LOGIQUE. – *La théorie élémentaire de la multiplication est conséquence d'un nombre fini d'axiomes de* $I\Sigma_0$. Note (*) de **Patrick Cegielski,** présentée par Gustave Choquet.

Nous montrons ci-dessous que la théorie élémentaire de la multiplication des entiers naturels est conséquence d'un nombre fini d'axiomes de la sous-théorie de l'arithmétique de Peano dans laquelle le schéma d'axiomes de récurrence est restreint aux formules à quantifications bornées.

We show that the theory of the multiplication of the natural numbers is consequence of a finite number of axioms of the subtheory of first order Peano arithmetic obtained by restricting the induction schema to formulas with only bounded quantifiers.

INTRODUCTION. – L'auteur a donné une axiomatique explicite de la théorie élémentaire de la multiplication (*voir* [1] ou [2]). On en déduit alors facilement que la théorie de la multiplication est conséquence de $I\Sigma_0$, la sous-théorie de l'arithmétique de Peano dans laquelle le schéma d'axiomes de récurrence est restreint aux formules à quantifications bornées : il suffit de démontrer que les axiomes de cette théorie sont des théorèmes de $I\Sigma_0$. Cependant deux schémas d'axiomes (divisibilité et séparation) avaient alors seulement été montrés être des schémas de théorèmes de $I\Sigma_0$. Nous allons montrer ici qu'ils sont conséquences de deux théorèmes de $I\Sigma_0$, d'où le résultat annoncé, répondant ainsi à une question de Bruno Poizat.

L'exponentiation dans $I\Sigma_0$. – La formule classique de Gödel permettant de définir l'exponentiation dans l'arithmétique de Peano (grâce à la fonction béta) n'est pas Σ_0 (i. e. à quantifications bornées), mais Paris (*voir* [3], p. 7-10) a exhibé une Σ_0-formule $E(x, y, z)$ fonctionnelle en z telle que :

1° $I\Sigma_0 \vdash \forall x \forall y \forall z (E(x, y, z) \rightarrow E(x, y+1, z.x))$.

2° $I\Sigma_0 \vdash \forall x \forall y \forall z (E(x, y+1, z) \rightarrow \exists t \leqq z (E(x, y, t) \wedge z = t.x))$.

3° $I\Sigma_0 \vdash \forall x E(x, 0, 1) \wedge \forall y \neq 0 E(0, y, 0) \wedge \forall y E(1, y, 1)$, mais, bien sûr, on n'a pas :

$$I\Sigma_0 \vdash \forall x \forall y \exists z E(x, y, z).$$

E vérifie alors dans $I\Sigma_0$ les propriétés usuelles de l'exponentiation, ainsi que :

4° $\forall x \forall y \forall z \forall u \forall v ((E(x, y, z) \wedge u \leqq x \wedge v \leqq y) \rightarrow \exists w E(u, v, w))$.

5° Pour n entier naturel on a :

$$\forall x \forall z (E(x, n, z) \leftrightarrow z = x^n)$$

(en particulier pour m, n, p entiers naturels on a :

$$E(m, n, p) \leftrightarrow p = m^n),$$

6° $\forall x \forall y \forall z \forall p ((\mathbb{P}(p) \wedge E(x, y, z)) \rightarrow E(V(p, x), y, V(p, z))$ (i. e. la valuation p-adique $V(p, x)$ de x^y est égale à la valuation p-adique de x, $V(p, x)$, à la puissance y).

Démonstrations. – 5° Par récurrence « extérieure » sur n. 6° Par récurrence sur y. Pour $y=0$, on a $E(x, 0, z)$, d'où $z=1$ d'après 3°, d'où $V(p, z)=1$ et ainsi on a bien $E(V(p, x), 0, 1)$ d'après 3°. Si on a $E(x, y+1, z)$ alors on a $E(x, y, t)$ avec $z=t.x$ d'après 2° d'où, par hypothèse de récurrence, $E(V(p, x), y, V(p, t))$, d'où, d'après 1°, $E(V(p, x), y+1, V(p, t).V(p, x))$, or $V(p, z)=V(p, t).V(p, x)$, donc $E(V(p, x), y+1, V(p, z))$.

Démonstration du résultat annoncé. — Les schémas d'axiomes de divisibilité et de séparation sont les suivants : pour n entier naturel non nul :

$$\forall x(x\neq 0 \to \exists y \exists z(x=y^n.z \wedge \forall y' \forall z'(x=y'^n.z' \to z/z')));$$

$$\forall x \forall y(x.y\neq 0 \to \exists z \forall p(\mathbb{P}(p) \to ((\mathrm{V}(p,x) \equiv_n \mathrm{V}(p,y) \wedge p/x.y) \to \mathrm{V}(p,z)=p)$$
$$\wedge(\mathrm{V}(p,x) \not\equiv_n \mathrm{V}(p,y) \vee p \nmid x.y) \to \mathrm{V}(p,z)=1))),$$

où $x \equiv_n y$ est mis pour $\exists z(y=z^n.x)$.

Ces schémas d'axiomes se déduisent dans $\mathrm{I}\Sigma_0$, grâce à 5°, des deux énoncés suivants :

$$\forall t \forall x(x\neq 0 \to \exists y \exists z \exists u(x=u.z \wedge \mathrm{E}(y,t,u)$$
$$\wedge \forall y' \forall z' \forall u'((x=u'.z' \wedge \mathrm{E}(y',t,u')) \to z/z'))),$$

$$\forall t \forall x \forall y(x.y\neq 0 \to \exists z \forall p(\mathbb{P}(p) \to ((\mathrm{V}(p,x) \equiv_t \mathrm{V}(p,y) \wedge p/x.y) \to \mathrm{V}(p,z)=p)$$
$$\wedge(\mathrm{V}(p,x) \not\equiv_t \mathrm{V}(p,y) \vee p \nmid x.y) \to \mathrm{V}(p,z)=1))),$$

où $x \equiv_t y$ est mis pour $\exists z \exists u(y=u.x \wedge \mathrm{E}(z,t,u))$.

Or ces énoncés sont des théorèmes de $\mathrm{I}\Sigma_0$. Cela se montre facilement par récurrence sur y, en utilisant 6° (*voir* [1] pour les analogues en ce qui concernait alors les schémas de théorèmes).

(*) Remise le 21 septembre 1981.

[1] P. CEGIELSKI, *Théorie élémentaire de la multiplication* (*Thèse de* 3e *cycle*, Paris-VI, 25 mars 1980).

[2] P. CEGIELSKI, *Comptes rendus*, 290, série B, 1980, p. 935.

[3] C. DIMITRACOPOULOS, *Matijasevic's Theorem and Fragments of Arithmetic* (*Ph. D. Thesis*, Manchester University, avril 1980).

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