Logique/*Logic*

La théorie des corps réels-clos inductifs est une extension conservative de l'Arithmétique de Peano

Patrick CEGIELSKI

Résumé – Nous appelons *théorie des corps réels-clos inductifs* la théorie logique du premier ordre dont le langage est celui des anneaux ordonnés augmenté d'un prédicat unaire, distinguant un sous-ensemble de l'ensemble de base, et dont les axiomes sont ceux des corps totalement ordonnés, plus tout polynôme vérifie la propriété des valeurs intermédiaires, plus les axiomes élémentaires pour que le sous-ensemble distingué ressemble aux entiers, et enfin un schéma d'axiomes d'induction sur les formules du langage complet, et donc avec quantifications sur les éléments du corps.

Nous démontrons que cette théorie est une extension conservative de l'Arithmétique de Peano.

The theory of inductive real-closed fields is a conservative extension of Peano arithmetic

Abstract – *By* theory of inductive real-closed fields *we mean the theory of first order with language of ordered rings extended by an unary predicate, and with following axioms: axioms for a totally ordered field, every polynomial has the intermediate value property, the familiar ordered semiring axioms of natural integers for the subset determined by the unary predicate, the induction scheme for every formula (with quantifiers over elements of the field, and not only integers).*

We prove this theory is a conservative extension of Peano Arithmetic.

INTRODUCTION. – Le résultat dont la démonstration est résumée dans cette Note, est une contribution au domaine de la Logique Mathématique appelé *programme de Hilbert relativisé* (*cf.* Simpson [4] et [5]) dont un des buts est de savoir ce que l'on peut dire des Mathématiques classiques dans une théorie assez faible.

On appelle *Arithmétique de Peano* **PA** la théorie égalitaire du premier ordre de langage $L(\mathbf{PA}) = \{S, +, ., 0\}$, où S est une application, + et . des opérations binaires, 0 un élément distingué, et vérifiant les axiomes propres suivants :

- 1° $\forall x (Sx \neq 0)$;
- 2° $\forall x, y (Sx = Sy \Rightarrow x = y)$;
- 3° pour toute formule $\varphi(x, \mathbf{y})$ de $L(\mathbf{PA})$ on a :

$$\forall \mathbf{y} ((\varphi(0, \mathbf{y}) \wedge \forall x (\varphi(x, \mathbf{y}) \rightarrow \varphi(Sx, \mathbf{y}))) \rightarrow \forall x \varphi(x, \mathbf{y}));$$

- 4° $\forall x (x + 0 = x)$;
- 5° $\forall x, y (x + Sy = S(x + y))$;
- 6° $\forall x (x . 0 = x)$;
- 7° $\forall x, y (x . Sy = x . y + x)$.

Il est bien connu que cette théorie permet de retrouver les résultats de l'arithmétique élémentaire (*cf.* Mendelson [3]).

Soit T une théorie du premier ordre de langage L contenant (+, ., 0, 1, **N**) avec **N** prédicat unaire. A toute formule φ du langage $L(\mathbf{PA})$ de l'Arithmétique de Peano on peut associer une formule φ' de L en remplaçant Sx par $x + 1$, et les quantificateurs par des quantificateurs relativisés à **N**. T est une *extension conservative* de **PA** si, et seulement si, pour tout énoncé φ de $L(\mathbf{PA})$ on a $T \vdash \varphi'$ si, et seulement si, $\mathbf{PA} \vdash \varphi$.

Note présentée par Gustave CHOQUET.

0764-4442/90/03100239 $ 2.00

On appellera *corps inductif* toute structure $\mathscr{K} = (K, +, ., \leqq, \mathbf{N})$ telle que :

– 1° $(K, +, ., \leqq)$ est un corps commutatif totalement ordonné;

– 2° $\mathbf{N}$ est un prédicat unaire tel que l'on ait :

(*a*) $\mathbf{N}(0)$; (*b*) $\forall x(\mathbf{N}(x) \Rightarrow \mathbf{N}(x+1))$; (*c*) pour toute formule du langage L' :

$$\mathscr{K} \models \forall \mathbf{y}((\varphi(0, \mathbf{y}) \wedge \forall x((\mathbf{N}(x) \wedge \varphi(x, \mathbf{y})) \Rightarrow \varphi(x+1, \mathbf{y})) \Rightarrow \forall x(\mathbf{N}(x) \Rightarrow \varphi(x, \mathbf{y}))).$$

Un *corps inductif* est *archimédien* si, et seulement si : $\forall x, \exists n \in \mathbf{N} : x \leqq n$.

Un *corps réel-clos inductif* est un corps inductif archimédien dans lequel tout polynôme vérifie la propriété des valeurs intermédiaires, *i.e.* pour $P(x, \mathbf{y}) \in \mathbb{Q}[X, X_1, \ldots, X_m]$ on a :

$$\forall \mathbf{c}(\exists a, b(a < b \wedge P(a, \mathbf{c}) < 0 \wedge P(b, \mathbf{c}) > 0 \Rightarrow \exists d(a < d < b \wedge P(d, \mathbf{c}) = 0))).$$

THÉORÈME. – *La théorie des corps réels-clos inductifs est une extension conservative de* **PA**.

Démonstration. – Il suffit de plonger un modèle quelconque de **PA** dans un corps réel-clos inductif tel que la sous-structure distinguée par $\mathbf{N}$ soit isomorphe au modèle de départ.

Soit $(\mathbf{N}, S, +, ., 0)$ une structure de Peano. Alors, par l'analogue de la construction classique de $\mathbb{Q}$ à partir de $\mathbb{N}$, il existe un corps commutatif totalement ordonné muni d'un prédicat unaire $\mathbf{N}(x)$, $Q = (\mathbf{Q}, +, ., 0, \leqq, \mathbf{N})$, unique à isomorphisme près, tel que $(\mathbf{N}, +, ., \leqq)$ soit isomorphe à $(\mathbf{N}_Q, +, ., \leqq)$, avec $\mathbf{N}_Q$ l'ensemble $\{x \in \mathbf{Q} \mid \mathbf{N}(x)\}$, et tel que tout élément r de $\mathbf{Q}$ s'écrive, de façon unique : $r = -p/q$ ou 0 ou p/q, avec $p, q \in \mathbf{N}^*$, $p \wedge q = 1$ (en confondant $\mathbf{N}$ et $\mathbf{N}_Q$). De plus il est facile de montrer que ce corps est inductif en codant les rationnels par des entiers.

Nous *noterons* classiquement $\mathbb{N}[x_1, \ldots, x_n]$ l'ensemble des polynômes (standards) à coefficients dans le modèle standard $\mathbb{N}$ et à un nombre fini standard de variables.

Une *relation* n-aire R sur $\mathbf{N}$ est *diophantienne* si, et seulement si, il existe $P, Q \in \mathbb{N}[x_1, \ldots, x_{n+p}]$ tels que :

$$R(x_1, \ldots, x_n) \Leftrightarrow \exists x_{n+1}, \ldots, x_{n+p}(P(x_1, \ldots, x_{n+p}) = Q(x_1, \ldots, x_{n+p})).$$

Une *application* n-aire f de $\mathbf{N}^k$ dans $\mathbf{N}$ est *diophantienne* si, et seulement si, son graphe

$$\{(x_1, \ldots, x_n, y) \in \mathbf{N}^{k+1} / y = f(x_1, \ldots, x_n, y)\}$$

est diophantien.

L'ensemble des *applications récursives* (totales) sur $\mathbf{N}$ est le plus petit ensemble d'applications à plusieurs variables à arguments et à valeurs dans $\mathbf{N}$ qui contient les applications successeur S, constante à 0, projections $P_i^n (1 \leqq i \leqq n)$; stable par composition, récurrence primitive et par minimisation régulière.

Le théorème MDRP (dû à Matiyassévitch, Davis, Julia Robinson, Putnam, 1970) dit qu'une application est diophantienne si, et seulement si, elle est récursive.

Il est habituellement énoncé pour le seul modèle standard, mais il est en fait valable pour un modèle quelconque de Peano. Il suffit par exemple d'en voir la démonstration de Davis [2] pour s'en convaincre.

De plus il existe $m (\leqq 14)$ tel que pour toute relation diophantienne $R(x_1, \ldots, x_n)$ il existe $P \in \mathbb{Z}[x_1, \ldots, x_{n+m}]$ tel que

$$R(x_1, \ldots, x_n) \Leftrightarrow \exists x_{n+1}, \ldots, x_{n+m}(P(x_1, \ldots, x_{n+m}) = 0).$$

Toute formule ouverte de L(**PA**) est **PA**-équivalente à une formule diophantienne.

Une *formule* de L(**PA**) *est dite* Δ_1 si, et seulement si, elle est **PA**-équivalente à une formule diophantienne ainsi que sa négation.

L'ensemble des Δ_1-formules est stable par les opérations booléennes, les quantifications bornées et, plus généralement, les quantifications bornées par des applications récursives des variables libres.

Une formule de L(**PA**) est une Σ_n-*formule* (resp. Π_n-*formule*) pour $n \geqq 2$ si, et seulement si, elle est de la forme : $\exists x_1, \forall x_2, \exists x_3, \ldots, Q_n x_n \psi$ (resp. $\forall x_1, \exists x_2, \forall x_3, \ldots, Q_n x_n \psi$), avec $Q_n = \exists$ ou $\forall$ (resp. $\forall$ ou $\exists$) suivant que n est impair ou pair, et ψ une Δ_1-formule.

Toute formule de L(**PA**) est **PA**-équivalente à une Σ_n-formule ou à une Π_n-formule.

Une Δ_n-*formule* est une formule de L(**PA**) qui est **PA**-équivalente à une Σ_n-formule et une Π_n-formule.

Nous *noterons* $\langle a_1, \ldots, a_k \rangle$ le code du k-uplet $(a_1, \ldots, a_k)$ pour un codage choisi une fois pour toutes, et $\Pi(x, i) = a_i$ si $1 \leqq i \leqq k$, 0 sinon, si x est un code. Π est **PA**-définissable.

Nous utiliserons aussi le codage de la *concaténation* des séquences, défini par :

$$\langle a_1, \ldots, a_k \rangle \wedge \langle b_1, \ldots, b_h \rangle = \langle a_1, \ldots, a_k, b_1, \ldots, b_h \rangle.$$

Si $\mathbf{a} = (a_1, \ldots, a_k)$ nous noterons $\tilde{a} = \langle a_1, \ldots, a_k \rangle$.

Il existe une Δ_1-formule Evaterm(e, x, y) de L(**PA**) telle que :

1° **PA** $\vdash \forall e, x, \exists ! y$ Evaterm (e, x, y);

2° pour tout terme $t(x_1, \ldots, x_m)$ de L(**PA**), il existe $e \in \mathbb{N}$ tel que pour tout modèle $\mathcal{N}$ de **PA** et $\mathbf{a} \in \mathbf{N}^m$ on ait :

$$\mathcal{N} \models \text{Evaterm}[e, \tilde{a}, t(a_1, \ldots, a_m)].$$

Il existe une Δ_1-formule $\text{Verif}_0(e, x)$ de L(**PA**) telle que pour toute formule *ouverte* $\varphi(x_1, \ldots, x_m)$ de L(**PA**), il existe un entier naturel $e \in \mathbb{N}$ tel que pour tout modèle $\mathcal{N}$ de **PA** et $\mathbf{a} \in \mathbf{N}^m$ on ait :

$$\mathcal{N} \models \varphi[\mathbf{a}] \quad \text{si, et seulement si,} \quad \mathcal{N} \models \text{Verif}_0[e, \tilde{a}].$$

Pour tout entier naturel non nul $p \in \mathbb{N}^*$ il existe une Σ_p-formule (resp. une Π_p-formule) de L(**PA**), Σ_p-Verif(e, x) [resp. Π_p-Verif(e, x)], telle que pour toute Σ_p-formule (resp. Π_p-formule) $\varphi(\mathbf{x})$ de L(**PA**), il existe un entier naturel $e \in \mathbb{N}$ tel que pour tout modèle $\mathcal{N}$ de **PA** et $\mathbf{a} \in \mathbf{N}^m$, on ait :

$$\mathcal{N} \models \varphi[\mathbf{a}] \quad \text{si, et seulement si,} \quad \mathcal{N} \models \Sigma_p\text{-Verif}[e, \tilde{a}] \quad (\text{resp. } \mathcal{N} \models \Pi_p\text{-Verif}[e, \tilde{a}]).$$

A tout élément b de **Q**, ensemble de base de Q, on associe l'entier (non standard) : $\underline{\tilde{b}} = \langle b_1, b_2, b_3 \rangle$, avec $b_i \in \mathbf{N}$, $b_3 \neq 0$, $b = (-1)^{b_1} \cdot (b_2 / b_3)$. [On peut exiger de plus, si on veut, $b_1 \in \{0, 1\}$, $b_2 \wedge b_3 = 1$]. On notera $\underline{\tilde{\mathbf{Q}}}$ l'ensemble de ces entiers.

On appelle Σ_p-*formule* (resp. Π_p-*formule*) de L(Q) toute formule prénexe avec un nombre quelconque de quantificateurs, commençant par le quantificateur $\exists$ (resp. $\forall$) et avec p alternances de quantificateurs.

Pour toute Σ_p-formule (resp. Π_p-formule) $\varphi(x_1, \ldots, x_n)$ de L(Q), il existe une Σ_p-formule (resp. Π_p-formule) de L(**PA**), $\varphi'(x_1, \ldots, x_n)$, que l'on peut déterminer effectivement, telle que pour tout modèle $\mathcal{N}$ de **PA** et $a_1, \ldots, a_n \in \mathbf{Q}$, on ait :

$$\mathbf{Q} \models \varphi[a_1, \ldots, a_n] \quad \text{si, et seulement si,} \quad \mathcal{N} \models \varphi'[\tilde{a}_1, \ldots, \tilde{a}_n].$$

A tout m-uplet (m standard) $\mathbf{b} = (b_1, \ldots, b_m)$ de **Q** on associe l'entier (non standard) : $\underline{\tilde{\mathbf{b}}} = \langle \tilde{b}_1, \tilde{b}_2, \ldots, \tilde{b}_m \rangle$.

Pour tout entier naturel non nul $p \in \mathbb{N}^*$ il existe une Σ_p-formule (resp. une Π_p-formule) de L(**PA**), Σ_p-Verif(e, x) (resp. Π_p-Verif(e, x)), telle que pour toute Σ_p-formule (resp. Π_p-formule) $\varphi(\mathbf{x})$ de L(Q), il existe un entier naturel $e \in \mathbb{N}$ tel que pour tout modèle $\mathcal{N}$

de **PA** et $\mathbf{b} \in \mathbf{Q}^m$ on ait :

$$Q \models \varphi[\mathbf{b}] \quad \text{si, et seulement si, } \mathcal{A} \models \Sigma_p\text{-Verif}[e, \tilde{b}] \quad \text{resp. } \mathcal{A} \models \Pi_p\text{-Verif}[e, \tilde{b}]).$$

Pour tout $p \in \mathbb{N}^*$, une *suite rationnelle* $(u_n)_{n \in \mathbf{N}} \in \mathbf{Q}^{\mathbf{N}}$ (indexée par **N** et non $\mathbb{N}$) est dite Σ_p-(resp. Π_p-) *définissable* si, et seulement si, il existe $e \in \mathbf{N}$ (et non plus $e \in \mathbb{N}$) et $\tilde{b} \in \tilde{\mathbf{Q}}$ tels que :

$$\mathcal{A} \models (\forall n \in \mathbf{N},\ \exists ! x\, \Sigma_p\text{-Verif}(e, \langle n, x \rangle \wedge \tilde{b})) \wedge (\forall n \in \mathbf{N}\, \Sigma_p\text{-Verif}[e, \langle n, \tilde{u}_n \rangle \wedge \tilde{b}])$$

(respectivement avec Π_p).

On *notera* Σ_p-Déf$(\mathbf{Q}^{\mathbf{N}})$ l'ensemble des suites rationnelles Σ_p-définissables de Q (de même avec Π_p).

En fait : Σ_p-Déf$(\mathbf{Q}^{\mathbf{N}}) \subseteqq \Pi_p$-Déf$(\mathbf{Q}^{\mathbf{N}})$. Nous noterons donc Δ_p-Déf$(\mathbf{Q}^{\mathbf{N}}) = \Sigma_p$-Déf$(\mathbf{Q}^{\mathbf{N}})$ et nous parlerons des suites rationnelles Δ_p-*définissables*.

Toute suite rationnelle de Cauchy Δ_p-définissable est bornée. L'ensemble C-Δ_p-Déf$(\mathbf{Q}^{\mathbf{N}})$ des suites rationnelles Δ_p-définissables de Cauchy est une sous-algèbre unitaire de $(\mathbf{Q}^{\mathbf{N}}, +, .\,_{\mathbf{Q}}, \leqq)$.

Pour des suites rationnelles (a_n) et (b_n) on *notera* $(a_n) \equiv (b_n)$ si, et seulement si :

$$\forall \varepsilon \in \mathbf{Q}^+ *,\ \exists N \in \mathbf{N} : n > N \ \Rightarrow\ |a_n - b_n| < \varepsilon.$$

$\equiv$ est une relation d'équivalence sur Δ_p-déf$(\mathbf{Q}^{\mathbf{N}})$ et on *note* Δ_p-déf$(\mathbf{R}) = $C-$\Delta_p$-déf$(\mathbf{Q}^{\mathbf{N}})/\equiv$ l'ensemble des *réels* Δ_p-*définissables*. On définit les opérations et la relation d'ordre sur Δ_p-déf$(\mathbf{R})$ de façon habituelle. Alors $(\Delta_p\text{-déf}(\mathbf{R}), +, ., \leqq)$ est un corps commutatif totalement ordonné.

L'application de **Q** dans Δ_p-déf$(\mathbf{R})$, qui à q associe la classe de la suite rationnelle Δ_p-définissable de Cauchy constante à q, est un isomorphisme de corps ordonnés. Nous considérerons que **Q**, et donc **N**, est inclus dans Δ_p-déf$(\mathbf{R})$.

Toute suite rationnelle Δ_p-définissable de Cauchy converge dans le corps Δ_p-déf$(\mathbf{R})$, vers le réel qu'elle définit. Tout réel Δ_p-définissable [ce qui se dit dans L(Q)] est limite d'une suite Δ_p-définissable de rationnels.

Un tel corps Δ_p-déf$(\mathbf{R})$ est archimédien et inductif (toute quantification sur des éléments de ce corps se ramenant à des quantifications sur des paramètres rationnels e et b).

On démontre enfin que ce corps est réel-clos : un polynôme P étant donné, on se plonge dans un Δ_q-déf$(\mathbf{R})$ dans lequel il admet une racine [la limite de la suite rationnelle (r_n) définie par $r_n = a + i.(b-a)/2^n$, avec i le plus petit entier tel que $P(r_n) > 0$], puis on montre qu'en fait cette racine est Δ_p-définissable. ■

Note remise le 18 septembre 1989, acceptée le 11 décembre 1989.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] P. CEGIELSKI, *La théorie des corps réels-clos inductifs est une extension conservative de l'Arithmétique de Peano*, Rapport du Laboratoire d'Informatique Théorique et Programmation, Université Paris-VII, 1989.

[2] M. DAVIS, Hilbert's tenth problem is unsolvable, *American Mathematical Monthly* 80, March 1973, p. 233-269; also appendix of Dover reedition of Davis, *Computability and Unsolvability* (1re éd. McGraw-Hill, 1958).

[3] E. MENDELSON, *Introduction to Mathematical Logic*, 1re éd. 1964, 2e éd. 1979, VIII + 328 p., 3e éd. 1987.

[4] S. G. SIMPSON, Subsystems of Z_2 and Reverse Mathematics, *appendix* to Takeuti, *Proof theory*, North Holland, 2e éd., 1987, p. 432-446.

[5] S. G. SIMPSON, Partial realizations of Hilbert's program, *The Journal of Symbolic Logic*, 53, n° 2, juin 1988, p. 349-363.

Laboratoire d'Informatique Théorique et Programmation, 12, *bis rue Paul-Éluard*, 93200 *Saint-Denis* et *Université Paris-VII*, 2, *place Jussieu*, 75251 *Paris Cedex* 05.