MÉMOIRES DE LA S. M. F.

ANNE BAUVAL

La théorie d'un anneau de polynômes

Mémoires de la S. M. F. 2^e série, tome 16 (1984), p. 77-84
<http://www.numdam.org/item?id=MSMF_1984_2_16__77_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p. 77-84

LA THÉORIE D'UN ANNEAU DE POLYNOMES

Anne BAUVAL, Université de Paris 7

0. INTRODUCTION

Pour tout corps F et tout ensemble non vide I, la théorie du premier ordre de l'anneau $F[X_i]_{i\in I}$ détermine la théorie faible du second ordre de F. Avant de détailler nos résultats, dont le théorème est le principal, précisons ce que nous entendons par "théorie faible du second ordre".

DÉFINITIONS

A tout modèle $M = (A ; \mathcal{J})$ d'un langage du premier ordre L, on peut associer

- $Pf(M) = (A, Pf(A) ; \mathcal{J}, \epsilon)$, modèle du langage du premier ordre étendant L par adjonction d'une seconde sorte de variables, parcourant l'ensemble Pf(A) des parties finies de A, et d'un symbole d'appartenance ϵ,

- $Sf(M) = (A, Sf(A) ; \mathcal{J}, \epsilon, \cap)$, modèle du langage du premier ordre étendant L par adjonction d'une seconde sorte de variables, parcourant l'ensemble Sf(A) des suites finies dans A, d'un symbole d'appartenance ϵ, et d'un symbole de concaténation $\cap$,

- $Sf'(M) = (A, \mathbb{N}, Sf(A) ; \mathcal{J}, +, ., t, \ell)$, modèle du langage du premier ordre étendant L par adjonction de deux sortes de variables, l'une parcourant l'ensemble $\mathbb{N}$ des entiers naturels, l'autre parcourant Sf(A), de symboles + et . interprétés par l'addition et la multiplication dans $\mathbb{N}$, d'un symbole de fonction ℓ interprété par l'application de Sf(A) dans $\mathbb{N}$ qui à toute suite associe sa longueur, et d'un symbole de fonction t interprété par l'application de $Sf(A) \times \mathbb{N}$ dans A qui à $(S,n) = (x_o \ldots x_{\ell(S)}, n)$ associe x_n si $n < \ell(S)$ et e si $n \geq \ell(S)$, e étant une constante fixée de M,

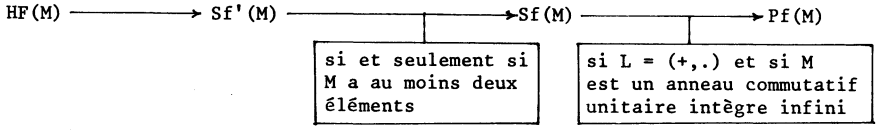
- $HF(M) = (HF(A) ; \mathcal{J}, A, \epsilon)$, modèle du langage du premier ordre étendant L par adjonction d'un prédicat unaire A et d'un symbole d'appartenance ϵ, HF(A) étant l'ensemble des ensembles héréditairement finis au-dessus de A et les éléments de A étant considérés comme atomiques.

La théorie de ce dernier modèle peut être baptisée "théorie faible du second ordre de M".

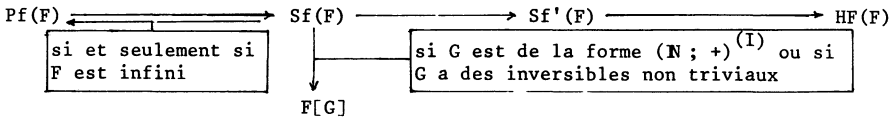
0037-9484/84 03 77 08/$ 2.80/

PRINCIPAUX RÉSULTATS

La notation "... → ..." signifiant "... est définissable dans ..., uniformément en tout modèle M de L", la séquence Pf(M) → Sf(M) → Sf'(M) → HF(M) est triviale, et réciproquement,



De plus, si L = (+,.) et si M est un corps F, ce diagramme peut être complété ainsi, les définissabilités étant uniformes en tout corps F et tout monoïde commutatif totalement ordonnable non trivial G :



ce qui généralise des résultats antérieurs ([R] § 4, [P] théorème 2.1, [B1]).

En outre, pour tout monoïde arithmétique G, l'anneau A[G]est définissable dans HF(A), uniformément en tout anneau A, (en particulier si G est égal à la somme directe $(\mathbb{N}\ ;+)^{(I)}$ avec I au plus dénombrable ; A[G] est alors isomorphe à $A[X_i]_{i\in I}$).

Le langage de Sf peut être assimilé à un fragment de $L_{\omega_1\omega}$. La théorie faible du second ordre d'un corps ne détermine pas toujours sa théorie dans $L_{\omega_1\omega}$, car il existe des corps dénombrables non isomorphes ayant même théorie faible du second ordre ; nous montrerons même qu'il existe $2^{\aleph_0}$ corps dénombrables non isomorphes ayant même théorie faible du second ordre que $\mathbb{R}$.

Nous démontrerons enfin quelques résultats annexes sur les modèles de la théorie d'un anneau de polynômes.

Tous les résultats ci-dessus sont démontrés de façon plus détaillée dans [B2] et [B3].

THÉORIE D'UN ANNEAU DE POLYNOMES

TABLE DES MATIÈRES

A. BAUVAL

I. DÉFINITION DE HF(M) DANS Sf'(M), UNIFORMEMENT EN M

Pour tout entier naturel N, soit E_N la relation binaire sur $\mathbb{N}$ définie par $m E_N n$ si et seulement si $n > N$ et le coefficient de 2^m dans l'écriture de $n - N$ en binaire est 1 ; $HF(\{1,2,\ldots,N\})$ est isomorphe à $(\mathbb{N};\{1,2,\ldots,N\},E_N)$.

Soient $(S,m) \in Sf(A) \times \mathbb{N}$, $N = \ell(S)$, et $a_1,\ldots,a_N \in A$ tels que $S = a_1 \ldots a_N$. Nous dirons que (S,m) représente un élément a de HF(A) si et seulement si $a_1,\ldots,a_N$ sont distincts et l'isomorphisme de $(\mathbb{N};\{1,\ldots,N\},E_N)$ sur $HF(\{a_1,\ldots,a_n\})$ qui envoie i sur a_i pour tout $i \in \{1,\ldots,N\}$ envoie m sur a.

L'ensemble des représentants d'éléments de HF(A), la relation liant deux représentants d'un même élément, l'ensemble des représentants d'éléments de A, et la traduction, en termes de représentants, de l'appartenance dans HF(M) et de l'interprétation $\mathcal{I}$ dans M des symboles non logiques de L, sont définissables dans Sf'(M).

II.- DÉFINITION DE Sf'(M) DANS Sf(M), UNIFORMEMENT EN M AYANT AU MOINS DEUX ÉLÈMENTS

Si M a moins de deux éléments, Sf(M) est définissable dans $(\mathbb{N};+)$, donc sa théorie est décidable, alors que celle de Sf'(M) ne l'est jamais.

Une suite finie S dans A sera représentée dans Sf(M) par la même suite S. Un entier naturel n sera représenté par la suite ee...e (n fois) ; l'ensemble des représentants d'entiers naturels est définissable dans Sf(M).

Des formules assez compliquées permettent de définir les relations $\ell(S) = \ell(S')$ et $\ell(S) \mid \ell(S')$ dans Sf(M). On en déduit une définition dans Sf(M), en termes de représentants, de ℓ,t,+,et ..

III.- DÉFINITION DE Sf(M) DANS Pf(M), UNIFORMEMENT EN M ANNEAU COMMUTATIF UNITAIRE INTÉGRÉ INFINI

Pour tout modèle fini M, Pf(M) est fini, donc sa théorie est décidable, tandis que d'après le paragraphe précédent, celle de Sf(M) ne l'est pas, dès que M a au moins deux éléments, donc dans ce cas, non seulement Sf(M) n'est pas définissable dans Pf(M), mais sa théorie n'est même pas interprétable dans celle de Pf(M).

Un élément x de A sera représenté dans Pf(M) par le même élément x. Soit $S = a_0 a_1 \ldots a_{n-1} \in Sf(A)$ (ou $S = \emptyset$ et $n = 0$) ; nous dirons qu'un élément (y,B,C,D) de $AXPf(A)^3$ est un représentant de S si et seulement si les quatre conditions suivantes sont satisfaites :

1. $y \neq 0$, $1,y,\ldots,y^{n-1}$ sont distincts, et $B = \{1,y,\ldots,y^{n-1}\}$
2. $C = \{a_k / k \in \mathbb{N}, k < n, a_k \neq 0\}$

3. $D = \{a_k y^k / k \in \mathbb{N}, k < n, a_k \neq 0\}$

4. Pour tout entier naturel $k < n$ et pout tout $a \in C\backslash\{a_k\}$, $ay^k \notin D$.

Toute suite a une infinité de représentants.

L'ensemble des représentants d'éléments de Sf(A), la relation liant deux représentants d'une même suite, et la traduction en termes de représentants de ϵ et $\cap$ dans Sf(M) sont définissables dans Pf(M).

IV.- DÉFINITION DE Pf(F) DANS F[G], UNIFORMEMENT EN TOUT CORPS F ET TOUT MONOIDE COMMUTATIF TOTALEMENT ORDONNABLE NON TRIVIAL G

F est définissable dans F[G] par la formule $x = 0 \vee x = 1 \vee$ (x et x - 1 sont inversibles). On utilise un paramètre $P \in F[G]$ tel que pour tout $x \in F$, $P - x$ soit non inversible dans F[G] ; il existe de tels P, par exemple $P = g^2 + g$ avec $g \in G\backslash\{1\}$.

Un élément x de F sera représenté dans F[G] par le même élément x. Un élément non nul Q de F[G] représentera la partie finie $\{x \in F / F[G] \models P - x | Q\}$. Toute partie finie A de F a des représentants (par exemple $Q = \prod_{x \in A} (P - x)$).

La relation liant deux représentants d'une même partie finie de F et la traduction de ϵ dans Pf(F) en termes de représentants sont définissables dans F[G].

V. DÉFINITION DE Sf(F) DANS F[G], UNIFORMEMENT EN TOUT CORPS F ET TOUT MONOIDE COMMUTATIF TOTALEMENT ORDONNABLE NON TRIVIAL G QUI EST DE LA FORME $(\mathbb{N};+)^{(I)}$ OU QUI A DES INVERSIBLES NON TRIVIAUX

La propriété "F est fini" s'exprime par un énoncé dans Pf(F) donc aussi dans F[G] d'après le paragraphe précédent, uniformément en tout corps F et tout monoïde commutatif totalement ordonnable non trivial G. D'après les § III et IV, Sf(F) est définissable dans F[G], uniformément en tout corps F infini et tout monoïde commutatif totalement ordonnable non trivial G. Il reste donc à traiter le cas où F est fini et où G est de la forme $(\mathbb{N};+)^{(I)}$ ou a des inversibles non triviaux.

Pour tout corps fini F, soient N le nombre d'éléments de F, Ω_F l'ensemble des générateurs du groupe cyclique $(F\backslash\{0\}; .)$, $w \in \Omega_F$, f la bijection de $\{0,1,\ldots,N-1\}$ dans F qui à k associe 0 si k = 0 et w^k sinon, et $*$ l'opération sur $\{0,1,\ldots,N-1\}$ tranformée par f^{-1} de l'addition sur F.

Soit $p_0 = 2$, $p_1 = 3,\ldots$ la liste croissante des entiers naturels premiers. En représentant un élément a de F par l'entier $f^{-1}(a)$ et une suite finie $a_0 \ldots a_{n-1}$ dans F par le couple $(\prod_{i<n} p_i^{f^{-1}(a_i)}, n)$ on montre que Sf(F) est définissable dans $(\mathbb{N}; +, ., N, *)$, uniformément en tout corps fini F et tout $w \in \Omega_F$.

On peut également définir $(\mathbf{N}\ ;+,.,N,*)$ dans $F[G];+,.,w)$, uniformément en F corps fini, $w \in \Omega_F$, et G monoïde commutatif totalement ordonnable non trivial et définir Ω_F dans $(F[G];+,.)$ uniformément en F corps fini et G monoïde commutatif totalement ordonnable non trivial, grâce aux formules de R. Robinson [R] dans le cas où G est de la forme $(\mathbf{N}\ ;+)^{(I)}$, et grâce à la propriété suivante dans le cas où G a des inversibles non triviaux : pour tous I,J inversibles dans F[G] tels que $I \notin F$, $F[G] \models I - 1 \mid J - 1$ si et seulement s'il existe un entier relatif m tel que $J = I^m$.

VI.- DÉFINITION DE A[G] DANS HF(A) UNIFORMEMENT EN TOUT ANNEAU A, POUR TOUT MONOIDE ARITHMÉTIQUE G

$(\mathbf{N}\ ;+,.)$ est définissable dans HF(M), uniformément en tout modèle M, donc G est définissable dans HF(A), uniformément en tout anneau A, comme un quotient $(G'\ ;.)/\sim$.

Un élément P de A[G] sera représenté dans HF(A) par toute fonction f d'une partie finie de G' dans A telle que pour tout $g \in G$, si le coefficient de g dans P est non nul, il existe $h \in \mathrm{dom}(f)$ tel que la classe de h modulo $\sim$ soit g, et pour tout $h \in \mathrm{dom}(f)$, f(h) est égal au coefficient dans P de la classe de h modulo $\sim$.

L'ensemble des représentants d'éléments de A[G], la relation liant deux représentants d'un même élément, et la traduction de l'addition et de la multiplication dans A[G] en termes de représentants sont définissables dans HF(A).

REMARQUE.- Pour tout ensemble non vide I et pour tous corps F et F', si $F[X_i]_{i\in I} \equiv F'[X_i]_{i\in I}$, alors pour tout ensemble J, $F[X_j]_{j\in J} \equiv F'[X_j]_{j\in J}$. En effet, d'après les § I, II, V, HF(F) est définissable dans $F[X_i]_{i\in I}$, uniformément en tout corps F ; d'après le présent paragraphe, si J est fini ou dénombrable, $F[X_j]_{j\in J}$ est définissable dans HF(F), uniformément en tout corps F ; enfin, si J est infini, pour tout corps F, $F[X_j]_{j\in J} \equiv F[X_n]_{n\in\omega}$.

VII.- EXISTENCE DE $2^{\aleph_o}$ CORPS DÉNOMBRABLES NON ISOMORPHES AYANT MÊME THÉORIE FAIBLE DU SECOND ORDRE QUE $\mathbf{R}$

Nous allons construire une famille $(F_\lambda)_{\lambda<2^{\aleph_o}}$ de sous-corps dénombrables de $\mathbf{R}$, distincts et sous-structures élémentaires au sens du second ordre faible de $\mathbf{R}$, (donc réel-clos).

De tels corps sont non isomorphes, car si f est un isomorphisme entre deux sous-corps réel-clos F et F' de $\mathbf{R}$, f fixe 1, donc f fixe tout élément de $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$; de plus, f transforme tout carré en un carré donc f préserve l'ordre, et comme

$\mathbb{Q}$ est dense dans $\mathbb{R}$, f est l'identité sur F, donc F' = F.

Pour construire cette famille, nous utiliserons la propriété suivante : pour tout modèle M = (A ; J) et pour toute sous-structure élémentaire N' de HF(M), il existe une partie B de A telle que N' = HF(B ; $J_{\restriction B}$). Donc pour tout $a \in \mathbb{R}$, par le théorème de Löwenheim-Skolem descendant, il existe un sous-corps dénombrable F de $\mathbb{R}$ tel que $a \in F$ et $HF(F) \prec HF(\mathbb{R})$.

On construit la famille $(F_\lambda)_{\lambda<2^{\aleph_o}}$ par induction. Il existe un sous-corps dénombrable F_o de $\mathbb{R}$ tel que $HF(F_o) \prec HF(\mathbb{R})$. Soit μ un ordinal inférieur à $2^{\aleph_o}$ et supposons les F_λ construits pour tout $\lambda < \mu$. $\text{card}(\bigcup_{\lambda<\mu} F_\lambda) \leq (\text{card}(\mu) . \aleph_o) < 2^{\aleph_o}$, donc il existe $a \in \mathbb{R}$ tel que $a \notin \bigcup_{\lambda<\mu} F_\lambda$. On prend pour F_μ un sous-corps dénombrable de $\mathbb{R}$ contenant a et tel que $HF(F_\mu) \prec HF(\mathbb{R})$. Ainsi pour tout $\lambda < \mu$, $F_\lambda \neq F_\mu$.

VIII.- MODÈLES DE LA THÉORIE D'UN ANNEAU DE POLYNOMES

THÉORÈME.- Soit B un anneau commutatif intègre définissable dans $B[X_1,\ldots,X_n]$ par une formule Con. 1) Pour tout anneau A élémentairement équivalent à $B[X_1,\ldots,X_n]$, si B' est le sous-anneau défini dans A par Con et si $(B'^*)^{-1}A$ est factoriel ou noethérien (en particulier si A l'est), alors A est isomorphe à $B'[X_1,\ldots,X_n]$.

2) Pour tout sous-anneau élémentaire A de $B[X_1,\ldots,X_n]$, il existe $Y_1,\ldots,Y_n \in B[X_1,\ldots,X_n]$ et B' sous-anneau élémentaire de B tels que $A = B'[Y_1,\ldots,Y_n]$ et $B[X_1,\ldots,X_n] = B[Y_1,\ldots,Y_n]$.

En utilisant les formules de R. Robinson [R] et en analysant les propriétés de la fonction "degré en une indéterminée d'un polynôme", on parvient à construire des formules E_k, G_k (pour $k < n$) telles que sous les hypothèses du théorème, $B[X_1,\ldots,X_k] \models E_k(X_1,\ldots,X_k)$ et pour tous $Y_1,\ldots,Y_k \in A$ tels que $A \models E_k(Y_1,\ldots,Y_k)$, et pour tout $Q \in A$, $A \models C_k(Y_1,\ldots,Y_k,Q)$ si et seulement si $Q \in B'[Y_1,\ldots,Y_k]$, et $Y_1,\ldots,Y_k$ sont algébriquement indépendants sur B'. D'où le théorème.

COROLLAIRE.- Soient n un entier naturel non nul, et B l'un des anneaux suivants $\mathbb{Z}$, $\mathbb{Q}$, tout corps algébriquement clos de degré de transcendance fini sur son sous-corps premier, le corps des réels algébriques, ou tout corps fini.

1) Tout anneau factoriel ou noethérien élémentairement équivalent à $B[X_1,\ldots,X_n]$ est isomorphe à $B[X_1,\ldots,X_n]$.

2) $B[X_1,\ldots,X_n]$ n'a pas de sous-anneau élémentaire strict.

Pour tout ensemble non vide I, tout corps F est définissable dans $F[X_i]_{i\in I}$, et on peut définir $\mathbb{Z}$ dans $\mathbb{Z}[X_i]_{i\in I}$, car $\mathbb{N}$ est définissable par la formule sui-

vante, qui utilise les formules Pri et Pow de R. Robinson [R] :
$N(R) : \forall P \exists Q [(Pri(P) \wedge P \neq 2 \wedge P \neq 3) \rightarrow (Pow(P,Q) \wedge (P-1)^2 | Q - R(P-1) - 1)]$.
Chacun des anneaux du corollaire vérifie donc les hypothèses du théorème, et ces anneaux sont déterminés à isomorphisme près par leur théorie faible du second ordre, et n'ont pas de sous-structure élémentaire (au sens du second ordre faible) stricte, d'où le corollaire.

$o^o o$

REFERENCES

[B1] A. BAUVAL : Une condition nécessaire d'équivalence élémentaire entre anneaux de polynômes sur des corps, C.R. Acad. Sc., Paris, t. 295 (1982), série I, pp. 31-33.

[B2] A. BAUVAL : La théorie du premier ordre des anneaux de polynômes sur des corps, thèse de 3° cycle, Université de Paris VII, 1983.

[B3] A. BAUVAL : Polynomial rings and weak second order logic, soumis au J.S.L.

[P] P.C. PAPPAS : The model theoretic structure of group rings, Ph. D. Thesis, Pennsylvania State University, 1982.

[R] R. ROBINSON : Undecidable rings, Transactions A.M.S. 1951, pp. 181-203.

Anne Bauval
Université de Paris 7
U.E.R. de Mathématiques
Tour 45-55 - 5ème étage
2, Place Jussieu
75251 PARIS CEDEX 05