Groupe de travail
d'analyse ultramétrique

Luc Bélair

Le théorème de MacIntyre sur les ensembles définissables dans les corps p-adiques

Groupe de travail d'analyse ultramétrique, tome 13 (1985-1986), p. 15-30

<http://www.numdam.org/item?id=GAU_1985-1986__13__15_0>

LE THEOREME DE MACINTYRE SUR LES ENSEMBLES DEFINISSABLES DANS LES CORPS p-ADIQUES

Luc Bélair

§0. INTRODUCTION

Soit p un nombre premier, $\mathbb{Q}_p$ le corps des nombres p-adiques, $\mathbb{Z}_p$ l'anneau des entiers p-adiques et v_p la valuation p-adique sur $\mathbb{Q}_p$. Considérons d'abord trois types de sous-ensembles de l'espace p-adique, que nous appellerons ensembles de base.

Ensembles de base

I. $\{ x \in \mathbb{Q}_p^m : f(x) = 0 \}$

II. $\{ x \in \mathbb{Q}_p^m : v_p(g(x)) \leq v_p(f(x)) \}$

III. $\{ x \in \mathbb{Q}_p^m :$ il existe $y \in \mathbb{Q}_p$ t.q. $f(x) = y^n \}$

où $f,g \in \mathbb{Q}_p[X_1,\ldots,X_m]$, $m,n \in N$.

Une combinaison booléenne d'ensembles de base est un sous-ensemble S de $\mathbb{Q}_p^m$ obtenu en prenant un nombre fini d'intersections, d'unions et de complémentaires d'ensembles de type I, II et III. Un ensemble définissable est un ensemble obtenu par un nombre fini de projections et de complémentaires de projection à partir de tels ensembles S. Ainsi $D = \{ x \in \mathbb{Q}_p^m : \exists\, y \in \mathbb{Q}_p^k \ (x,y) \in S \}$ est l'ensemble définissable obtenu de $S \subset \mathbb{Q}_p^{m+k}$ par la projection $\mathbb{Q}_p^{m+k} \longrightarrow \mathbb{Q}_p^m$. Les entiers p-adiques forment un ensemble définissable qui est en fait du type III. En effet on a $\mathbb{Z}_p = \{ x \in \mathbb{Q}_p : \exists\, y \in \mathbb{Q}_p \ 1 + px^2 - y^2 = 0 \}$. Le théorème de Macintyre donne la structure des ensembles définissables comme combinaisons booléennes d'ensembles de base.

Théorème de Macintyre ([M]). Soit $S \subset \mathbb{Q}_p^{m+k}$ une combinaison booléenne d'ensembles de base alors $D = \{ x \in \mathbb{Q}_p^m : \exists\, y \in \mathbb{Q}_p^k \ (x,y) \in S \}$ est aussi une combinaison booléenne d'ensembles de base.

Tel quel, ce théorème a été utilisé par J.Denef ([D]) en conjugaison avec des méthodes standard pour montrer la rationalité de séries de Poincaré définies sur $\mathbb{Z}_p$. Une analyse plus fine des ensembles définissables lui a permis de donner des démonstrations élémentaires et de généraliser ces résultats. Dans un autre ordre d'idée, le théorème de Macintyre s'avère un élément clé dans l'introduction par E.P.Robinson d'un schéma affine, le spectre p-adique ([R],[B],[S],[B-S]), qui en un mot se veut l'analogue p-adique du spectre réel introduit par M.-F.Coste-Roy et M.Coste en géométrie algébrique réelle ([C-R]).

Nous présentons ici une démonstration essentiellement complète du théorème de Macintyre, qui fait appel à la théorie des modèles. Nous avons voulu réduire au minimum les ingrédients de logique mathématique nécessaires. Il existe maintenant des preuves directes [W], [D1] et les ensembles définissables sont étudiés de façon plus précise dans [D],[D1],[D2]. La théorie des modèles fournit cependant une démonstration qui compense son caractère non constructif en étant plus conceptuelle. La théorie des modèles de $\mathbb{Q}_p$ fut d'abord étudiée dans [A-K] et [E]. Celle de ses extensions finies est traitée dans [P-R] où, par exemple, on généralise le théorème de Macintyre.

§1. THEORIE DES MODELES

On peut exprimer le théorème de Macintyre en termes logiques. A tout ensemble $S \subset \mathbb{Q}_p^m$ comme ci-dessus on associe la formule $\phi_S(\bar{x})$ qui décrit S i.e. les conditions qui définissent S même, où $\bar{x}$ désigne la multi-variable $(x_1,\ldots,x_m)$:

Exemple. Soit $f,g,h \in \mathbb{Q}_p[X_1,\ldots,X_m]$ alors

à $S = (\{ x : f(x)\neq 0 \}^c \cap \{ x : v_p(1) \leq v_p(g(x)^{-1}) \}) \cup \{ x : \exists\, y\in\mathbb{Q}_p \ y^n = h(x) \}$

on associe $\phi_S(\bar{x}) := (f(\bar{x})\neq 0 \wedge v_p(1) \leq v_p(g(\bar{x})^{-1})) \vee (\exists y\ y^n = h(\bar{x}))$.

Notons que ϕ_S ne contient pas de quantificateur $\exists,\forall$ sauf ceux provenant de la description d'ensembles du type III. Traduit en ces termes le théorème de Macintyre devient:

Théorème de Macintyre. Pour tout $S \subset \mathbb{Q}_p^{m+k}$ comme ci-dessus il existe une formule $\psi(\bar{y})$ sans quantificateur sauf ceux provenant de la description d'ensemble du type III telle que dans $\mathbb{Q}_p$ on ait $\exists \bar{x}\ \phi_S(\bar{x},\bar{y})$ ssi $\psi(\bar{y})$.

L'idée fondamentale de la théorie des modèles pour étudier $\mathbb{Q}_p$ est de le remplacer par une classe de corps qui partagent de mêmes propriétés de premier ordre dans un langage approprié. Pour étudier les corps on adopte le langage de premier ordre L qui contient les opérations et constantes habituelles $+,-,\cdot,^{-1},0,1$, des variables $x,y,z,\ldots$ qui prennent leurs valeurs sur les éléments des corps en question, ainsi que les signes logiques standard $\wedge,\vee,\sim$(négation) et les quantificateurs $\exists,\forall$ sur les variables. On s'intéresse à $\mathbb{Q}_p$ en tant que corps valué i.e. muni d'une valuation au sens de Krull (groupe de valuation pas forcément $\mathbb{Z}$), la valuation p-adique. On introduit donc un langage des corps valués L(V) en ajoutant à L un symbole de relation à une variable V(x) pour désigner l'anneau de valuation dans un corps valué donné. Ainsi on lit V(x) comme $x \in V$. On introduit les notions suivantes.

Définition. Soit $f,g \in \mathbb{Z}[X_1,\ldots,X_m]$

(1) Les formules de base de L = les $f(\bar{x}) = 0$

(2) Les formules de base de L(V) = on ajoute les $V(f(\bar{x})\cdot g(\bar{x})^{-1})$

(3) Les formules de L, L(V) = la plus petite classe contenant les formules de base et close p/r à $\wedge,\vee,\sim,\exists,\forall$.

(4) Les formules sans quantificateur de L, L(V) = cette fois on clôt p/r à $\wedge,\vee,\sim$ seulement. Par exemple, pour les corps, toute formule sans quantificateur de L est équivalente à une formule du type $f_1(\bar{x})=0 \wedge\ldots\wedge f_k(\bar{x})=0 \wedge g(\bar{x})\neq 0$.

(5) Un énoncé σ = une formule où toutes les variables sont quantifiées. Par

exemple $\exists \bar{x}\ f(\bar{x})=0$.

(6) Une théorie T = un ensemble d'énoncés. Par exemple dans L on a la théorie CAC des corps algébriquement clos. Soit $f_n(X,Y_1,\ldots,Y_n)$ le polynôme générique unitaire de degré n alors CAC = axiomes de corps + $\{\forall \bar{y}\exists x\ f_n(x,\bar{y})=0 : n\in\mathbb{N}\}$. Dans un corps donné on interprète les formules de la façon évidente et on dit qu'un corps K est un modèle d'une théorie T si tout énoncé de T est vrai dans K .

(7) On écrit $T \models \sigma$ ssi σ est vrai dans tout modèle de T . Par exemple dans L soit T=CAC et $\sigma_{100} := \exists x_1 \ldots \exists x_{100} \bigwedge_{i\neq j} x_i \neq x_j$ alors $T \models \sigma_{100}$ puisque tout corps algébriquement clos est infini.

Toutes ces notions de formules etc. sont définies relativement à un langage fixé, ici L, L(V), $L(V,P_n)$ (ci-dessous) auquel on ajoutera à l'occasion des constantes pour pouvoir parler des extensions d'un corps fixé. Un théorème fondamental de la théorie des modèles est le théorème de compacité. C'est l'outil principal de la théorie des modèles que nous allons utilisé. Nous renvoyons à [Ek] pour une preuve utilisant les ultraproduits.

Théorème de compacité. Soit T une théorie et σ un énoncé alors $T \models \sigma$ ssi il existe un sous-ensemble fini T' de T tel que $T' \models \sigma$.

Par exemple on a vu que $CAC \models \sigma_{100}$. Mais pour voir qu'un corps algébriquement clos possède au moins cent éléments il suffit de savoir que tout polynôme de degré inférieur ou égal à cent admet une racine, ce qui est bien donné par un sous-ensemble fini de CAC . Notons que la contraposée de ce théorème nous dit, en prenant par exemple $\sigma := \forall x\ (x\neq x)$, qu'un ensemble d'énoncés admet un modèle si et seulement si tout sous-ensemble fini en admet un (Nous n'utiliserons cette remarque que dans l'appendice).

Avant de revenir à $\mathbb{Q}_p$ rappelons qu'un anneau de valuation V d'un corps détermine une valuation sur ce corps de façon essentiellement unique et qu'on peut décrire (dans L(V)) les opérations algébriques et la relation d'ordre du groupe de

valuation et du corps des restes de la valuation associée grâce à la structure d'anneau de V. De sorte que bien qu'ayant fixé le langage $L(V)$ pour préciser nos résultats il sera commode par la suite de parler en termes de la valuation induite que nous noterons génériquement par v. On pourra consulter [Ri] pour les éléments de théorie des valuations utilisés ici. Nous introduisons maintenant la classe de corps valués associée à $\mathbb{Q}_p$.

Définition. La théorie des corps p-adiquement clos, CpC, est celle qu'on obtient en traduisant dans $L(V)$ les propriétés suivantes de corps valué (K,v). Soit $\mathrm{val}\,K$ le groupe de valuation et $\mathrm{res}\,K$ le corps des restes :

1) (K,v) satisfait le lemme de Hensel et est de caractéristique 0

2) $\mathrm{val}\,K$ est un $\mathbb{Z}$-groupe, plus précisément $v(p)$ y est le plus petit élément positif et pour chaque $n \geq 2$ on a $\forall\gamma\ \exists\delta\ \ \gamma = n.\gamma_1 + r.v(p)$ pour un $0 \leq r < n$

3) $\mathrm{res}\,K$ est (canoniquement) égal à $\mathbb{F}_p$.

En particulier $\mathbb{Q}_p$ avec la valuation p-adique est un corps p-adiquement clos de même que les nombres algébriques p-adiques i.e. la clôture algébrique relative de $\mathbb{Q}$ dans $\mathbb{Q}_p$ avec la valuation induite. Par abus, on parlera "des CpC".

Définition. Une théorie T d'un langage L admet l'élimination des quantificateurs, ou EQ, si pour toute formule sans quantificateur $\phi(\bar{x},\bar{y})$ de L il existe une formule sans quantificateur $\psi(\bar{y})$ de L t.q. dans tout modèle de T on ait $\exists\bar{x}\ \phi(\bar{x},\bar{y})$ ssi $\psi(\bar{y})$, autrement dit t.q. $T \models \forall\bar{y}\ (\exists\bar{x}\ \phi(\bar{x},\bar{y}) \leftrightarrow \psi(\bar{y}))$.

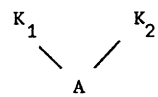
Sous la deuxième forme où nous l'avons énoncé le théorème de Macintyre mentionne des formules "sans quantificateur sauf ceux provenant de formules du type $\exists y\ y^n = f(\bar{x})$ ". Or ces formules ne sont nulles autres que les formules sans quantificateur qu'on obtient en ajoutant les nouvelles formules $P_n(f(\bar{x}))$ comme formules de base et en les interprétant dans tout CpC comme $\exists y\ y^n = f(\bar{x})$. Plus précisément, on introduit le langage $L(V,P_n)$ qu'on obtient en ajoutant à $L(V)$ un symbole de relation à une variable $P_n(x)$ pour $n=2,3,\ldots$. On ajoute les $P_n(f(\bar{x}))$ aux formules de base et $P_n(x) \leftrightarrow \exists y\ y^n = x$ aux axiomes de CpC.

On peut maintenant formuler précisément le théorème de Macintyre.

Théorème de Macintyre. La théorie CpC admet EQ dans le langage $L(V,P_n)$.

On a un critère de la théorie des modèles pour EQ en termes de sous-stuctures. Pour notre propos il suffit de dire qu'une sous-structure A d'un modèle K correspond dans L à un sous-corps, dans L(V) à un sous-corps muni de la valuation induite, et dans $L(V,P_n)$ à un sous-corps muni de la valuation induite dans lequel on distingue les ensembles $P_n^A = A \cap K^n$.

Proposition I. Une théorie T admet EQ ssi pour toute paire de modèles K_1, K_2 de T ayant une sous-stucture commune A , pour toute formule sans quantificateur $\phi(\bar{x},\bar{y})$ et pour tout $\bar{a} \in A$, la formule $\exists \bar{x}\ \phi(\bar{x},\bar{a})$ est vraie dans K_1 ssi elle l'est dans K_2 .



modèles de T , $\exists \bar{x}\ \phi(\bar{x},\bar{a})$ vrai dans K_1 ssi vrai dans K_2

sous-stucture

.

Une preuve utilisant le théorème de compacité se trouve en appendice. Nous utiliserons la notion voisine de théorie modèle-complète.

Définition. Une théorie T est modèle-complète si le critère énoncé dans la proposition précédente est valide quand A est un modèle de T . Ce qui est donc équivalent à ce que, pour toute paire de modèles $K \subset K'$ où K est une sous-stucture de K' , pour toute formule $\phi(\bar{x},\bar{y})$ sans quantificateur et tout $\bar{k} \in K$, on ait $\exists \bar{x}\ \phi(\bar{x},\bar{k})$ vrai dans K ssi vrai dans K' .

Exemple. ([Ro]) Dans L la théorie CAC est modèle-complète.

En effet soit $K \subset K'$ algébriquement clos.Comme on l'a déjà remarqué une formule sans quantificateur $\phi(\bar{x},\bar{y})$, pour CAC , peut se ramener à la forme $f_1(\bar{x},\bar{y})=0 \wedge \ldots \wedge f_s(\bar{x},\bar{y})=0 \wedge g(\bar{x},\bar{y})\neq 0$ où $f_i, g \in \mathbb{Z}[\bar{X},\bar{Y}]$. Ainsi il faut vérifier qu'étant donné un système (§)

$$(\S) \qquad f_1(\bar{x})=0 \ , \ \ldots, \ f_s(\bar{x})=0 \ , \ g(\bar{x})\neq 0 \qquad , \ f_i, g \in K[\bar{X}] \ .$$

le système (§) a une solution dans K ssi il en a une dans K' . Ceci est une forme du théorème des zéros de Hilbert mais nous présentons la preuve de Robinson puisque nous suivrons un schéma analogue pour traiter le cas p-adique. Une direction est triviale. Supposons donc que (§) a une solution $x_1,\ldots,x_m$ dans K' . On peut supposer que $x_i \notin K$ pour quelque i . Considérons

$$K \subset K(x_1)^a \subset K(x_1,x_2)^a \ \ldots \subset K(x_1,\ldots,x_m)^a \subset K'$$

où ^{a} désigne la clôture algébrique. Ceci nous donne une suite croissante de corps intermédiaires algébriquement clos K_i t.q. (§) a une solution dans le dernier corps de la suite et le degré de transcendance $\deg \mathrm{tr}\ K_{i+1}/K_i = 1$. On peut donc supposer $\deg \mathrm{tr}\ K'/K = 1$ puisque si on établit le résultat dans ce cas alors de proche en proche (§) aura une solution dans tous les K_i et donc dans K . Soit donc $\deg \mathrm{tr}\ K'/K = 1$. Alors (§) a une solution dans toute extension algébriquement close propre K'' de K puisque K'' contient un sous-corps algébriquement clos de degré de transcendance 1 sur K qui est isomorphe à K' . Ainsi on a

$$CAC + \Delta(K) + \{ \ t \neq k : k \in K \ \} \models \exists \bar{x} \ \phi(\bar{x},\bar{k})$$

dans le langage L auquel on ajoute une constante k pour chaque élément $k \in K$ et une autre constante t , et où $\Delta(K)$, appelé le diagramme de K , est "la table de multiplication de K " i.e. toutes les formules $k_1+k_2=k_3$, $k_1 \cdot k_2 = k_3$, $k_1 \neq k_2$ qui sont vraies dans K . Il est clair qu'un modèle de $\Sigma = CAC+\Delta(K)+\{t\neq k : k\in K\}$ n'est rien d'autre qu'une extension K''/K comme ci-dessus avec un $t \in K''\backslash K$. Par le théorème de compacité il existe un sous-ensemble fini Σ' de Σ t.q. $\Sigma' \models \exists \bar{x} \ \phi(\bar{x},\bar{k})$ et donc en particulier on a

$$CAC + \Delta(K) + \{ \ t \neq k_1,\ldots,t \neq k_n \ \} \models \exists \bar{x} \ \phi(\bar{x},\bar{k})$$

pour certains $k_i \in K$ en nombre fini. Mais K lui-même est un modèle de $CAC+\Delta(K)+\{t\neq k_i : i=1,\ldots,n\}$ puisque K est infini. D'où $\exists \bar{x} \ \phi(\bar{x},\bar{k})$ est vrai

dans K i.e. (§) a une solution dans K .

Corollaire. CAC admet EQ dans L .

En effet dans notre critère pour EQ on pourra tester la véracité de la formule $\exists \bar{x}\ \phi(\bar{x},\bar{a})$, $\bar{a} \in A$, dans la clôture algébrique A^a de A , dont les deux modèles contiennent des copies isomorphes au-dessus de A . Notons que ce corollaire, interprété en termes de sous-ensembles, est le théorème de Chevalley affirmant que la projection d'un ensemble constructible de $\mathbb{C}^{m+k}$ sur $\mathbb{C}^m$ est de nouveau un ensemble constructible de $\mathbb{C}^m$. Le théorème de Macintyre peut donc être interprété en termes de constructibles p-adiques à savoir les ensembles S .

Nous allons suivre ce schéma pour démontrer le théorème de Macintyre dans sa version logique. Les ingrédients essentiels dans la preuve ci-dessus était
1) l'existence et l'unicité de la clôture algébrique sur un corps de base et
2) le fait que les conditions $\{ t \neq k : k \in K \}$ pour K algébriquement clos déterminent l'extension $K(t)/K$ à K-isomorphisme près.

§2. LE THEOREME DE MACINTYRE

Nous allons d'abord voir qu'on a une "clôture p-adique" . Pour (K,v) un corps valué, V_K désigne l'anneau de valuation. Soit R un anneau alors $R^\cdot$ désigne le groupe multiplicatif des éléments inversibles et $R^{\cdot n}$ le sous-groupe des puissances n-ièmes pour n=2,3,... .

Proposition 2.1. Soit $(K,v)/(E,v)$ une extension de corps valué où K est un CpC et E est relativement algébriquement clos dans K . Alors E est un CpC .

Démonstration. Il est clair que E est hensélien et que res $E = \mathbb{F}_p$. La proposition découle donc du lemme suivant.

Lemme 2.2. Pour chaque $n\geq 2$, $K^{\cdot}/K^{\cdot n} \simeq \mathbb{Q}_p^{\cdot}/\mathbb{Q}_p^{\cdot n}$ avec mêmes représentants dans $\mathbb{N}$. Plus exactement pour tout $x\in K^{\cdot}$ on a $\lambda p^{-r}x\in K^{\cdot n}$ pour quelque $\lambda=1,\ldots,p^{2v_p(n)+1}$ $p\nmid\lambda$, et quelque $0\leq r<n$.

Démonstration. On a $v(x) = n.v(y) + r.v(p)$ pour quelque $y\in K$, $0\leq r<n$. Ainsi $v(xy^{-n}p^{-r}) = 0$ et donc $xp^{-r} \equiv u \mod K^{\cdot n}$ où $v(u)=0$. Or par le lemme de Hensel $u \in K^{\cdot n}$ ssi u "$\in$" $(V_K/(p^s))^{\cdot n} \simeq (\mathbb{Z}/(p^s))^{\cdot n}$ où $s=2v_p(n)+1$. □

La preuve de la proposition suivante est reprise de [P-R].

Proposition 2.3. Soit (K,v) un CpC . Alors (K,v) est maximal de dimension (dans la terminologie de F.Delon) i.e. pour toute extension E/K finie on a $[E:K]=ef$ où e est l'indice de ramification et f le degré résiduel.

Démonstration. Le sous-groupe $\mathbb{Z}.v(p)$ de val K engendré par $v(p)$ est un sous-groupe convexe. On peut donc considérer la valuation composée w :

$$K^{\cdot} \xrightarrow{v} \text{val } K \longrightarrow \text{val } K/\mathbb{Z}.v(p) \qquad (w)$$

Le corps des restes K_w de (K,w) est de caractéristique 0 et on vérifie aisément que, par image réciproque, v induit une valuation sur K_w , qu'on notera aussi v , et telle que res (K_w,v) = res (K,v) et val $K_w = \mathbb{Z}.v(p)$. D'autre part (K,v) hensélien implique que (K,w) et (K_w,v) le sont aussi. Or la théorie des valuations assure que (K,w) étant hensélien avec corps des restes de caractéristique 0 , et (K_w,v) étant hensélien de caractéristique 0 avec groupe de valuation isomorphe à $\mathbb{Z}$, sont tous deux maximaux de dimension. Montrons qu'alors (K,v) est lui-même maximal de dimension. En effet on peut reproduire cette construction dans une extension finie E/K en prenant cette fois la clôture convexe de $\mathbb{Z}.v(p)$ dans val E qui sera égale à $\mathbb{Z}.v(\pi)$ pour un certain $\pi\in E$. On a alors les extensions $(E,w)/(K,w)$, $(E_w,v)/(K_w,v)$ et

$$[E:K] = [E_w:K_w]\,[\text{val } E/\mathbb{Z}.v(\pi):\text{val } K/\mathbb{Z}.v(p)] \qquad .$$

Comme K_w est maximal de dimension et $\mathbb{Z}.v(p)=\mathbb{Z}.v(\pi)\cap\text{val } K$ on peut développer

le membre de droite et obtenir l'égalité voulue. □

En particulier un CpC n'admet aucune extension algébrique immédiate propre.

Lemme 2.4. Soit $(L,v)/(K,v)$ une extension de corps valués où K,L sont des CpC et L/K est algébrique. Alors $L = K$.

Démonstration. Comme val K et val L sont des $\mathbb{Z}$-groupes avec même plus petit élément positif on a $n.\text{val } K = n.\text{val } L \cap \text{val } K$ pour tout entier n. Or L/K algébrique implique que val L/val K est torsion d'où val L=val K, l'extension est immédiate, et $L=K$. □

On a donc une clôture p-adique pour un sous-corps valué d'un CpC : sa clôture algébrique relative. Cependant cette clôture n'est en général pas unique en tant que corps valué car il y a plusieurs façons de plonger un groupe abélien ordonné discret dans un $\mathbb{Z}$-groupe. La proposition suivante montre que c'est le seul obstacle.

Proposition 2.5. (Unicité de la clôture p-adique dans le langage $L(V,P_n)$)
Soit $(A_i,v_i) \subset (K_i,v_i)$ $i=1,2$ où K_i est un CpC et K_i/A_i est algébrique. Soit $f : A_1 \xrightarrow{\sim} A_2$ un isomorphisme de corps valué t.q. $K_1^{\cdot n} \cap A_1 = K_2^{\cdot n} \cap A_2$ via f pour tout n. Alors f se prolonge en un isomorphisme de corps valué $K_1 \simeq K_2$.

Démonstration. Il suffit de prolonger f à un sous-corps intermédiaire A_1' t.q. $n.\text{val } A_1' = n.\text{val } K_1 \cap \text{val } A_1'$ pour tout n, car alors val A_1' sera un $\mathbb{Z}$-groupe et en passant au hensélisé $A_1'^h \simeq A_2'^h = f(A_1')^h$ les $A_i'^h$ seront des CpC et on pourra conclure par le lemme 2.4. Il suffit évidemment de considérer $n=q$ premier. Soit donc q premier, $a_1 \in A_1$, $a_2 = f(a_1)$, t.q. $v(a_1)/q \in \text{val } K_1 \setminus \text{val } A_1$. Notons que $X^q - a_i$ est irréductible sur A_i. On peut supposer que $a_1 \in K_1^{\cdot q}$ (cf.2.2) et donc aussi $a_2 \in K_2^{\cdot q}$. Soit $y_1 \in K_1$ t.q. $y_1^q = a_1$ et $e_n \in \mathbb{N}$ $n=2,3\ldots$ t.q. $e_n y_1 \in K_1^{\cdot n}$. Nous allons prolonger f à $A_1(y_1)$ tout en préservant ses propriétés ce qui assurera $v(a_1)/q \in \text{val}(\text{dom } f)$. Ainsi un isomorphisme partiel maximal prolongeant f et préservant ses propriétés nous donne le prolongement de f cherché. Notons

que la valuation induite sur $A_1(y_1)$ est complètement déterminée : on a

$$v(c_0 + c_1y_1 + \ldots + c_{q-1}y^{q-1}) = \min v(c_iy^i)$$

car $v(y_1) \notin \text{val } A_1$ et q est premier. Il s'agit donc de bien choisir une racine q-ième de a_2. On la choisit comme suit.

$$(\S) \quad \exists\, y_2 \in K_2 \text{ t.q. } y_2^q = a_2 \text{ et } e_n y_2 \in K_2^{\cdot n} \text{ pour } n=2,3\ldots$$

(§) $\Rightarrow$ la proposition : soit un tel y_2. On a un isomorphisme de corps valués $\overline{f} : A_1(y_1) \xrightarrow{\sim} A_2(y_2)$ qui prolonge f et t.q. $\overline{f}(y_1)=y_2$. Il faut voir que $K_1^{\cdot n} \cap A_1(y_1) = K_2^{\cdot n} \cap A_2(y_2)$ via $\overline{f}$. Soit $x_1 \in A_1(y_1)$, $x_2=\overline{f}(x_1)$. On a $v(x_1d_1y_1^j)=0$ pour un $d_1 \in A_1$. Posons $d_2=f(d_1)$, ainsi $v(x_2d_2y_2^j)=0$. Il existe $\lambda \in \mathbb{N}$ t.q. $v(\lambda)=0$ et $\lambda x_1d_1y_1^j \in K_1^{\cdot n}$ (c.f.2.2) et donc aussi $\lambda x_2d_2y_2^j \in K_2^{\cdot n}$ (c.f.2.2 et le fait que $V_{A_i}/(p^s) = V_{K_i}/(p^s) \simeq \mathbb{Z}/(p^s)$). D'où $x_1 \in K_1^{\cdot n}$ ssi $\lambda d_1y_1^j \in K_1^{\cdot n}$ ssi $\lambda d_1e_n^{-j} \in K_1^{\cdot n}$ ssi $\lambda d_2e_n^{-j} \in K_2^{\cdot n}$ ($\lambda d_1e_n^{-j} \in A_1$), ssi $\lambda d_2y_2^j \in K_2^{\cdot n}$ ssi $x_2 \in K_2^{\cdot n}$.

Preuve de (§) : notons d'abord qu'il y a le même nombre de racines q-ièmes de 1 dans les K_i : elles sont contenues dans le hensélisé de $(\mathbb{Q},v_p) \subset (K_i,v_i)$. Si il y en a une seule alors il y a un seul y_2 et rien à montrer puisque dans ce cas $x \in K_i^{\cdot n}$ ssi $x^q \in K_i^{\cdot nq}$ et $(e_ny_1)^q = e_n^q a_1 \in A_1$ etc. Soit donc $z \in K_2$ une racine primitive q-ième de 1 et b t.q. $b^q=a_2$. Alors les racines q-ième de a_2 sont $b, bz, \ldots, bz^{q-1}$. Supposons (§) faux. Alors il existe $n_0,\ldots,n_{q-1}$ tel que $e_{n_j}bz^j \notin K_2^{\cdot n_j}$ et donc $e_nbz^j \notin K_2^{\cdot n}$ où $n=\text{ppcm}(n_j)$ ($e_n^{-1}e_{n_j} \in K_i^{\cdot n_j}$). Mais $e_ny_1 \in K_1^{\cdot n}$ implique $e_n^qa_1 \in K_1^{\cdot nq}$, d'où $e_n^qa_2=(e_nb)^q \in K_2^{\cdot nq}$, $(e_nbx^n)^q=1$ pour un certain $x \in K_2$, et $e_nbz^j \in K_2^{\cdot n}$ pour quelque j, contradiction. □

De la même façon que pour CAC le théorème de Macintyre est donc un corollaire de la proposition suivante.

Proposition 2.6. CpC est modèle-complète dans le langage $L(V,P_n)$.

Démonstration. Soit $(K,v) \subset (K',v)$ des CpC . Notons que K est nécessairement une sous-structure i.e. $P_n^K = K^n = K \cap K'^n$ car par ce qui précède K est rel. alg. clos dans K' . La formule test $\phi(\bar{x},\bar{k})$ est ici de la forme

$$f_1(\bar{x})=0 \wedge \ldots \wedge f_\ell(\bar{x})=0 \wedge g(\bar{x})\neq 0$$

$$\wedge \ (\underset{i\ j}{\mathbb{M}\mathbb{W}} (\sim)P_{n_{ij}}(h_{ij}(\bar{x})) \ \wedge \ (\underset{s\ t}{\mathbb{M}\mathbb{W}} (\sim)V(g_{st}(\bar{x})\cdot h_{st}(\bar{x})^{-1}))$$

où les $f,g,h \in K[X_1,\ldots,X_m]$ et où $(\sim)$ indique qu'on a possiblement une négation. Encore une fois on montre l'implication non triviale. Supposons que $\exists \bar{x}\ \phi(\bar{x},\bar{k})$ soit vraie dans K' . En passant aux clôtures p-adiques on peut supposer, comme pour CAC , que deg tr $K'/K = 1$. On a deux cas :

(1) $\underline{\text{val } K' = \text{val } K}$: soit $b \in K' \backslash K$. Alors b est transcendant sur K et K' est la clôture p-adique de $K(b)$. Soit

$$\Sigma = \text{CpC} + \Delta(K,v) + \{t \neq k : k \in K\}$$
$$+ \{v(t-k_0) = v(k_1) : k_0,k_1 \in K \text{ et } v(b-k_0)=v(k_1)\}$$

on montre que

$$\Sigma \vdash \exists \bar{x}\ \phi(\bar{x},\bar{k})$$

où $\Delta(K,v)$ est le diagramme de (K,v) dans $L(V)$ dans le sens évident (cf. l'exemple CAC), et où on laisse le soin au lecteur de traduire les égalités $v(t-k_0)=v(k_1)$ dans $L(V)$. En effet, soit $(K'',v) \supset (K,v)$ un modèle de Σ , $t \in K'' \backslash K$ satisfaisant les conditions données. Alors les résultats de Kaplansky sur les suites pseudo-convergentes d'Ostrowski disent précisément que (K,v) n'admettant aucune extension algébrique immédiate propre, les conditions $v(b-k_0)=v(k_1)$ déterminent $(K(b),v)$ à K-isomorphisme près. On a donc un K-isomorphisme de corps valués $f:K(t) \xrightarrow{\sim} K(b)$ t.q. $f(t)=b$. Soit $K(t)^{p-ad}$ la clôture p-adique de $K(t)$ dans K'' . En utilisant le fait que val $K(t)$=val K on montre comme en (2.5) que $(K(t)^{p-ad})^{\cdot n} \cap K(t) = (K')^{\cdot n} \cap K(b)$. D'où, par (2.5) , $K(t)^{p-ad} \simeq K'$ et donc $\exists \bar{x}\ \phi(\bar{x},\bar{k})$ est aussi vraie dans K'' .

Par le théorème de compacité, comme pour CAC , on se ramène à résoudre dans K un système

$$\begin{aligned} t &\neq k_i && i=1,\dots,n_0 \\ v(t-k_{j,0}) &= v(k_{j,1}) && j=1,\dots,n_1 \end{aligned}$$

sachant que b en est une solution dans K' . Des réductions comme dans [Ro] pour le cas des corps valués algébriquement clos, qu'on trouvera en appendice, nous ramènent à un système

$$v(y) = 0 \quad , \quad v(y-c_i) = 0 \qquad \text{où } c_i \in K \text{ et } v(c_i)=0 \ .$$

Mais ce système n'est rien d'autre que $y \neq 0$, $y \neq c_i$ dans le corps des restes res K = res K' = $\mathbb{F}_p$ ce qui nous assure qu'il y a une solution dans K .

(2) val K $\subsetneq$ val K' : soit $b \in K'$ t.q. $v(b) \in$ val K'\val K . Notons que n.val K=n.val K'∩val K , n=2,3... . On considère cette fois

$$\begin{aligned} \Sigma = \ & CpC + \Delta(K,v) + \{t \neq k : k \in K\} \\ & + \{v(k_0) < v(t) < v(k_1) : k_i \in K \ , \ v(k_0)<v(b)<v(k_1)\} \\ & + \{P_n(e_n t) : e_n \in N \quad e_n b \in (K')^{\cdot n} \ , \ n=2,3\dots\} \ . \end{aligned}$$

Comme précédemment, en suivant encore de plus près (2.5), on montre que $\Sigma \models \exists \overline{x}\ \phi(\overline{x},\overline{k})$ (N.B. $v(\Sigma\ k_i b^i) = \min v(k_i b^i)$ par hypothèse sur b et la remarque ci-dessus). Par le théorème de compacité on se ramène à résoudre dans K :

$$\begin{aligned} t &\neq k_i && ,i= ,\dots,\ell \\ \delta < v(t) &< \gamma && , \text{ en passant au min. et au max., } \delta,\gamma \in \text{val K} \\ & P_n(e_n t) && , \text{ en passant au p.p.c.m.} \end{aligned}$$

en sachant que b est une solution dans K' . On a $\lambda p^{-r} b = y'^n$ pour quelque y' dans K' et λ,r comme en (2.2). On en déduit que $e_n \ell p^r \in (K')^{\cdot n}$, $\ell=\lambda^{-1}$, d'où $e_n \ell p^r \in K'^{\cdot n}$, et que $\delta - r.v(p) < n.v(y') < \gamma - r.v(p)$. Soit $\delta - r.v(p) = n.\beta + s.v(p)$ où $\beta \in$ val K et $0 \leq s < n$, et soit $y \in K$ t.q. $v(y) = \beta + v(p)$. Alors $e_n \ell p^r y^n \in K^{\cdot n}$

et $\delta < v(p^r y^n) < \gamma$. Comme K possède une infinité d'éléments ayant même valuation on peut choisir y tel qu'on ait aussi $\ell p^r y^n \neq k_i$ et alors $\ell p^r y^n$ est une solution dans K . □

APPENDICE

I. Réduction du système dans (2.6)

On a le système

$$(\S) \qquad t \neq k_i \ , \ v(t-k_j) = \gamma_j \qquad \text{où } k_i \in K \ , \ \gamma_j \in \text{val } K$$

à résoudre dans K en sachant que b en est une solution dans K' et que val K est égal à val K' . On remplace d'abord $t \neq k_i$ par $v(t-k_i)=\gamma_i$ où $\gamma_i = v(b-k_i)$ qui appartient à val K . On a maintenant

$$(\S') \qquad v(t-k_j) = \gamma_j \qquad j=1,\ldots,\ell \ .$$

Si $k_i=k_j$ pour $i \neq j$ alors $\gamma_i=\gamma_j$. On peut donc supposer que $k_i \neq k_j$ pour $i \neq j$. D'autre part si $\gamma_i \neq \gamma_j$ alors $v(k_i-k_j)=\min(\gamma_i,\gamma_j)$. D'où par exemple si $\gamma_i<\gamma_j$ alors on peut omettre $v(t-k_i)=\gamma_i$ puisque $v(x-k_j)=\gamma_j$ implique $v(x-k_i)=\gamma_i$. En répétant ce processus on se réduit à un nouveau système

$$(\S'') \qquad v(t-k_j) = \gamma \qquad j= \ ,\ldots,m \ .$$

Par ailleurs si $v(k_1-k_j) \neq \gamma$ alors $v(b-k_j)=\min(\gamma, v(k_1-k_j))$ et par le même genre d'argument que précédemment on peut omettre de tels k_j du système. On peut donc supposer que $v(k_1-k_j)=\gamma$, $j=1,\ldots,m$. Soit $k \in K$ t.q. $v(k)=\gamma$. Posons $y=(t-k_1)/k$ et $c_j=(k_j-k_1)/k$. Alors ($\S''$) devient $v(y) = 0$, $v(y-c_j) = 0$ où $v(c_j)=0$, et si y est une solution alors $t=ky+k_1$ est une solution de ($\S''$) .

II. Démonstration de la Proposition 1 .

On travaille dans les langages $L, L(V), L(V,P_n)$ plus des constantes, et avec une théorie T dont les modèles sont des corps et où P_n est bien formé des puissances n-ièmes. Si T admet EQ alors la condition est satisfaite car il existe une formule sans quantificateur $\psi(\bar{y})$ équivalente à $\exists\bar{x}\ \phi(\bar{x},\bar{y})$ dans K_1, K_2 et la véracité de $\psi(\bar{a})$ ne dépend que de la sous-stucture A seule. On vérifie ce dernier point directement sur les formules de base et facilement sur les formules sans quantificateur. Réciproquement, soit T satisfaisant la condition et $\phi(\bar{x},\bar{y})$ une formule sans quantificateur. Considérons l'ensemble X des formules sans quantificateur $\psi(\bar{y})$ t.q. $T \models \forall\bar{y}(\exists\bar{x}\ \phi(\bar{x},\bar{y}) \rightarrow \psi(\bar{y}))$. On montre que $T + \{\psi(\bar{a}) : \psi\in X\} \models \exists\bar{x}\ \phi(\bar{x},\bar{a})$ dans le langage où on ajoute des constantes $\bar{a}=a_1,\ldots,a_m$. Dans ce cas le théorème de compacité implique qu'il suffit d'un nombre fini $\psi_1,\ldots,\psi_n$ de ψ_i dans X d'où $T \models \forall\bar{y}(\psi_1(\bar{y})\wedge\ldots\wedge\psi_n(\bar{y}) \rightarrow \exists\bar{x}\ \phi(\bar{x},\bar{y}))$ et puisque les $\psi_i\in X$ on a en fait $\leftrightarrow$ à la place de $\rightarrow$ et le tour est joué. Soit donc K un modèle de $T+\{\psi(\bar{a}):\psi\in X\}$ et $\bar{a}=a_1,\ldots,a_m\in K$. Soit A le sous-corps engendré par les a_i qui est de la façon évidente une sous-structure de K . Montrons que la théorie $T+\Delta(A)+\exists\bar{x}\ \phi(\bar{x},\bar{a})$ possède un modèle. En effet si tel est le cas on aura un autre modèle K' de T ayant A comme sous-structure et où $\exists\bar{x}\ \phi(\bar{x},\bar{a})$ est vrai. Par hypothèse $\exists\bar{x}\ \phi(\bar{x},\bar{a})$ devra donc aussi être vrai dans K (dans $L(V,P_n)$ on met aussi dans $\Delta(A)$ les $P_n(a)$ pour les $a\in K^{\cdot n}$) . Par le théorème de compacité il suffit de montrer que tout sous-ensemble fini de $T+\Delta(A)+\exists\bar{x}\ \phi(\bar{x},\bar{a})$ possède un modèle. Or une partie finie de $\Delta(A)$ est équivalente, en prenant la conjonction de tous ses membres, à une formule sans quantificateur $\psi(\bar{a})$. Puisque $\psi(\bar{a})$ est vrai dans K alors $\sim\psi(\bar{a}) \notin X$ d'où on conclut que $T+\psi(\bar{a})+\exists\bar{x}\ \phi(\bar{x},\bar{a})$ a un modèle . □

BIBLIOGRAPHIE

[A-K] J.Ax et S.Kochen. Diophantine Problems over Local Fields.II., Amer.Jour.Math. 87 (1965) , pp.631-648.

_____. Diophantine Problems over Local Fields.III, Annals of Math. 83 (1966) , pp.437-456.

[B] L.Bélair. Topics in the Model Theory of p-Adic Fields and Spectra, thèse, Yale, 1985.

[B-S] L.Bröcker et J.H.Schinke. On the L-Adic Spectrum, pré-publication, 1985.

[C-R] M.Coste et M.-F.Coste-Roy. La topologie du spectre réel,dans Ordered Fields & Real Algebraic Geometry, Contemporary Math. Vol.8, AMS, 1982.

[D] J.Denef. The Rationality of the Poincaré Series Associated to the p-Adic Points on a Variety, Inventiones Math. 77 (1984), pp.1-23.

[D1] _____. p-Adic Semi-Algebraic Sets and Cell Decompositions,pré-publication.

[D2] _____. On the Evaluation of Certain p-Adic Integrals, PM Séminaire de théorie des nombres, Paris 1983-84.

[Ek] P.Eklof. Ultraproducts for Algebraists, dans Handbook of Math. Logic éd. par J.Barwise, North Holland, 1977.

[E] Y.Ershov. On Elementary Theories of Local Fields, Algebra i Logika 4 (1965) No.2, pp.5-30.

[M] A.Macintyre. On Definable Subsets of p-Adic Fields, Jour.Symb.Logic 41 (1976) No.3, pp.605-610.

[P-R] A.Prestel et P.Roquette. Formally p-Adic Fields, LNM 1050, Springer, 1984.

[Ri] P.Ribenboim. Théorie des valuations, Presses de l'U. de Montréal, 1964.

[Ro] A.Robinson. Complete Theories, North Holland, 1956.

[R] E.P.Robinson. Affine Schemes and p-Adic Geometry, thèse, Cambridge, 1983.

_____. The p-Adic Spectrum, Jour. Pure & Appl. Alg. 40 (1986) No.3.

[S] J.H.Schinke. Das (p,d)-adische Spektrum, thèse, Münster, 1985.

[W] V.Weispfenning. Quantifier Elimination and Decision Procedure for Valued Fields, dans Logic Colloquium, Aachen 1983, LNM, Springer, 1986.

BÉLAIR Luc
Université PARIS 7 - CNRS
Equipe de logique mathématique
Tour 45-55, 5ème étage
2 Place Jussieu
75251 PARIS CEDEX 05