus simple suivante:

i*) *Les relations* $\rho_1, ..., \rho_n$ *et les graphes des fonctions* $\varphi_1, ..., \varphi_m$ *sont tous dans* $\mathfrak{R}$, *ainsi que leurs produits par des* X^k.

3.8. Une méthode commode, dite de Beth & Padoa (cf. [BE]), pour montrer des résultats de non-définissabilité est fondée sur le résultat suivant, dû à Svenonius (cf. [PB] p. 241).

PROPOSITION. *Soit* $\Omega = \langle \mathbf{N}; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n, \rho \rangle$ *une structure du langage* $L = (f_1, ..., f_m; R_1, ..., R_n, R)$.

1°) *Les trois conditions suivantes sont équivalentes:*

i) *La relation* ρ *n'est pas définissable (par une formule du langage réduit* $L\backslash\{R\}$*) dans la structure réduite* $\langle \mathbf{N}; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n \rangle$.

ii) *Il existe une structure* $\Theta = \langle X; \psi_1, ..., \psi_m; \tau_1, ..., \tau_n, \tau \rangle$ *et une fonction* ξ *de* X *dans* X *telles que*

— *les deux structures* Ω *et* Θ *vérifient exactement les mêmes énoncés du langage* L;

— *la fonction* ξ *ne respecte pas la relation* τ *mais respecte les relations* τ_i *et leurs images réciproques par les fonctions qui sont des composées des fonctions* ψ_j *et des fonctions de brassage (cf. 3.6) (c'est le cas, par exemple, si* ξ *respecte les relations* τ_i *et les fonctions* ψ_j*).*

iii) *Il existe une structure* $\Theta = \langle X; \psi_1, ..., \psi_m; \tau_1, ..., \tau_n, \tau \rangle$ *et une bijection* ξ *de* X *dans* X *telles que*

— *les deux structures* Ω *et* Θ *vérifient exactement les mêmes énoncés du langage* L;

— *la fonction* ξ *respecte les relations* τ_i *et les fonctions* ψ_i *mais pas la relation* τ.

(i.e. ξ *est un automorphisme de la structure réduite*

$$\Theta = \langle X; \psi_1, ..., \psi_m; \tau_1, ..., \tau_n \rangle$$

mais pas de la structure Θ*).*

2°) *Dans le cas où la relation* ρ_i *est la relation d'égalité sur* $\mathbf{N}$, *alors*

on peut aussi faire en sorte que la relation τ_i *précédente soit la relation d'égalité sur* X.

Remarque. Si ρ est l'égalité sur $\mathbf{N}$, alors ou bien ξ n'est pas injective, ou bien la relation τ de la condition iii) n'est pas l'égalité sur X.

Exemples. 1°) On voit que le langage réduit à l'égalité et à la multiplication ne définit pas l'ordre (ni — a fortiori — l'addition) sur $\mathbf{N}$ en considérant

— la structure $\Theta = \langle \mathbf{N}; \times; =, < \rangle$

— et la bijection ξ de $\mathbf{N}$ sur $\mathbf{N}$ définie comme suit: $\xi(x)$ s'obtient à partir de x en échangeant, dans la décomposition de Gauss, les exposants de 2 et 3 et en laissant inchangés les autres.

2°) On voit que le langage réduit à l'égalité et au successeur ne définit pas l'ordre en considérant

— la structure $\Theta = \langle X; f, =, < \rangle$ suivante du langage $(S; =, <)$ où

$$X = \{ \sum_{0 \leqslant i \leqslant n} 2^{-i} : n \in \mathbf{N} \} \cup \{ 2 + \sum_{-\infty < i \leqslant n} 2^{-|i|} : n \in \mathbf{Z} \} \cup \{ 5 + \sum_{-\infty < i \leqslant n} 2^{-|i|} : n \in \mathbf{Z} \},$$

$=$ et $<$ sont les relations d'égalité et d'ordre usuelles sur les réels,

$$f : X \mapsto X, \quad f(a + \sum_{i \leqslant n} 2^{-|i|}) = a + \sum_{-i \leqslant n+1} 2^{-|i|}$$

où $(a, n) \in [\{1\} \times \mathbf{N}] \cup [\{2\} \times \mathbf{Z}] \cup [\{5\} \times \mathbf{Z}]$

(cette structure Θ satisfait les mêmes énoncés que $\langle \mathbf{N}; S, =, < \rangle$);

— et l'involution σ qui échange $2 + \Sigma$ avec $5 + \Sigma$ et laisse invariants les autres points de X.

3°) On voit que le langage réduit à la multiplication et à la coprimarité ne définit pas l'égalité en considérant

— la structure $\Theta = \langle \mathbf{N}; \times; =, \perp \rangle$

— et la fonction ξ de $\mathbf{N}$ sur $\mathbf{N}$ définie comme suit: $\xi(x)$ est le produit des facteurs premiers de x, i.e. ξ réduit à 1 les exposants des primaires dans la décomposition de Gauss de x.

3.9. Contrairement à ce qu'on peut penser a priori, il n'est pas toujours trivial de montrer que la relation d'égalité est définissable dans une structure (cf. 4.8 et le § 5).

Par exemple, la définissabilité de l'égalité dans chacune des structures $\langle \mathbf{N}; +; \perp \rangle$, $\langle \mathbf{N}; S, \times; \perp \rangle$ et $\langle \mathbf{N}; \mathrm{Pred}, \times; \perp \rangle$ (où Pred est la fonction prédécesseur, qui vaut 0 en 0) nécessite les équivalences suivantes (conséquences non triviales des Corollaires de 2.8 et 2.6) entre les conditions:

i) x et y sont égaux;

ii) pour tout $m \geqslant 0$, on a $\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m)$;

iii) $\mathrm{SUPP}(x) = \mathrm{SUPP}(y)$ et, pour tout $m \geqslant 0$, on a $\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1)$;

iv) $\mathrm{SUPP}(x) = \mathrm{SUPP}(y)$, x et y sont simultanément nuls ou non nuls, et, pour tout $m \geqslant 0$, on a $\mathrm{SUPP}[\mathrm{Pred}(mx-1] = \mathrm{SUPP}[\mathrm{Pred}(my-1)]$;

Ces conditions se traduisent par des formules des langages $(+; \perp)$ et $(S, \times; \perp)$:

$$\forall i \forall p \{[p \perp (x+i)] \leftrightarrow [p \perp (y+i)]\},$$

$$\forall p [(p \perp x) \leftrightarrow (p \perp y)] \wedge \forall m \forall p \{[p \perp S(m \times x)] \leftrightarrow [p \perp S(m \times y)]\},$$

$$A(x, y) \wedge \forall p [(p \perp x) \leftrightarrow (p \perp y)] \wedge \forall m \forall p \{[p \perp \mathrm{Pred}(m \times x)] \leftrightarrow [p \perp \mathrm{Pred}(m \times y)]\}$$

où A est la formule [Zéro $(x) \leftrightarrow$ Zéro (x)], Zéro (x) étant la formule $\forall u(x \times u = x)$.

3.10. Pour conclure cette revue des notions de Logique utilisées dans cette étude, nous précisons la notion — usuelle mais implicite en général — d'*extension par définitions* d'une structure (ou d'un langage).

Soit Ω une structure de base $\mathbf{N}$ du langage L et soient $\psi_1, ..., \psi_p$ des relations sur $\mathbf{N}$ et $\tau_1, ..., \tau_q$ des fonctions sur $\mathbf{N}$ qui sont définissables dans la structure Ω (par des formules du langage L).

Il est commode de considérer

— la structure Ω' obtenue en rajoutant à Ω ces relations et fonctions ψ_i et τ_j;

— le langage L' associé à Ω', obtenu en rajoutant au langage L de nouveaux symboles de relation et fonction $R_1, ..., R_p$ et $f_1, ..., f_p$.

PROPOSITION. *A toute formule* $F(x_1, ..., x_k)$ *du langage* L' *on peut associer une formule du langage* L, *notée* $\mathrm{Trad}[F](x_1, ..., x_k)$, *de sorte que la relation sur* $\mathbf{N}$ *définie par* $F(x_1, ..., x_k)$ *dans la structure* Ω' *coïncide avec celle définie dans la structure* Ω *par* $\mathrm{Trad}[F](x_1, ..., x_k)$.

Remarque. Comme il a déjà été dit en 3.3, nous utiliserons — abusivement — souvent les notations ψ_i et τ_j au lieu de R_i et f_j.