C.R. Math. Rep. Acad. Sci. Canada - Vol. X, No. 6, December 1988 décembre 285

MODELES PREMIERS ET CORPS REGULIEREMENT CLOS

Luc Bélair (1)

Presented by A.H. Lachlan, F.R.S.C.

RESUME. Dans le langage d'élimination des quantificateurs, et hormis le cas naturel, il n'y a pas de modèle premier au-dessus d'un ensemble de paramètres (dénombrable) dans la théorie des corps régulièrement clos de caractéristique 0 et dont le groupe de Galois absolu est (top.) libre sur e générateurs, $e \in \omega$.

§ 0. INTRODUCTION

Un corps K est dit régulièrement clos si toute variété affine sur K, absolument irréductible, possède un point rationnel sur K. Cette propriété est apparue dans l'étude de la théorie du premier ordre des corps finis [Ax] (voir aussi [FJ]). Soit $\mathfrak{L}$ le langage des anneaux, RGC la théorie des corps régulièrement clos, $\mathrm{Sol}_n(x_1, \ldots, x_n)$, $n \in \omega$, des prédicats dont l'interprétation est RGC $\models \mathrm{Sol}_n(\overrightarrow{x}) \leftrightarrow \exists y\, (y^n + x_1 y^{n-1} + \ldots + x_n = 0)$, et $\mathfrak{L}(\mathrm{Sol}_\omega) = \mathfrak{L} + \{\mathrm{Sol}_n : n \in \omega\}$. Cherlin, Macintyre et van den Dries [CMD] ont montré que la théorie des corps d'Iwasawa parfaits régulièrement clos élimine les quantificateurs dans le langage $\mathfrak{L}(\mathrm{Sol}_\omega)$ muni de prédicats témoignant de chaque type d'isomorphisme des images finies du groupe de Galois absolu. On obtient en particulier, pour tout $e \geq 1$, l'élimination des quantificateurs (E.Q.) de la théorie RGC_e des corps parfaits régulièrement clos dont le groupe de Galois absolu est (topologiquement) libre sur e générateurs (voir aussi [JK]). Dans cette note nous démontrons un résultat sur les modèles premiers au-dessus d'ensembles de paramètres pour RGC_e dans le langage d'élimination $\mathfrak{L}(\mathrm{Sol}_\omega)$, résultat déjà connu de Macintyre et van den Dries (ibid.), mais

(1) Les résultats de cette note ont été obtenus alors que l'auteur était boursier postdoctoral du C.R.S.N.G. dans l'Equipe de logique mathématique C.N.R.S., Université de Paris-VII. L'auteur remercie également A.Macintyre pour plusieurs discussions utiles.

dont la preuve semble avoir été oubliée. Si F est un corps, alors $F^{\bullet}$ désigne son groupe multiplicatif, G(F) son groupe de Galois absolu, et pour $\vec{\sigma} \in G(F)^e$, $Inv(\vec{\sigma})$ est le corps des invariants de $\vec{\sigma}$. Notre démonstration utilise des techniques telles qu'indiquées dans [CMD]: en particulier le lemme de Gaschutz ([Ga], théorème I), ainsi que le théorème de compacité en conjugaison avec les méthodes de Jarden pour construire des modèles de RGC_e [Ja]. Notons que dans la théorie RGC, les prédicats Sol_n se prolongent de façon unique d'un anneau intègre à son corps des fractions.

§ 1. LE RESULTAT

Soit $M \models RGC_e$ et $A \subseteq M$ un sous-corps de M. Si M/A est algébrique, alors, dans le langage $\mathfrak{L}(Sol_\omega)$, M est premier au-dessus de A. En effet, si ι: $A \hookrightarrow N$ est un $\mathfrak{L}(Sol_\omega)$-plongement de A dans un autre modèle N, alors tout polynôme sur A a un zéro dans M si et seulement si il en a un dans N. Par un lemme de Ax (voir [Po]), ι se prolonge en un $\mathfrak{L}(Sol_\omega)$-plongement $M \hookrightarrow N$ au-dessus de A. Le théorème ci-dessous montre que, au moins en caractéristique zéro et si A est dénombrable, c'est le seul cas possible. Notons, par exemple, qu'on peut plonger un corps algébriquement clos dénombrable dans un modèle de RGC_e (voir [Ja]).

Théorème. Soit $M \models RGC_e$, de caractéristique zéro, et $A \subseteq M$ un sous-corps dénombrable de M. Alors, dans $\mathfrak{L}(Sol_\omega)$, M est premier au-dessus de A si et seulement si l'extension M/A est algébrique.

Démonstration. Supposons que M/A n'est pas algébrique. Si M est premier au-dessus de A alors, par le lemme de Ax, M est aussi premier au-dessus de la clôture algébrique relative de A dans M. On peut donc supposer que A est relativement algébriquement clos dans M. Il suffit de montrer que M n'est pas atomique sur A. Soit donc $t \in M$, un élément transcendant sur A. On montre que le type tp(t/A) de t au-dessus de A n'est pas isolé. Soit $\alpha(v, \vec{a}) \in$ tp(t/A), nous allons montrer que α n'isole pas tp(t/A). Par E.Q. on a:

$$RGC_e \models \alpha(v, \vec{a}) \leftrightarrow \bigvee_j \bigwedge_i \exists w_i(F_{ij}(w_i, v, \vec{a}) = 0) \wedge \neg \exists w_j(H_j(w_j, v, \vec{a}) = 0)$$

où $F_{ij}, H_j \in \mathbb{Z}[X, Y, \vec{Z}]$. Il suffit de considérer l'une de ces conjonctions satisfaite par t. On peut donc supposer:

$$RGC_e \models \alpha(v, \vec{a}) \leftrightarrow \bigwedge_i \exists w_i(F_i(w_i, v, \vec{a}) = 0) \wedge \neg\exists w(H(w, v, \vec{a}) = 0) .$$

On travaille dans une clôture algébrique fixée de M. Soit L le corps de décomposition des F_i, H au-dessus de A(t), M' la clôture algébrique relative de A(t) dans M, et B = L $\cap$ M', de sorte que M' et L sont linéairement disjoints au-dessus de B. Notons que G(M'), G(A) sont tous deux (topologiquement) engendrés par e générateurs. Soit A" la clôture algébrique relative de A dans M'L, alors pour tout corps intermédiaire $B \subseteq E \subseteq M'$ on a [EA": BA"] = [A": A] = [A"M': M']. Notons que Gal(L/B) est aussi engendré par e générateurs. Le lemme suivant est un corollaire immédiat de la Proposition 7 de [Du].

Lemme 1. Soit $\{k_1, k_2, \ldots\}$ un ensemble infini d'entiers distincts, et $f_n(X) = X^2 - (t + k_n)(t + k_{n+1})$, pour n = 1, 2, ... Alors les polynômes $f_n(X, t)$ sont absolument irréductibles et engendrent des extensions linéairement disjointes au-dessus de A(t).

Par hypothèse M' possède au plus e extensions de chaque degré dans une clôture algébrique fixée, et donc l'indice des carrés $(M')^{\cdot 2}$ dans $(M')^{\cdot}$ est au plus e + 1. On peut donc trouver un ensemble infini d'entiers distincts $\{k_1, k_2, \ldots\}$ tel que $X^2 - (t + k_n)(t + k_{n+1})$ ait une racine dans M' pour tout n = 1, 2, ... Le lemme 1 implique alors que pour toute extension finie de A(t) dans M', il existe des entiers k, k' tel que $X^2 - (t + k)(t + k')$ n'a pas de racine dans cette extension mais en possède une dans M'. Soit $f(X, t)$ un tel polynôme de degré 2 pour B, et B_1/B l'extension quadratique engendrée par f; ainsi $M \models \alpha(t) \wedge \exists x(f(x, t) = 0)$. Nous allons construire un modèle $N \models RGC_e$ tel que $A(t) \subseteq N$, $N \models \alpha(t) \wedge \neg\exists x(f(x, t) = 0)$, et A soit relativement algébriquement clos dans N, ce qui assurera que $\alpha(t)$ n'isole pas $tp(t/A)$. Il suffit de construire un modèle de la théorie suivante du langage $\mathcal{L}(B)$, où $\Delta(B)$ est le diagramme de B:

$$RGC_e + \Delta(B) + \alpha(t) + \neg\exists x(f(x, t) = 0) + \{\neg\exists x(g(x) = 0) \ : \ 0 \neq g \in A[X]\} .$$

Pour satisfaire les conditions sur A, il suffit, par compacité, de considérer une extension galoisienne finie A'/A à éviter. Notons que A" est aussi la clôture algébrique relative de A dans L; on peut supposer que A' est une extension de A" et posons $d = [A'\colon A'']$. Les extensions A"/A et BA"/B sont aussi galoisiennes. Par hypothèse, A" coïncide avec la clôture algébrique relative de A dans B_1L. Il s'ensuit que A' et B_1L sont linéairement disjoints au-dessus de A", d'où $[B_1LA'\colon B_1L] = [A'\colon A''] = d = [A'L\colon L]$. Comme $[B_1L\colon B_1] = [L\colon B]$, on en conclut que B_1 et A'L sont linéairement disjoints au-dessus de B. Il est clair que L et A'B sont linéairement disjoints au-dessus de A"B ($[A'B\colon A''B] = d$), et donc Gal(A'L/A"B) est produit direct de Gal(A'B/A"B) et Gal(L/A"B), et les applications de restriction Gal(A'L/A'B) $\longrightarrow$ Gal(L/A"B), Gal(A'L/L) $\longrightarrow$ Gal(A'B/A"B) sont des isomorphismes.

<u>Lemme 3</u>. <u>Soit</u> $x \in$ Gal(A'B/B) <u>et</u> $y \in$ Gal(L/B) <u>tel que les restrictions</u> $x|A''B$ <u>et</u> $y|A''B \in$ Gal(A"B/B) <u>coïncident</u>. <u>Alors il existe</u> $z \in$ Gal(A'L/B) <u>tel que</u> $z|A'B = x$ <u>et</u> $z|L = y$.

<u>Lemme 4</u>. <u>Il existe</u> $\sigma_1, \ldots, \sigma_e \in$ Gal(A'L/B) <u>tel que</u> $Inv(\vec{\sigma}) \cap L = B$ <u>et</u> $Inv(\vec{\sigma}) \cap A'B = B$.

<u>Démonstration</u>. Les groupes Gal(A'B/B), Gal(L/B), Gal(A"B/B) sont des images homomorphes de G(M') et par conséquent engendrés chacun par e éléments. Soit $\theta_1, \ldots, \theta_e$ des générateurs de Gal(A"B/B), alors par le lemme de Gaschutz les θ_i se relèvent en des générateurs g_i et h_i de

Gal(A'B/B) et Gal(L/B) respectivement. Par le lemme précédent il existe $\sigma_1, \ldots, \sigma_e \in$ Gal(A'L/B) tel que $\sigma_i|A'B = g_i$ et $\sigma_i|L = h_i$. □

Comme B_1 et A'L sont linéairement disjoints au-dessus de B, il existe $\theta_1, \ldots, \theta_e \in$ Gal(BA'L/B) tel que $\mathrm{Inv}(\vec{\theta}) \cap L = B$, $\mathrm{Inv}(\vec{\theta}) \cap A'B = B$ et $\mathrm{Inv}(\vec{\theta}) \cap B_1 = B$. Notons que B, une extension finie de A(t), est dénombrable et hilbertien. Par les résultats de Jarden [Ja], il existe $\vec{\sigma} \in G(B)^e$ tel que $\mathrm{Inv}(\vec{\sigma}) \models RGC_e$ et $\vec{\sigma}|A'LB = \vec{\theta}$. Alors $\mathrm{Inv}(\vec{\sigma})$ est un modèle de $RGC_e + \Delta(B) + \alpha(t) + \neg\exists x(f(x, t) = 0)$ et ne contient aucun élément de A'. □

Notre démonstration montre aussi qu'en toute cardinalité d'ensemble de paramètres A, ou bien A se plonge dans un modèle M tel que M/A est algébrique, et alors M est premier au-dessus de A, ou bien il n'y a pas de modèle atomique sur A.

§ 2. APPLICATION AUX CORPS p-ADIQUES

Dans le cas particulier e = 1, la théorie RGC_1 a pour modèles les modèles infinis de la théorie des corps finis, et en particulier de la théorie des corps premiers finis $T = \mathrm{Th}(\{\mathbb{F}_p\text{: p premier}\})$. Soit $\mathbb{Q}_p$ le corps des nombres p-adiques, et considérons la théorie de corps valué $\Sigma = \mathrm{Th}(\{\mathbb{Q}_p\text{: p premier}\})$ (voir [Bé]). La théorie T apparaît alors comme théorie résiduelle des modèles de Σ d'égale caractéristique zéro. La théorie Σ élimine les quantificateurs dans le langage $\mathcal{L}'$, obtenu de $\mathcal{L}$ en ajoutant pour chaque $n \geq 2$: un nombre fini de constantes, un prédicat $\underline{P}_n(x)$ interprété par $\underline{P}_n(x) \longleftrightarrow \exists y(y^n = x)$, et un prédicat $S_n(x_1, \ldots, x_n)$ interprété comme Sol_n au niveau du corps des restes (ibid.). Des techniques standard de la théorie des modèles des corps valués permettent de démontrer que pour $M \models \Sigma$, d'égale caractéristique 0, et $A \subset M$ un sous-corps, si, dans $\mathcal{L}'$, M est premier au-dessus de A, alors, dans $\mathcal{L}(\mathrm{Sol}_\omega)$, le corps des restes de M est premier au-dessus du corps des restes de A. Ceci permet de "relever" le résultat du paragraphe § 1. au niveau de la théorie Σ: soit M, A comme ci-dessus et A dénombrable, alors, dans le langage $\mathcal{L}'$, M est premier au-dessus de A si et seulement si l'extension M/A est algébrique. On peut trouver un tel A dont le corps des restes est algébriquement clos, de sorte qu'il n'y a pas de modèle de Σ qui, dans $\mathfrak{B}'$, soit premier au-dessus de ce A. Il s'ensuit que, dans $\mathfrak{B}'$, la théorie Σ ne possède pas de fonctions de Skolem définissables (voir [VdD]). Ceci a une incidence sur l'étude de l'uniformité par rapport au paramètre p dans les résultats de Denef sur la rationalité de séries de Poincaré p-adiques (voir [Ma]).

REFERENCES BIBLIOGRAPHIQUES

[Ax] J.Ax, "The Elementary Theory of Finite Fields", Ann. of Math. 88 (1968), p.239-271.

[Bé] L.Bélair, "Substructures and Uniform Elimination for p-Adic Fields", Ann. Pure & Appl. Logic (à paraître).

[CMD] G.Cherlin, A.Macintyre et L.van den Dries, "The Elementary Theory of Regularly Closed Fields", Crelle (à paraître).

[Du] J.-L.Duret, "Les corps pseudo-finis ont la propriété d'indépendance", C.R.Acad. Sci. Paris (Sér. A) 290 (1980), p.981-983.

[FJ] M.Fried et M.Jarden. Field Arithmetic. Springer-Verlag, 1986.

[Ga] W.Gaschutz, "Zu einem von B.H. und H. Neumann gestellten Problem", Math. Nachrichten 14 (1956), p.249-252.

[Ja] M.Jarden, "Elementary Statements over Large Algebraic Fields", Trans. A.M.S. 164 (1972), p.67-91.

[JK] M.Jarden et U.Kiehne, "The Elementary Theory of Algebraic Fields of Finite Corank", Inv. Math. 30 (1975), p.275-294.

[Ma] A.Macintyre, "Twenty Years of p-Adic Model Theory", in Logic Colloquium '84, Manchester, North-Holland, 1986.

[Po] B.Poizat, "Une preuve d'un théorème de James Ax sur les extensions algébriques d'un corps", C.R.Acad. Sci. Paris, 291 (1980), p.245.

[VdD] L.van den Dries, "Algebraic Theories with Definable Skolem Functions", Jour. Symb. Logic 49 (1984), p.625-629.

Received September 9, 1988

Département de Mathématiques et Informatique,
Université du Québec à Montréal,
Québec, Canada H3C 3P8