LOGIQUE. — La théorie élémentaire de la divisibilité est finiment axiomatisable.

Note de **Patrick Cegielski,** présentée par Gustave Choquet.

Remise le 25 juin 1984.

Dans ce qui suit on donne une axiomatique finie explicite de la théorie du premier ordre de la divisibilité des entiers naturels non nuls, ainsi qu'une élimination des quantificateurs (ce qui redémontre qu'elle est décidable).

LOGIC. — The Elementary Theory of Divisibility of Natural Numbers is Finitely Axiomatisable.

We give an explicit finite axiomatisation of the first order theory of the divisibility of the natural numbers, and an elimination of quantifiers (this gives a new proof of its decidability).

Soit DIV la théorie du premier ordre de la divisibilité des entiers naturels non nuls, c'est-à-dire de la structure $(\mathbf{N}^*,/)$. Comme pour toute théorie d'une structure de cardinal infini, on sait que DIV est non-contradictoire (si ZF l'est), complète et non-catégorique (la structure ci-dessus, appelée *modèle standard* de la théorie étudiée, n'est pas le seul modèle, même à isomorphisme près). Cette théorie est décidable (énoncé par Skolem en 1930, mais démontré pour la première fois par Mostowski en 1952) et donc récursivement axiomatisable. Dans cette Note nous montrons que cette théorie est même finiment axiomatisable tout en donnant une axiomatique explicite assez naturelle.

1. AXIOMATIQUE DE LA THÉORIE DE LA DIVISIBILITÉ. — La structure $(\mathbf{N}^*, /)$ est la somme directe de ω copies de $(\mathbf{N}, \leqq)$ (ce qui se voit grâce à la décomposition des entiers en facteurs premiers). L'axiomatique exprime ceci dans le langage du premier ordre de la structure, soit $L=(/)$, où $/$ est un prédicat binaire. On peut bien entendu définir dans celui-ci l'ensemble des nombres premiers $\mathbf{P}$ et les nombres p-primaires $\mathrm{PR}(p, .)$ (c'est-à-dire tels que p soit le seul nombre premier les divisant). On peut aussi y définir la fonction $V(p, x)$ qui associe à x le plus grand nombre p-primaire divisant x; nous appelons $V(p, x)$ *valuation p-adique* de x, et non l'exposant de p de celui-ci, qu'il n'est pas possible de définir dans ce langage. On en arrive à l'axiomatique suivante :

*A*1. *Réflexivité* : $\forall x\,(x/x)$.

*A*2. *Antisymétrie* : $\forall x, \forall y\,((x/y \wedge y/x) \rightarrow x=y)$.

*A*3. *Transitivité* : $\forall x, \forall y, \forall z\,((x/y \wedge y/z) \rightarrow x/z)$.

*A*4. *Plus petit élément* : $\exists x, \forall y\,(x/y)$ (Cet élément, qui est unique d'après A2, est noté **1**).

*d*1. p est un *nombre premier*, et on note $\mathbf{P}(p)$, si et seulement si on a :

$$p \neq 1 \wedge \forall x\,(x/p \rightarrow (x=1 \vee x=p)).$$

*A*5. *Existence de nombres premiers* : $\forall x, \exists p\,(\mathbf{P}(p) \wedge p \nmid x)$.

*d*2. x est un *nombre p-primaire*, et on note $\mathrm{PR}(p, x)$, si et seulement si on a :

$$\mathbf{P}(p) \wedge \forall q\,((\mathbf{P}(q) \wedge q \neq p) \rightarrow q \nmid x).$$

*A*6. *$/$ total sur* $\mathrm{PR}(p, .)$:

$$\forall p, \quad \forall x, \quad \forall y \quad ((\mathrm{PR}(p, x) \wedge \mathrm{PR}(p, y)) \rightarrow (x/y \vee y/x)).$$

*A*7. *Successeur sur* $\mathrm{PR}(p, .)$:

$$\forall p, \quad \forall x\,(\mathrm{PR}(p, x) \rightarrow \exists y\,(\mathrm{PR}(p, y) \wedge x/y \wedge y \neq x \wedge \forall z\,((\mathrm{PR}(p, z) \wedge x/z \wedge z \neq x) \rightarrow y/z))).$$

0249-6321/84/02990367 $ 2.00

(Cet y, qui est unique d'après A2, est noté $S\,x$ et s'appelle le *successeur* de x.)

A8. Prédécesseur sur PR $(p, .)$:

$$\forall p,\quad \forall x\,((\mathrm{PR}\,(p, x) \wedge x \neq 1) \rightarrow \exists y\,(\mathrm{PR}\,(p, y) \wedge \mathrm{S}\,y = x)).$$

d3. On appelle *valuation p-adique* de x, et on note $\mathrm{V}(p, x)$, le plus grand nombre p-primaire qui divise x :

$$y = \mathrm{V}(p, x) \leftrightarrow (\mathrm{PR}\,(p, y) \wedge y/x \wedge \forall z\,((\mathrm{PR}\,(p, z) \wedge z/x) \rightarrow z/y)).$$

A9. Existence des valuations : $\forall x, \forall p\,(\mathbf{P}\,(p) \rightarrow \exists y\,(y = \mathrm{V}(p, x)))$.

A10. Valuation et division : $\forall x, \forall y\,(\forall p\,(\mathbf{P}\,(p) \rightarrow \mathrm{V}(p, x)/\mathrm{V}(p, y)) \rightarrow x/y)$.

LEMME 1. — (*Caractérisation par les valuations*) :

$$\forall x,\quad \forall y\,(\forall p\,(\mathbf{P}\,(p) \rightarrow \mathrm{V}(p, x) = \mathrm{V}(p, y)) \leftrightarrow x = y).$$

LEMME 2. — $\forall x\,(x \neq 1 \rightarrow \exists p\,(\mathbf{P}\,(p) \wedge p/x))$.

A11. P.G.C.D. :

$$\forall x,\quad \forall y,\quad \exists z,\quad \forall p\,(\mathbf{P}\,(p) \rightarrow ((\mathrm{V}\,(p, x)/\mathrm{V}\,(p, y) \rightarrow \mathrm{V}\,(p, z) = \mathrm{V}\,(p, x)) \wedge (\mathrm{V}\,(p, y)/\mathrm{V}\,(p, x) \rightarrow \mathrm{V}\,(p, z) = \mathrm{V}\,(p, y)))).$$

(Ce z, qui est unique d'après le lemme 1, est noté $x \wedge y$ et s'appelle le *p. g. c. d.* de x et de y.)

LEMME 3. — (*Une propriété du p. g. c. d.*) :

$$\forall x,\quad \forall y\,(x \wedge y/x \wedge x \wedge y/y \wedge \forall z\,((z/x \wedge z/y) \rightarrow z/x \wedge y)).$$

Attention! : Les axiomes A 1 à A 10 ne permettent pas de montrer l'équivalence de A 11 et du lemme 3.

A12. P.P.C.M. :

$$\forall x,\quad \forall y,\quad \exists z,\quad \forall p\,(\mathbf{P}\,(p) \rightarrow ((\mathrm{V}\,(p, x)/\mathrm{V}\,(p, y) \rightarrow \mathrm{V}\,(p, z) = \mathrm{V}\,(p, y)) \wedge (\mathrm{V}\,(p, y)/\mathrm{V}\,(p, x) \rightarrow \mathrm{V}\,(p, z) = \mathrm{V}\,(p, x)))).$$

(Ce z est noté $x \vee y$ et s'appelle le *p. p. c. m.* de x et de y; on a une propriété analogue au lemme 3.)

A13. Troncage inverse :

$$\forall x,\quad \forall y,\quad \exists z,\quad \forall p\,(\mathbf{P}\,(p) \rightarrow ((p \nmid x \rightarrow \mathrm{V}\,(p, z) = \mathrm{V}\,(p, y)) \wedge (p/x \rightarrow \mathrm{V}\,(p, z) = 1))).$$

(Ce z, qui est unique, est noté $\bar{\mathrm{T}}(x, y)$, et s'appelle le *tronqué inverse* de y par x : si $y = \prod p^{\alpha}$ alors $\bar{\mathrm{T}}(x, y) = \prod_{p \nmid x} p^{\alpha}$.)

LEMME 4. — *Troncage direct* :

$$\forall x,\quad \forall y,\quad \exists z,\quad \forall p\,(\mathbf{P}\,(p) \rightarrow ((p/x \rightarrow \mathrm{V}\,(p, z) = \mathrm{V}\,(p, y)) \wedge (p \nmid x \rightarrow \mathrm{V}\,(p, z) = 1))).$$

(Ce z est noté $\mathrm{T}(x, y)$ et s'appelle le *tronqué direct* de y par x.)

*A*14. *Incrémentation :*

$$\forall x, \quad \exists y, \quad \forall p\ (\mathbf{P}(p) \to ((p \mid x \to \mathrm{V}(p, y) = 1) \wedge (p/x \to \mathrm{V}(p, y) = \mathrm{SV}(p, x)))).$$

(Ce y est noté $\mathrm{I}x$ et s'appelle l'*incrémenté* de x : si $x = \prod p^{\alpha}$ alors $\mathrm{I}x = \prod p^{\alpha+1}$.)

*A*15. *Sélection :*

$$\forall x, \quad \forall y, \quad \exists z, \quad \forall p\ (\mathbf{P}(p) \to (\mathrm{V}(p, z) = 1 \quad \text{ou} \quad p \quad \text{et} :$$
$$\mathrm{V}(p, z) = p \leftrightarrow (p/x \wedge p/y \wedge \mathrm{V}(p, x)/\mathrm{V}(p, y))).$$

(Ce z, qui est unique, se note $\mathrm{supp}(x, y)$.)

2. Grandes lignes de la démonstration. — Soit $\mathscr{R}$ un modèle de DIV, la théorie de langage L ayant pour axiomes propres les quinze axiomes précédents, p un nombre premier de $\mathscr{R}$; on note A_p l'ensemble des nombres p-primaires de $\mathscr{R}$ et $\mathscr{R}_p$ la structure $(\mathrm{A}_p, /)$. On montre que $\mathscr{R}_p$ est un modèle de la théorie du successeur, c'est-à-dire de la théorie de $(\mathbf{N}, \leqq)$, grâce à une axiomatisation de cette dernière théorie (à savoir les axiomes A1, A2, A3, A6, A4, A7, A8 précédents dans le langage approprié). A toute formule φ de L on associe la formule φ^p de $\mathrm{L}' = (/, \mathrm{V})$ dont l'ensemble des variables libres est celui de φ plus la variable p, obtenue en remplaçant chaque variable libre x par $\mathrm{V}(p, x)$. Alors pour $\mathbf{a} \in \mathrm{A}^n$, on a :

$$\mathscr{R} \models \varphi^p(\mathbf{a}) \text{ si, et seulement si, } \mathscr{R}_p \models \varphi[\mathrm{V}(p, \mathbf{a})].$$

Pour θ formule de L et $k \in \mathbf{N}^*$, on note $\mathrm{A}_k(\theta)$ (il y a au moins k nombres premiers p tels que les valuations p-adiques vérifient θ) la formule :

$$\exists p_1, \ldots, \exists p_k \Big(\bigwedge_{1 \leqq i < j \leqq k} p_i \neq p_j \wedge \bigwedge_{1 \leqq i \leqq k} (\mathbf{P}(p_i) \wedge \theta^{p_i}) \Big).$$

Si DIV′ est l'extension par définition évidente au langage L′ alors :

Théorème. — *Toute formule* φ *de* L *est* DIV′*-équivalente à une combinaison booléenne, que l'on donne explicitement, de formules du type* $\mathrm{A}_k(\theta)$.

Ceci s'obtient en modélisant la méthode de Feferman-Vaught [1]. Il en résulte immédiatement que la théorie DIV est complète et décidable.

3. Elimination des quantificateurs. — Pour $n \in \mathbf{N}^*$, on note $\mathrm{E}_n(x)$ (a au moins n éléments) la relation :

$$\exists p_1, \ldots, \exists p_n \Big(\bigwedge_{1 \leqq i < j \leqq n} p_i \neq p_j \wedge \bigwedge_{1 \leqq i \leqq n} (\mathbf{P}(p_i) \wedge p_i/x) \Big).$$

Alors la théorie DIV^0 de langage $\mathrm{L}^0 = (1, \mathrm{Supp}(x, y), \mathrm{I}, \text{p. g. c. d.}, (\mathrm{E}_n)_{n \in \mathbf{N}^*})$, extension évidente de DIV, élimine les quantificateurs.

Références bibliographiques

[1] S. Feferman et R. L. Vaught, *Fundamenta Mathematicae*, 1959, p. 57-103.

27, *rue Dézobry*, 93200 *Saint-Denis*.