Ann. sc. math. Québec, **14** (2), 1990, 109–120.

LE THÉORÈME DE MACINTYRE UN THÉORÈME DE CHEVALLEY p-ADIQUE

LUC BÉLAIR

RÉSUMÉ. Nous exposons une démonstration du théorème de A. Macintyre sur la structure des ensemble algébriquement définissables dans les corps p-adiques en illustrant des techniques élémentaires de théorie des modèles.

ABSTRACT. We illustrate elementary methods from model theory through a proof of A. Macintyre's theorem on the structure of algebraically definable subsets of p-adic space.

0. Introduction. Dans un article de 1976 (voir [**M1**]) A. Macintyre démontre un théorème sur la structure des sous-ensembles algébriquement définissables de l'espace p-adique $\mathbb{Q}_p^n$, où $\mathbb{Q}_p$ est le corps des nombres p-adiques, p premier (voir 1). Ces ensembles sont construits à partir d'ensembles du type $\{x \in \mathbb{Q}_p^n \mid f(x) = 0\}$, où $f(X_1, \ldots, X_n)$ est un polynôme, par un nombre fini d'opérations booléennes (union, intersection, complémentaire) et projections ($\mathbb{Q}_p^{m+n} \to \mathbb{Q}_p^n$) successives. La preuve repose sur un critère de théorie des modèles et le travail de Ax-Kochen [**AK**]. Macintyre en tire plusieurs conséquences qui tendent à montrer que ce résultat se rapproche davantage du théorème analogue de Tarski (ou Tarski-Seidenberg) pour les nombres réels $\mathbb{R}$, qu'un résultat du même type pour $\mathbb{Q}_p$ déjà connu depuis Ax-Kochen. Le théorème de Tarski dit que dans le cas réel les ensembles en question sont des combinaisons booléennes d'ensembles de type $\{x \in \mathbb{R}^n \mid f(x) \geq 0\}$. Avec les travaux de Denef en 1984 [**D1**], le théorème de Macintyre a attiré l'attention des théoriciens des nombres. En effet, Denef l'utilise pour évaluer certaines intégrales p-adiques et montrer la rationalité de séries de Poincaré p-adiques (voir 1). Avec des raffinements, il réussit même à le faire de façon "élémentaire" (voir [**D1**]).

Le but de cet article est d'exposer une démonstration "algébrique" (voir 2) du théorème de Macintyre en illustrant des techniques élémentaires de la théorie des modèles. Seule la démonstration de la proposition 4.5 est originale (et reléguée en appendice). Nous renvoyons à l'exposé [**M2**] pour plus de détails sur ce théorème, ses conséquences, et l'analogie avec $\mathbb{R}$.

Le paragraphe 1 est une introduction aux corps p-adiques. On y donne aussi la terminologie des corps valués utilisée dans le paragraphe 4. Le théorème est énoncé de façon précise au paragraphe 2, et on le met en parallèle avec un théorème de C. Chevalley en géométrie algébrique élémentaire. Dans le paragraphe 3 nous illustrons les principes de notre démonstration en donnant une preuve du théorème de Chevalley. La démonstration du théorème de Macintyre fait l'objet du paragraphe 4. Là où elle n'est pas explicitée, notre notation est standard ($\mathbb{Z}$ pour les entiers, etc.).

Reçu le 3 février 1989.

Cet article est une version remaniée d'un exposé donné au Séminaire du Groupe d'Étude d'Analyse ultranumérique, Paris, 13^e année (1985–86).

1. Les nombres p-adiques. Soit p un nombre premier. Les nombres p-adiques sont la création de K. Hensel (voir [**Ha**]). On peut les voir apparaître dans l'étude des congruences. Soit $f \in \mathbf{Z}[X_1, \ldots, X_n]$, un polynôme à coefficients entiers, alors l'équation $f(X_1, \ldots, X_n) = 0$ possède une solution dans les "entiers p-adiques" si et seulement si elle en possède une dans les entiers modulo p^k pour tout $k \geq 1$. Si on s'intéresse aux équations dans tous les $\mathbf{Z}/(p^k)$ à la fois, il est naturel de remplacer cet anneau de caractéristique non nulle et contenant des éléments nilpotents par l'anneau intègre de caractéristique zéro des entiers p-adiques, noté $\mathbf{Z}_p$. On passe ensuite au corps des fractions de $\mathbf{Z}_p$ qui constitue le corps des nombres p-adiques, $\mathbf{Q}_p$. Ces corps revêtent leur plus grande importance dans l'idée de passage du "local" au "global": l'existence d'une solution dans tous les $\mathbf{Q}_p$ (local) assurerait l'existence d'une solution dans $\mathbf{Q}$ (global). Il en est rarement ainsi, mais si on exige aussi l'existence d'une solution dans $\mathbf{R}$ alors ce principe est vrai, par exemple, dans le cas des formes quadratiques (voir par exemple [**Se**]). Mesurer l'inexactitude de ce principe "local-global" constitue un thème important de la théorie de nombres.

On peut construire $\mathbf{Q}_p$ de plusieurs façons. Considérons l'anneau formé des sommes infinies $a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots$, où $a_i \in \mathbf{Z}$, $0 \leq a_i < p$, et où on additionne et on multiplie de la façon naturelle en base p. C'est un anneau unitaire commutatif intègre de caractéristique zéro, c'est l'*anneau des entiers p-adiques* $\mathbf{Z}_p$. Notons que chaque entier 1, 2, 3, 4, ... peut s'écrire comme une telle somme finie; par contre $-1 = (p-1) + (p-1)p + \cdots + (p-1)p^n + \cdots$. On vérifie, par exemple, que $1 - p$ est inversible dans $\mathbf{Z}_p$, à savoir $(1-p)^{-1} = 1 + p + p^2 + p^3 + \cdots + p^n + \cdots$. Le *corps des nombres p-adiques*, $\mathbf{Q}_p$, est le corps des fractions de $\mathbf{Z}_p$. On voit que l'anneau quotient $\mathbf{Z}_p/(p^k)$ est canoniquement isomorphe à $\mathbf{Z}/(p^k)$. En particulier $\mathbf{Z}_p/(p)$ est canoniquement isomorphe à $\mathbf{F}_p$, le corps fini à p éléments, et l'idéal engendré par p, (p), est donc maximal. On peut définir l'application $v_p \colon \mathbf{Z}_p \setminus \{0\} \to \mathbf{Z}$, à savoir pour $a = a_0 + a_1 p + \cdots$, $v_p(a) = \min\{n \in \mathbf{N} \mid a_n \neq 0\}$, et elle se prolonge naturellement à $\mathbf{Q}_p \setminus \{0\}$: pour $x = ab^{-1}$, $a, b \in \mathbf{Z}_p$, $v_p(x) = v_p(a) - v_p(b)$. Pour $a \in \mathbf{Z}_p$, $v_p(a)$ est la plus grande puissance de p dans la décomposition de a en facteurs premiers. L'application v_p a les propriétés suivantes:

(A1) $v_p(1) = 0$;
(A2) $v_p(xy) = v_p(x) + v_p(y)$;
(A3) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

On peut l'utiliser pour définir une norme $|\ |_p$ sur $\mathbf{Q}_p$, à savoir $|x|_p = p^{-v_p(x)}$, et montrer que $(\mathbf{Q}_p, |\ |_p)$ est le complété de $\mathbf{Q}$ pour cette norme. L'anneau $\mathbf{Z}_p$ est aussi la limite projective du système d'applications naturelles $\mathbf{Z}/(p^n) \to \mathbf{Z}/(p^m)$, $n \geq m$, $n, m \in \mathbf{N}$.

Soit $f_1, \ldots, f_r \in \mathbf{Z}_p[X_1, \ldots, X_n]$, $\widetilde{N}_m$ le nombre de solutions $(x_1, \ldots, x_n)$, $x_i \in \mathbf{Z}_p/(p^m)$ du système $f_1(X_1, \ldots, X_n) = 0, \ldots, f_r(X_1, \ldots, X_n) = 0$ dans $\mathbf{Z}_p/(p^m)$ et N_m le nombre de telles solutions qui proviennent de solutions $(y_1, \ldots, y_n)$, $y_i \in \mathbf{Z}_p$, dans $\mathbf{Z}_p$. Soit les séries formelles $\widetilde{P}(T) = \sum \widetilde{N}_m T^m$, et $P(T) = \sum N_m T^m$. Borewicz et Shafarevic avait conjecturé que $\widetilde{P}(T)$ était une fonction rationnelle, ce qui fut établi par Igusa et Meuser, et Denef a montré que $P(T)$ est aussi une fonction rationnelle, en réponse à une question de Serre et Oesterlé (voir [**D1**]).

Au paragraphe 4, nous allons considérer $\mathbf{Q}_p$ comme corps valué (voir [**Ri**]). Soit un corps K, on pose $K^\bullet = K \setminus \{0\}$. La notion de corps valué est axiomatisée par les propriétés A1, A2, A3 ci-dessus pour un corps K muni d'une application v surjective de $K^\bullet$ dans un groupe abélien ordonné (pas nécessairement $\mathbf{Z}$). On dit que v est une *valuation* sur K et que (K, v) est un *corps valué*. L'image de $K^\bullet$ par v, noté $\operatorname{val} K$, est appelé le *groupe de valuation* de (K, v). Par exemple, le corps des fractions rationnelles complexes $\mathbf{C}(T)$ (ou celui des fonctions méromorphes autour de 0) possède une valuation naturelle, à savoir

l'application qui donne l'ordre de 0 comme zéro ou pôle de la fonction. Il est bien connu que la notion de valuation au sens ci-dessus est essentiellement équivalente à celle d'anneau de valuation. Un sous-anneau V d'un corps K est dit *anneau de valuation* de K si pour tout $x \in K$, $x \in V$ ou $x^{-1} \in V$. L'anneau de valuation correspondant à (K, v) est $V_{(K,v)} = \{x \in K \mid v(x) \geq 0\}$ (où 0 est l'élément neutre du groupe de valuation). À partir d'un anneau de valuation V on récupère une valuation en considérant l'application canonique $K^\bullet \to K^\bullet/U$, où U est le groupe multiplicatif des éléments de V qui sont inversibles dans V (*i.e.* $x \in V$ et $x^{-1} \in V$). Dans un anneau de valuation V, les éléments non inversibles forment un idéal M, nécessairement maximal, et l'anneau quotient V/M est appelé le *corps des restes*. Le corps des restes de (K, v) est noté $\operatorname{res} K$. Pour $(\mathbb{Q}_p, v_p)$, ces notions se traduisent ainsi: l'anneau de valuation de $(\mathbb{Q}_p, v_p)$ est précisement $\mathbb{Z}_p$, son corps des restes est $\mathbb{F}_p$, et son groupe de valuation est $(\mathbb{Z}, +, 0, \leq)$. On utilisera l'abus de notation V_K pour désigner l'anneau de valuation de (K, v).

On dit que $(K, v) \subset (E, w)$ est une *extension de corps valués* si $K \subset E$ et v est la restriction de w à K, ou en termes d'anneau de valuation si $V_K = V_E \cap K$. Une extension de corps valués induit naturellement des inclusions au niveau des corps des restes et des groupes de valuation. Le degré de l'extension de corps $\operatorname{res} E / \operatorname{res} K$ est appelé *degré résiduel*, et l'indice de $\operatorname{val} K$ dans $\operatorname{val} E$ est appelé *indice de ramification*. On dit qu'une extension est *immédiate* si le degré résiduel et l'indice de ramification sont tous deux 1, *i.e.* si le corps résiduel et le groupe de valuation n'augmentent pas. En rapport avec l'étude des congruences mentionnée au tout début, mentionnons l'important.

LEMME DE HENSEL. *Soit $f \in \mathbb{Z}_p[X]$ (en particulier $f \in \mathbb{Z}[X]$). Si f possède une racine simple dans $\mathbb{Z}_p/(p)$ ($\simeq \mathbb{F}_p$), alors f possède une racine $a \in \mathbb{Z}_p$ qui est envoyée sur α par l'application canonique $\mathbb{Z}_p \to \mathbb{Z}_p/(p)$.*

Le lemme de Hensel se démontre par la méthode des tangentes de Newton, qui ici est sûre de converger. On dit qu'un corps valué (K, v) est *hensélien*, ou satisfait le lemme de Hensel, si l'énoncé ci-dessus est valide en remplaçant $\mathbb{Z}_p$ par V_K, et $\mathbb{Z}_p/(p)$ par $\operatorname{res} K$. Tout corps valué (K, v) peut être plongé (en tant que corps valué, dans une "clôture hensélienne", appelée son *hensélisé*, qui est lui-même un corps valué hensélien et qui se plonge (de façon unique) au-dessus de (K, v) dans tout corps valué hensélien qui est une extension de (K, v). Par exemple, le corps des séries de Laurent qui sont algébriques sur $\mathbb{C}(T)$ constitue le hensélisé de $\mathbb{C}(T)$ pour la valuation décrite ci-dessus. Une version plus utile, mais équivalente, du lemme de Hensel est la suivante.

LEMME DE HENSEL (VERSION NEWTON). *Soit (K, v) un corps valué, $f \in V_K[X]$, $a \in V_K$, tel que $v(f(a)) > 2v(f'(a))$ (f' est la dérivée formelle de f). Alors il existe $b \in V_K$ tel que $f(b) = 0$ et $v(b - a) > 2v(f'(a))$.*

Elle permet de calculer une borne qui détermine jusqu'à quel $\mathbb{Z}_p/(p^m)$ il suffit de chercher une solution de $f(X) = 0$. Par exemple, pour $p = 2$ et $b \in \mathbb{Z}_p$, $X^2 - b = 0$ a une solution dans $\mathbb{Z}_p$ si et seulement s'il y en a une modulo $p^{v_p(b)+3}$.

2. Un théorème de Chevalley p-adique. Considérons trois types de sous-ensemble de l'espace p-adique, que nous appelllerons *ensembles de bases.*

ENSEMBLES DE BASE.

I. $\{x \in \mathbb{Q}_p^m \mid f(x) = 0\}$
II. $\{x \in \mathbb{Q}_p^m \mid \text{il existe } y \in \mathbb{Q}_p \text{ tel que } f(x) = y^n\}$
III. $\{x \in \mathbb{Q}_p^m \mid v_p(g(x)) \leq v_p(f(x))\}$

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

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, III. Un ensemble *définissable* est un ensemble obtenu par un nombre fini de projections et de complémentaires de projections à partir de tels ensembles S. Ainsi $\{x \in \mathbb{Q}_p^m \mid \exists y \in \mathbb{Q}_p^k, (x,y) \in S\}$ est l'ensemble obtenu de $S \subset \mathbb{Q}_p^{m+k}$ par la projection $\mathbb{Q}_p^{m+k} \to \mathbb{Q}_p^m$. Les entiers p-adiques forment un ensemble définissable qui est en fait de type II, $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \exists y \in \mathbb{Q}_p, 1 - p^3x^4 = y^2\}$. Le théorème de Macintyre donne la structure des ensembles définissables comme combinaisons booléennes d'ensembles de base.

THÉORÈME DE MACINTYRE. *Soit $S \subset \mathbb{Q}_p^{m+k}$ une combinaison booléenne d'ensembles de base, alors l'image de S par la projection $\mathbb{Q}_p^{m+k} \to \mathbb{Q}_p^m$ est aussi une combinaison booléenne d'ensembles de base.*

Il faut noter que la description de $\mathbb{Z}_p$ comme ensemble de type II fait en sorte que les ensembles de type III sont aussi de type II. En effet, on a $v(x) \leq v(y)$ ssi, $x = y = 0$ ou $x \neq 0$ et $0 \leq v(yx^{-1})$, ssi $x = y = 0$ ou $x \neq 0$ et il existe $z \in \mathbb{Q}_p$ tel que $1 + p^3(yx^{-1})^4 = z^2$, ssi $x = y = 0$ ou $x \neq 0$ et il existe $t \in \mathbb{Q}_p$ tel que $x^4 + p^3y^4 = t^2$, ssi il existe $t \in \mathbb{Q}_p$ tel que $x^4 + p^3y^4 = t^2$. Ainsi le théorème de Macintyre s'énonce aussi en termes des ensembles de base de type I, II. Il est commode d'avoir les ensembles de type III puisqu'ils décrivent explicitement la topologie p-adique et la structure de corps valué.

Nous présentons dans 4 une démonstration du théorème de Macintyre qui fait appel à la théorie des modèles à la Abraham Robinson. Il existe maintenant des preuves élémentaires (voir [**We**], [**D3**]) et et les ensembles définissables sont étudiés de façon plus précises dans [**D1**], [**D2**], [**DV**]. La théorie des modèles fournit cependant une démonstration qui compense son caractère non constructif en étant plus conceptuelle. Notre démonstration s'apparente à démontrer le théorème des zéros de Hilbert en remplaçant la théorie de l'élimination classique par celles des idéaux de polynômes. Le théorème de Macintyre a été généralisé aux extensions finies de $\mathbb{Q}_p$ dans [**PR**] et la preuve ci-dessous peut être ajustée en conséquence (Il apparaîtra clairement au spécialiste que les arguments utilisés ici sont essentiellement équivalents aux arguments de saturation utilisés dans [**M1**] ou [**PR**]).

Le théorème de Chevalley auquel nous faisons allusion est le suivant. On considère les sous-ensembles de base de type I de $\mathbb{C}^m$ définis par des polynômes $f(X_1, \ldots, X_m)$ à coefficients complexes. Les géomètres appellent une intersection finie de tels ensembles un *ensemble algébrique* et une combinaison booléenne de tels ensembles, un *ensemble constructible.*

THÉORÈME DE CHEVALLEY. *La projection d'un ensemble constructible est un ensemble constructible, i.e. soit $S \subset \mathbb{C}^{m+k}$ une combinaison booléenne d'ensemble de base de type I sur $\mathbb{C}$, alors l'image de S par la projection $\mathbb{C}^{m+k} \to \mathbb{C}^m$ est aussi une combinaison booléenne d'ensembles de base de type I, sur $\mathbb{C}$.*

Le théorème de Macintyre peut donc être interprété en termes d'ensembles "constructibles p-adiques", à savoir les ensembles S.

Pour illustrer notre méthode, nous allons d'abord donner une preuve du théorème de Chevalley qui fait appel à la théorie des modèles.

3. Éléments de théorie des modèles. On peut exprimer le théorème de Macintyre en termes logiques. À tout ensemble $S \subset \mathbb{Q}_p^m$ comme ci-dessus on associe la formule $\phi_S(\overline{x})$ qui décrit S *i.e.* les conditions qui définissent S même, où $\overline{x}$ désigne la multivariable $(x_1, \ldots, x_n)$.

EXEMPLE 3.1. Soit $f, g, h \in \mathbb{Q}_p[X_1, \ldots, X_n]$, alors à

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

on associe

$$\phi_s(\overline{x}) := \left(f(\overline{x}) \neq 0 \wedge (v_p(1) \leq v_p(g(\overline{x})^{-1})\right) \vee \exists y(y^n = h(\overline{x})).$$

Notons que ϕ_s ne contient pas de quantificateurs $\exists$, $\forall$ sauf ceux provenant de la description d'ensembles de type II. 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 $\psi(\overline{y})$ sans quantificateur sauf ceux provenant de la description d'ensembles de type II, telle que dans $\mathbb{Q}_p$ on ait $\exists \overline{x}\, \phi(\overline{x}, \overline{y})$ ssi $\psi(\overline{y})$.*

Le théorème nous dit donc que dans $\mathbb{Q}_p$, on peut éliminer les quantificateurs existentiels, *i.e.* calculer les projections $\mathbb{Q}_p^{m+k} \to \mathbb{Q}_p^m$, aux dépens des seuls quantificateurs provenant des formules $\exists y(h(\overline{x}) = y^n)$, *i.e.* des projections d'ensembles $\{(x, y) \in \mathbb{Q}_p^{m+1} \mid h(x)^n = y\}$ dans $\mathbb{Q}_p^m$. 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 dans un langage approprié. On adopte d'abord un langage de premier ordre pour les corps, L, qui contient les symboles habituels $+$, $-$, $\cdot$, $^{-1}$, 0, 1, des variables x, y, z, ... qui prennent leurs valeurs sur les *éléments* des corps en question, ainsi que les signes logiques standard $\wedge$, $\vee$, $\neg$ ("non"), $\to$, $\leftrightarrow$ et les quantificateurs $\exists$, $\forall$ sur les variables. On s'intéresse à $\mathbb{Q}_p$ en tant que corps valué avec la valuation p-adique. On introduit donc un langage des corps valués $L(V)$ en ajoutant à L un symbole V, ou $V(x)$, 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. Notons qu'on interprète éventuellement $\to$ et $\leftrightarrow$ à l'aide de $\wedge$, $\vee$, $\neg$ par les équivalences standard.

DÉFINITION 3.2. Soit $f, g \in \mathbb{Z}[X_1, \ldots, X_m]$, $m \in \mathbb{N}$.

(1) Les *formules de base de L*: ce sont les $(f(\overline{x}) = 0)$.
(2) Les *formules de base de $L(V)$*: on ajoute les $V(f(\overline{x}) \cdot g(\overline{x})^{-1})$.
(3) Les *formules* de L, $L(V)$: La plus petite classe contenant les formules de base et close par rapport à $\wedge$, $\vee$, $\neg$, $\exists$, $\forall$.
(4) Les *formules sans quantificateur* de L, $L(V)$: cette fois-ci on clôt par rapport à $\wedge$, $\vee$, $\neg$ seulement. Les formules sans quantificateur sont donc les "combinaisons booléennes" de formules de base. Par exemple, pour les corps, toute formule sans quantificateur de L est équivalente à une disjonction de formules du type $f_1(\overline{x}) = 0 \wedge \cdots \wedge f_r(\overline{x}) \wedge \neg(g(\overline{x}) = 0)$.
(5) Un *énoncé σ*: c'est une formule où toutes les variables sont quantifiées. Par exemple $\exists \overline{x}(f(\overline{x}) = 0)$. Dans L, la classe des corps algébriquement clos est axiomatisée par l'ensemble d'énoncés CAC, à savoir CAC = axiomes de corps + $\{\forall \overline{y} \exists x(f_n(x, \overline{y}) = 0) \mid n \in \mathbb{N}\}$, où $f_n(X, Y_1, \ldots, Y_n)$ est le polynôme générique unitaire de degré n dont les coefficients sont les Y_i. Dans un corps donné on interprète les formules de la façon évidente et on dit qu'un corps K est un *modèle* d'un ensemble T d'énoncés si tout énoncé de T est vrai dans K.
(6) Soit T un ensemble d'énoncés. On écrit $T \models \sigma$, si σ est vrai dans tout modèle de T. Par exemple dans L, soit $T = \text{CAC}$ et $\sigma_{100} := \exists x_1 \ldots x_{100} \left(\bigwedge_{i \neq j} \neg(x_i = x_j)\right)$, alors $T \models \sigma_{100}$ puisque tout corps algébriquement clos est infini.

Toutes ces notions de formules etc. sont définies relativement à un langage donné, ici L, $L(V)$ ou $L(V, P_n)$ (voir ci-dessous), auquel on ajoutera à l'occasion des constantes pour

pouvoir parler des extensions d'un corps donné. Un théorème fondamental de la théorie des modèles est le théorème de compacité. C'est le seul résultat de théorie des modèles que nous allons utiliser. Nous renvoyons à [**Ek**] pour une preuve.

THÉORÈME DE COMPACITÉ. *Soit T un ensemble d'énoncés, et σ un énoncé. Si $T \models \sigma$, alors 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 plus petit ou égal à cent admet une racine, ce qui est bien donné par un sous-ensemble fini de CAC. Notons que la réciproque du théorème de compacité est immédiate. Pour poursuivre notre analogie avec l'algèbre et le théorème de Chevalley, le théorème de compacité est, dans le cas qui nous occupe, du même ordre que la proposition affirmant que tout idéal (propre) de polynômes sur un corps est contenu dans un idéal premier. La forme contraposée avec $\sigma := \forall x \neg(x = x)$ est d'ailleurs plus suggestive sur ce point: un ensemble d'énoncés admet un modèle 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 d'un corps détermine une valuation sur ce corps de façon essentiellement unique et qu'on peut décrire (dans $L(V)$) les équations algébriques et la relation d'ordre du groupe de valuation et les équations algébriques du corps des restes 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 v. Nous introduisons maintenant la classe des corps valués associés à $\mathbb{Q}_p$.

DÉFINITION 3.3. Un *corps p-adiquement clos* est un modèle de l'ensemble d'énoncés CpC qu'on obtient en traduisant dans $L(V)$ les propriétés suivantes de corps valué.

(1) (K, v) satisfait le lemme de Hensel et est de caractéristique zéro.
(2) 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

$$\forall \gamma \exists \delta (\gamma = n \cdot \delta + r \cdot v(p), \text{ pour un certain } 0 \leq r < n).$$

En particulier $(\mathbb{Q}_p, v_p)$ est un corps p-adiquement clos, de même que la clôture algébrique relative de $\mathbb{Q}$ dans $\mathbb{Q}_p$ avec la valuation induite par v_p. Par la suite on identifie CpC avec la classe des corps p-adiquement clos.

DÉFINITION 3.4. Soit T un ensemble d'énoncés d'un langage $\mathcal{L}$, et soit $\mathcal{K}$ la classe des modèles de T. On dit que la classe $\mathcal{K}$ *admet l'élimination des quantificateurs* si pour toute formule sans quantificateur $\psi(\overline{x}, \overline{y})$ de $\mathcal{L}$, il existe une formule sans quantificateur $\psi(\overline{y})$ telle que dans tout modèle $K \in \mathcal{K}$ on ait $\exists \overline{x} \phi(\overline{x}, \overline{y})$ ssi $\psi(\overline{y})$, *i.e.* $T \models \forall \overline{y}(\exists \overline{x} \phi(\overline{x}, \overline{y}) \leftrightarrow \psi(\overline{y}))$.

Un exemple familier de ce phénomène est le critère du discriminant pour l'existence de racines réelles d'un polynôme quadratique:

$$\exists x_1 x_2 (\neg(x_1 = x_2) \wedge a x_1^2 + b x_1 + c = 0 \wedge a x_2^2 + b x_2 + c = 0)$$

ssi $b^2 - 4ac > 0$. 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 II". Il ne reste plus qu'à éliminer formellement les quantificateurs dans les formules de type II en ajoutant de nouvelles formules de base $P_n(f(\overline{x}))$ et en les interprétant dans CpC comme

$\exists y(f(\overline{x}) = y^n)$. Plus précisément, on introduit le langage $L(V, P_n)$ obtenu en ajoutant à $L(V)$ un symbole P_n, ou $P_n(x)$, pour $n = 2, 3, \ldots$. On ajoute les $P_n(f(\overline{x}))$ aux formules de base et $P_n(x) \leftrightarrow \exists y(x = y^n)$ aux axiomes de CpC. On peut maintenant formuler le théorème de Macintyre de façon plus précise.

THÉORÈME DE MACINTYRE. La classe CpC admet l'élimination des quantificateurs dans le langage $L(V, P_n)$.

Cette forme plus forte du théorème entraîne clairement la forme précédente puisqu'elle dit qu'on peut éliminer les quantificateurs $\exists$ (et de proche en proche, tous les quantificateurs: $\forall \overline{x}\phi(\overline{x}) \leftrightarrow \neg\exists\overline{x}\neg\phi(\overline{x})$), *i.e.* les projections, uniformément dans la classe CpC. On a un critère de la théorie des modèles pour l'élimination des quantificateurs en termes de sous-structures. 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 $P_n^A = A \cap K^{\bullet n}$, où $K^{\bullet n}$ est le sous-groupe multiplicatif des puissances n-ièmes.

PROPOSITION 3.5. *Avec les mêmes notations que la définition précédente, la classe $\mathcal{K}$ admet l'élimination des quantificateurs si et seulement si pour toute paire de modèles K_1, $K_2 \in \mathcal{K}$, ayant une sous-structure commune A, pour toute formule sans quantificateur $\phi(\overline{x}, \overline{y})$, et pour tout $\overline{a} \in A$, la formule $\exists\overline{x}\phi(\overline{x}, \overline{a})$ est vraie dans K_1, si et seulement si elle l'est dans K_2.*

Si $\mathcal{K}$ admet l'élimination des quantificateurs, alors la condition est satisfaite car il existe une formule sans quantificateur $\psi(\overline{y})$ équivalente à $\exists\overline{x}\phi(\overline{x}, \overline{y})$ dans K_1, K_2 et la véracité de $\psi(\overline{a})$ ne dépend que de la sous-structure A seule. On vérifie ce dernier point directement sur les formules de base, et facilement sur les formules sans quantificateur. Une démonstration de la réciproque se trouve en appendice. Nous utiliserons la notion voisine de classe modèle-complète.

DÉFINITION 3.6. Toujours dans la même notation, on dit que $\mathcal{K}$ est *modèle-complète* si le critère énoncé dans la proposition précédente est valide lorsque A est un modèle $K \in \mathcal{K}$. Ce qui est donc équivalent à ce que, pour toute paire de modèles $K \subset K'$ où K est une sous-structure de K', pour toute formule $\phi(\overline{x}, \overline{y})$ sans quantificateur et tout $\overline{k} \in K$, on ait $\exists\overline{x}\phi(\overline{x}, \overline{k})$ vrai dans K si et seulement si ce l'est dans K'.

Il est clair que ces notions dépendent étroitement du langage dans lequel on travaille. Identifions l'ensemble d'énoncés CAC, de L, avec la classe des corps algébriquement clos.

EXEMPLE 3.7 [**Ro**]. Dans L, la classe CAC est modèle-complète. En effet, soit $K \subset K'$ algébriquement clos. Comme on l'a déjà remarqué une formule sans quantificateur $\phi(\overline{x}, \overline{y})$ de L, pour les corps, est équivalente à une disjonction de formules de la forme $f_1(\overline{x}, \overline{y}) = 0 \wedge \cdots \wedge f_r(\overline{x}, \overline{y}) = 0 \wedge g(\overline{x}, \overline{y}) \neq 0$, où f_i, $g \in \mathbb{Z}[\overline{X}, \overline{Y}]$. Ainsi, il suffit de vérifier qu'étant donné un système $(*)$

$$f_1(\overline{x}) = 0, \ \ldots, \ f_r(\overline{x}) = 0, \ g(\overline{x}) \neq 0, \qquad f_i, g \in K[\overline{X}] \tag{$*$}$$

le système $(*)$ a une solution dans K si et seulement si 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', où l'un des x_i n'est pas dans K. Considérons

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

où ^{a} désigne la clôture algébrique. Ceci nous donne une suite croissante de corps algébriquement clos K_j tel que $(*)$ a une solution dans le dernier corps de la suite, et le degré de transcendance de K_{j+1} sur K_j est 1. On peut donc supposer que le degré de transcendance de K' sur K est 1 puisque si on établit le résultat dans ce cas, alors, de proche en proche, $(*)$ aura une solution dans tous les K_j et donc dans K. Dans ce cas, $(*)$ a alors une solution dans toute extension algébriquement close propre de 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

$$\mathrm{CAC} + \Delta(K) + \{\neg(t = k) \mid k \in K\} \models \exists \overline{x} \phi(\overline{x}, \overline{k})$$

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.* tous les énoncés $k_1 + k_2 = k_3$, $k_1 \cdot k_2 = k_3$, $\neg(k_1 = k_2)$ qui sont vrais dans K. Il est clair qu'un modèle de $\Sigma = \mathrm{CAC} + \Delta(K) + \{\neg(t = k) \mid k \in K\}$ n'est rien d'autre qu'une extension $K \subset K''$ comme ci-dessus avec $t \in K'' \setminus K$. Par le théorème de compacité, il existe un sous-ensemble fini Σ' de Σ tel que $\Sigma' \models \exists \overline{x} \phi(\overline{x}, \overline{y})$, et donc en particulier on a

$$\mathrm{CAC} + \Delta(K) + \{\neg(t = k_1), \ldots \neg(t = k_n)\} \models \exists \overline{x} \phi(\overline{x}, \overline{k})$$

pour certains $k_i \in K$ en nombre fini. Mais K lui-même est un modèle de $\mathrm{CAC} + \Delta(K) + \{\neg(t = k_i) \mid i = 1, \ldots, n\}$, car K est infini. D'où, $\exists \overline{x} \phi(\overline{x}, \overline{k})$ est vrai dans K, *i.e.* $(*)$ a une solution dans K.

COROLLAIRE (TARSKI). La classe CAC admet l'élimination des quantificateurs dans L.

En effet, dans notre critère pour l'élimination des quantificateurs on pourra tester la véracité de la formule $\exists \overline{x} \phi(\overline{x}, \overline{a})$, $\overline{a} \in A$, dans la clôture algébrique de A dont les deux modèles possèdent des copies isomorphes au-dessus de A. Le corollaire est un théorème de Tarski et on voit qu'il est équivalent au théorème de Chevalley dont nous avons parlé (*cf.* les différentes versions du théorème de Macintyre).

Nous allons suivre ce schéma pour démontrer le théorème de Macintyre. Les ingrédients essentiels de la démonstration ci-dessus étaient

(1) l'existence et l'unicité de la clôture algébrique sur un corps de base,
(2) le fait que les conditions $\{t \neq k \mid k \in K\}$, pour K algébriquement clos, déterminent l'extension $K(t)$ à K-isomorphisme près.

En formulant une démonstration à la A. Robinson du théorème de Tarski pour le corps $\mathbb{R}$, le lecteur verrait apparaître:

(1) la notion de clôture réelle d'un corps ordonné,
(2) la détermination des ordres qui font du corps des fractions rationnelles $K(t)$ un corps ordonné, pour K un corps réel clos (voir [**Ro**]).

4 Démonstration du théorème. Nous allons d'abord voir qu'on a une "clôture p-adique". Soit R un anneau, alors $R^\bullet$ désigne le groupe multiplicatif des éléments inversibles et $R^{\bullet n}$ le sous-groupe des puissances n-ièmes, $n = 1, 2, \ldots$

PROPOSITION 4.1. *Soit $(E,v) \subset (K,v)$ une extension de corps valués, où $K \in CpC$ et E est relativement algébriquement clos dans K. Alors $E \in CpC$.*

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

LEMME 4.2. *Pour tout $n \geq 2$, $K^\bullet/K^{\bullet n} \simeq \mathbb{Q}_p^\bullet/\mathbb{Q}_p^{\bullet n}$, et on a un ensemble de représentants des translatés dans $\mathbb{N}$. Plus précisément, pour tout $x \in K^\bullet$, on a $\lambda p^r x \in K^{\bullet n}$ pour certains λ, $r \in \mathbb{N}$ tel que $0 \leq r < n$, $0 \leq \lambda < p^{B(n)}$, p ne divise pas λ et $B(n) = 2v_p(n)+1$.*

DÉMONSTRATION: Puisque val K est un $\mathbb{Z}$-groupe, il existe $y \in K$ et $0 \leq j < n$ tel que $v(x) = n \cdot v(y) + j \cdot v(p)$. Ainsi $v(xy^{-n}p^{-j}) = 0$, et donc $xp^{n-j} \equiv u \mod K^{\bullet n}$, où $v(u) = 0$. Or, par le lemme de Hensel, $u \in K^{\bullet n}$ ssi u "$\in$" $(V/(p^s))^{\bullet n} \simeq (\mathbb{Z}/(p^s))^{\bullet n}$, où $s = 2v_p(n)+1$. Il suffit donc de multiplier xp^{n-j} par un λ approprié qui donne l'inverse multiplicatif de u dans $(V/(p^s))^\bullet$. □

La proposition suivante est reprise de [**PR**, lemme 2.9]. La démonstration repose sur les éléments de la théorie des valuations.

PROPOSITION 4.3. *Soit $(K,v) \in CpC$, alors pour toute extension $(K,v) \subset (E,v)$ donnée par une extension finie $K \subset E$, le degré de E sur K est égal au produit de l'indice de ramification et du degré résiduel.*

En particulier, un corps p-adiquement clos n'admet aucune extension algébrique immédiate propre. Ceci fournit le lemme suivant.

LEMME 4.4. *Soit $(K,v) \subset (L,v)$, une extension de corps valués où $K, L \in CpC$, et $K \subset L$ est une extension algébrique. Alors $K = L$.*

DÉMONSTRATION: Comme val K et val L sont des $\mathbb{Z}$-groupes avec le même plus petit élément positif, on a $n \cdot \text{val}\, K = n \cdot \text{val}\, L \cap \text{val}\, K$ pour tout entier n. Or, que l'extension soit algébrique entraîne que chaque élément du groupe quotient val L/ val K est d'ordre fini. Il s'ensuit que val L = val K, l'extension est immédiate, et $L = K$. □

On a donc une clôture pour un sous-corps valué d'un corps p-adiquement clos: sa clôture algébrique relative. Cependant, cette clôture n'est en général pas unique (à isomorphisme près) 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. Une démonstration est donnée en appendice,

PROPOSITION 4.5 (UNICITÉ DE LA CLÔTURE p-ADIQUE DANS LE LANGAGE $L(V,P_n)$). *Soit $(A_i,v_i) \subset (K_i,v_i)$, $i = 1,2$, des extensions de corps valués où $K_i \in CpC$ et K_i est algébrique sur A_i. Soit $f\colon A_1 \xrightarrow{\sim} A_2$, un isomorphisme de corps valué tel que pour tout n on ait $A_1 \cap K_1^{\bullet n} = A_2 \cap K_2^{\bullet n}$, via f. Alors f se prolonge en un isomorphisme de corps valués de K_1 sur K_2.*

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

PROPOSITION 4.6. *La classe CpC est modèle-complète dans le langage $L(V,P_n)$.*

DÉMONSTRATION: Soit une extension $(K,v) \subset (K',v)$,où K, $K' \in$ CpC. Notons que K est nécessairement une sous-structure pour $L(V,P_n)$, *i.e.* $P_n^k = K^{\bullet n} = K \cap (K')^{\bullet n}$, car par ce qui précède K est relativement algébriquement clos dans K'. La formule test $\phi(\overline{x},\overline{k})$ est cette fois de la forme

$$f(\overline{x}) = 0 \wedge \cdots \wedge f_m(\overline{x}) = 0 \wedge g(\overline{x}) \neq 0 \wedge \bigwedge_i (\neg) P_{n(i)}(h_i(\overline{x})) \wedge \bigwedge_j (\neg) V(g_j(\overline{x})h_j(\overline{x})^{-1})$$

où f, g, $h \in K[\overline{X}]$, et où $(\neg)$ indique qu'on a possiblement une négation. Supposons que $\exists \overline{x} \phi(\overline{x}, \overline{k})$ soit vraie dans K'. En passant aux clôtures p-adiques on peut supposer, comme pour CAC que le degré de transcendance de E sur K est 1. On a deux cas:

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

$$\Sigma = \mathrm{C}p\mathrm{C} + \Delta(K, v) + \{\neg(t = k) \mid k \in K\} + \{v(t - k_0) = v(k_1) \mid k_0, k_1 \in K \text{ et } v(b - k_0) = v(k_1)\}$$

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 $L(V)$. On montre que $\Sigma \models \exists \overline{x} \phi(\overline{x}, \overline{k})$. En effet, soit $(K, v) \subset (K'', v)$ un modèle de Σ et $t \in K'' \setminus K$ satisfaisant les conditions données. Alors la théorie des valuations dit 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 (voir [**Ri**, p. 96]). On a donc un K-isomorphisme de corps valués $f\colon K(t) \xrightarrow{\sim} K(b)$, tel que $f(t) = b$. Soit $K(t)^{p\text{-ad}}$ la clôture p-adique de $K(t)$ dans K''. En utilisant le fait que $\operatorname{val} K(t) = \operatorname{val} K$, on montre que $\left(K(t)^{p\text{-ad}}\right)^{\bullet n} \cap K(t) = (K')^{\bullet n} \cap K(b)$ d'où $K(t)^{p\text{-ad}} \simeq K'$ (*cf.* proposition 4.5) et donc $\exists \overline{x} \phi(\overline{x}, \overline{k})$ est aussi vraie dans K''.

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

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

sachant que b est une solution dans K'. Des réductions élémentaires comme dans [**Ro**, p. 56] nous ramène à un système

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

Mais ce système n'est rien d'autre que $y \not\equiv 0$, $y \not\equiv c_i$ dans le corps des restes $\operatorname{res} K = \operatorname{res} K' = \mathbb{F}_p$, ce qui assure qu'il y a une solution dans K.

(2) $\operatorname{val} K \subsetneq \operatorname{val} K'$: soit $b \in K'$ tel que $v(b) \in \operatorname{val} K' \setminus K$. Notons que $n \cdot \operatorname{val} K = \operatorname{val} K \cap n \cdot \operatorname{val} K'$, $n = 2, 3, \ldots$. On considère cette fois

$$\begin{aligned} \Sigma = \mathrm{C}p\mathrm{C} + \Delta(K, v) &+ \{\neg(t = k) \mid k \in K\} \\ &+ \{v(k_0) < v(t) < v(k_1) \mid k_i \in K,\ v(k_0) < v(b) < v(k_1)\} \\ &+ \{P_n(e_n t) \mid e_n \in \mathbb{N},\ e_n b \in K^{\bullet n}\ n = 2, 3, \ldots\} \end{aligned}$$

Comme précédemment on montre que $\Sigma \models \exists \overline{x} \phi(\overline{x}, \overline{k})$. Par le théorème de compacité on se ramène à résoudre dans K

$$t \neq k_i, \quad i = 1, \ldots, m, \quad \delta < v(t) < \gamma, \quad P_n(e_n t)$$

où δ, $\gamma \in \operatorname{val} K$ (en passant au minimum et au maximum) et $n \in \mathbb{N}$ (en passant au ppcm), en sachant que b est une solution dans K'. On a $\lambda p^{-r} b = z^n$, pour un certain $z \in K$ et λ, r comme dans le lemme 4.2. On en déduit $e_n d p^r \in (K')^{\bullet n}$, $d = \lambda^{-1}$, d'où $e_n d p^r \in K^{\bullet n}$, et $\delta - r v(p) < n \cdot v(z) < \gamma = r v(p)$. Soit $\beta \in \operatorname{val} K$, et $0 \leq s < n$ tel que $\delta - r v(p) = n \cdot \beta + s v(p)$, et $y \in K$ tel que $v(y) = \beta + v(p)$. Alors $e_n d p^r y^n \in K^{\bullet n}$ et $\delta < v(d p^r y^n) < \gamma$. Comme K possède une infinité d'éléments ayant la même valuation, on peut choisir y tel qu'on ait aussi $d p^r y^n \neq k_i$ et alors $d p^r y^n$ est une solution dans K. □

5. Conclusion. Le lien entre les opérations ensemblistes sur une classe d'ensembles "définissables" et les relations logiques entre les descriptions de ceux-ci, tel qu'illustré dans dans la traduction du théorème de Macintyre en termes "logiques", ne semble pas un fait universellement connu, comme le suggère Van den Vries ([**VD**, p. 191])::

> *" The Kuratowski-Tarski translation of logical formulas into intersection, complement, projection operations, etc., is of course familiar to logicians, but this routine sort of "linguistic" argument seems little known to mathematicians in general. Perhaps this explains why one sometimes finds explicit proofs that the closure of semialgebraic set is semialgebraic (and similar things) instead of a brief remark that this is immediate from the ε-δ formulation of closedness."*

Les ensembles "semialgébriques" dont on parle ici sont les combinaisons booléennes d'ensembles $\{x \in \mathbb{R}^n \mid f(x) \geq 0\}$, $f(X_1, \ldots, x_n)$ un polynôme, dans le théorème de Tarski. Nous renvoyons à l'article de Van den Dries [**VD**] qui illustre comment cette idée, simple en soi, peut être mise à contribution avec fruit.

Appendice.

DÉMONSTRATION DE LA PROPOSITION 3.6: On travaille dans les langages L, $L(V)$, $L(V, P_n)$, plus des constantes, et avec un ensemble d'énoncés T dont les modèles sont des corps où $P_n(x)$ est interprété par $\exists y(y^n = x)$. Supposons que K satisfait la condition et soit $\phi(\overline{x}, \overline{y})$ une formule sans quantificateur. Considérons l'ensemble X des formules sans quantificateur $\chi(\overline{y})$ telles que $T \models \forall \overline{y}(\exists \overline{x} \phi(\overline{x}, \overline{y}) \rightarrow \chi(\overline{y}))$. Traitant $\overline{y} = (y_1, \ldots, y_n)$ comme des (nouvelles) constantes arbitraires, on montre que $T + \{\chi(\overline{y}) \mid \chi \in X\} \models \exists \overline{x} \phi(\overline{x}, \overline{y})$. Dans ce cas le théorème de compacité entraîne qu'il suffit d'un nombre fini de $\chi_i \in X$, disons $\chi_1, \ldots, \chi_n$, d'où $T \models (\chi_1(\overline{y}) \wedge \cdots \wedge \chi_n(\overline{y})) \rightarrow \exists \overline{x} \phi(\overline{x}, \overline{y})$. On obtient l'équivalence voulue puisque $\chi_i \in X$. Soit donc K un modèle de $T + \{\chi(\overline{y}) \mid \chi \in X\}$, et $a_1, \ldots, a_n \in K$ les valeurs données à $y_1, \ldots, y_n$. Soit A le sous-corps engendré par les a_i qui est de façon évidente une sous-structure de K. Montrons que la théorie $T + \Delta(A) + \exists \overline{\phi}(\overline{x}, \overline{a})$ possède un modèle, $\overline{a} = (a_1, \ldots, a_n)$. En effet, si tel est le cas, on aura un autre modèle K' de T ayant A comme sous-structure et où $\exists \overline{x} \phi(\overline{x}, \overline{a})$ est vrai. Par hypothèse $\exists \overline{x} \phi(\overline{x}, \overline{a})$ devra donc être aussi vrai dans K comme on le voulait (dans $L(V, P_n)$ on met aussi dans $\Delta(A)$ les $P_n(a)$ pour $a \in A \cap K^{\bullet n}$). Par le théorème de compacité il suffit de montrer que tout sous-ensemble fini de $T + \Delta(A) + \exists \overline{x} \phi(\overline{x}, \overline{a})$ a un modèle. Or une partie finie de $\Delta(A)$ est équivalente, en prenant la conjonction de ses membres, à une formule sans quantificateur disons $\Theta(\overline{a})$. Puisque $\Theta(\overline{a})$ est vrai dans K, alors $\neg\Theta(\overline{a}) \notin X$. On en conclut que $T + \Theta(\overline{a}) + \exists \overline{x} \phi(\overline{x}, \overline{a})$ a un modèle, ce qui achève la démonstration. □

DÉMONSTRATION DE LA PROPOSITION 4.5: Il suffit de prolonger f à un sous-corps intermédiaire B_1 tel que pour tout n, $n \cdot \operatorname{val} B_1 = n \cdot \operatorname{val} K_1 \cap \operatorname{val} B_1$, car alors $\operatorname{val} B_1$ est un $\mathbb{Z}$-groupe, et en passant au hensélisé de B_1 et de son image $B_2 = f(B_1)$, disons H_1 et H_2, on obtient $H_1 \simeq H_2$ et $H_i \in C_p C$, et on peut conclure par le lemme 4.4. Il suffit évidemment de considérer $n = q$ premier. Soit donc q premier $a_1 \in A_1$, $a_2 = f(a_1)$, tel que $v(a_1)/q \in \operatorname{val} K_1 \setminus \operatorname{val} A_1$ (en particulier $a_1 \notin A_1^{\bullet q}$). Notons que $X^q - a_i$ est irréductible sur A_i. On peut supposer que $a_1 \in K_1^{\bullet n}$ (*cf.* lemme 4.2), et donc aussi $a_2 \in K_2^{\bullet q}$. Soit $y_1 \in K_1$ tel que $y_1^q = a_1$, et $e_n \in \mathbb{N}$, $n = 2, 3, 4, \ldots$, tels que $e_n y_1 \in K_1^{\bullet n}$. Nous allons prolonger f à $A_1(y_1)$ tout en préservant ses propriétés. Ceci permet d'appliquer le lemme de Zorn pour compléter la démonstration. Parce que $v(y_1) = v(a_1)/q \notin \operatorname{val} A_1$ et q premier, la valuation induite sur $A_1(y_1)$ est complètement déterminée: $v\left(\sum_{i=0}^{q-1} c_i y^i\right) = \min v(c_i y^i)$. Il s'agit alors de bien choisir une racine q-ième de a_2 dans A_2. On la choisit comme suit:

$$\text{il existe } y_2 \in K_2 \text{ tel que } y_2^q = a_2 \text{ et } e_n y_2 \in K_2^{\bullet n},\ n = 2, 3, \ldots \qquad (*)$$

$(*) \implies$ 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 tel que $\overline{f}(y_1) = y_2$. Il faut voir que $K_1^{\bullet n} \cap A_1(y_1) = K_2^{\bullet n} \cap A_2(y_2)$ via $\overline{f}$. Soit $x_1 \in A_1(y)$, $x_2 = \overline{f}(x_1)$. Il existe $d_1 \in A_1$ tel que $v(x_1 d_1 y_1^j) = 0$. Posons $d_2 = f(d_1)$, alors $v(x_2 d_2 y_2^j) = 0$. Il existe $\lambda \in \mathbb{N}$ tel que $v(\lambda) = 0$ et $\lambda x_1 d_1 y_1^j \in K_1^{\bullet n}$ et donc $\lambda x_2 d_2 y_2^j \in K_2^{\bullet n}$ (*cf.* lemme 4.2 et le fait que $V_{A_i}/(p^s) = V_{K_i}/(p^s) \simeq \mathbb{Z}/(p^s)$). D'où, $x_1 \in K_1^{\bullet n}$ ssi $\lambda d_1 y_1^j \in K_1^{\bullet n}$, ssi $\lambda d_1 e_n^{-j} \in K_1^{\bullet n}$, ssi $\lambda d_2 e_n^{-j} \in K_2^{\bullet n}$, ssi $\lambda d_2 y_2^j \in K_2^{\bullet n}$, ssi $x_2 \in K_2^{\bullet n}$.

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 $(\mathbb{Q}, v_p)$ qui se plonge dans chacun des K_i. Si il y en a une seule alors il y a un seul y_2 et on a fini puisque dans ce cas $x \in K_1^{\bullet n}$ ssi $x^q \in K_1^{\bullet nq}$, et $(e_n y_1)^q = e_n^q a_1 \in A_1$ etc. Soit donc $z \in K_2$ une racine primitive q-ième de 1, et $b \in K_2$ tel que $b^q = a_2$. Alors les racines q-ièmes de a_2 sont $b, bz, \ldots, bz^{q-1}$. Supposons $(*)$ faux. Alors il existe $n_0, \ldots, n_{q-1}$ tels que $e_{n_j} bz^j \notin K_2^{\bullet n_j}$, et donc $e_n bz^j \notin K_2^{\bullet n}$, où $n = \text{ppcm}(n_j)$ $(e_n^{-1} e_{n_j} \in K_i^{\bullet n_j})$. Mais $e_n y_1 \in K_1^{\bullet n}$ entraîne $e_n^q a_1 \in K_1^{\bullet nq}$, d'où $e_n^q a_2 = (e_n b)^q \in K_2^{\bullet nq}$, $(e_n b x^n)^q = 1$ pour un certain $x \in K_2$, et $e_n bz^j \in K_2^{\bullet n}$ pour un certain j, contradiction. □

BIBLIOGRAPHIE

[AK] J. Ax et S. Kochen, *Diophantine problems over local fields I*, Amer. J. Math. **87** (1965), 605–648; *III*, Ann. of Math **83** (1966), 439–456.

[D1] J. Denef, *The rationality of the Poincaré series associated to the p-adic points of a variety*, Inventiones Math. **77** (1984), 1–23.

[D2] J. Denef, *On the evaluation of certain p-adic integrals*, dans "Séminaire de théorie des nombres, Paris 1983-84," Progress in Math. **59**, Birkhauser, 1985.

[D3] J. Denef, *p-adic semi-algebraic sets and cell decomposition*, J. Reine Angew. Math. **369** (1986), 154–166.

[DV] J. Denef et L. Van den Dries, *p-adic and real subanalytic sets*, Ann. of Math. **128** (1988), 79-138.

[Ek] P. Eklof, *Ultraproducts of algebraists*, dans "Handbook of Mathematical Logic," North-Holland, 1977.

[Ha] H. Hasse, "Number Theory," Springer-Verlag, 1980.

[M1] A. Macintyre, *On definable subsets of p-adic fields*, J. Symbolic Logic **41** (1976), 605–610.

[M2] A. Macintyre, *Twenty years of p-adic model theory*, dans "Logic Colloquium '84, Manchester," North-Holland, 1986.

[PR] A. Prestel et P. Roquette, "Formally p-adic fields," Lect. Notes in Math. **1050**, Springer-Verlag, 1986.

[Ri] P. Ribenboim, "Théories des valuations," Presses de l'Univ. de Montréal, 1964.

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

[Se] J.-P. Serre, "Cours d'arithmétique," Presses Univ. de France, 1970.

[VD] L. Van den Dries, *A generalization of the Tarski-Seidenberg theorem, and some non-definability results*, Bull. A.M.S. **15** (1986), 189–193.

[We] V. Weispfenning, *Quantifier elimination and decision procedure for valued fields*, dans "Logic Colloquium '83, Aachen," Lect. Notes in Math. **1103**, Springer-Verlag, 1986.

L. Bélair
Département de mathématiques et informatique
Université du Québec à Montréal
C.P. 8888 Succ. A
Montréal, Québec H3C 3P8