Théorie des modèles des corps valués et applications

François-Xavier Villemin

7 septembre 2004

Table des matières

Introduction

Les structures algébriques sont intrinsèquement liées à la théorie des modèles. Dans cet exposé, après avoir introduit les bases de la théorie algébrique des corps valués, on s'intéresse essentiellement à son aspect modèle-théorique, et l'on démontre des résultats de complétude (partie 3) et d'élimination de quantificateurs (partie 4) pour certaines classes de corps valués, ainsi que des applications en algèbre (partie 5).

1 Généralités algébriques sur les corps valués

1.1 Définitions

Définition 1.1 [Groupe ordonné] Soit Γ un groupe commutatif, noté additivement, et $\leq$ une relation d'ordre sur Γ. On dit que $(\Gamma, \leq)$ est un groupe ordonné si pour tous $a \leq b$ et c dans Γ, $a + c \leq b + c$.

On remarque qu'un groupe totalement ordonné est sans torsion, soit en effet $c \neq 0$. On peut supposer, en considérant c et $-c$, que $c > 0$. Alors $n.c \geq (n-1).c \geq \ldots \geq c > 0$.

Définition 1.2 [Corps valué] Soit K un corps, $(\Gamma, \leq)$ un groupe commutatif totalement ordonné, et v une application de K dans $\Gamma \cup \{\infty\}$ (avec la convention $a + \infty = \infty + \infty = \infty$). v est une valuation sur K si elle vérifie pour tous x, y dans K :

- *$v(x) = \infty$ si et seulement si $x = 0$*
- *$v(xy) = v(x) + v(y)$*
- *$v(x + y) \geq \min\{v(x), v(y)\}$*

On dit alors que (K, v) est un corps valué.

Le groupe de valuation de K est $v(K^*)$ (noté abusivement $v(K)$).

Remarques :

(i) Un corps valué est donc la donnée de K, Γ et v. On supposera toujours dans la suite que $v(K^*) = \Gamma$, i.e. v surjective. Cela justifie aussi en quelque sorte de ne pas préciser le groupe de valuation dans la notation (K, v).

(ii) La donnée d'un élément $v(0) = \infty$ permet de donner une interprétation topologique à la valuation, mais elle n'est pas fondamentale dans la définition d'un corps valué.

Définition 1.3 Étant donné deux corps valués $(K, v) \subset (L, w)$, on dit que K est un sous-corps valué de L si la valuation de L prolonge celle de K.

Étant donné $f : (K, v) \to (K', v')$ un isomorphisme de corps, on dit que f est un isomorphisme de corps valués si il existe un morphisme ϕ croissant du groupe de valuation de K dans le groupe de valuation de K' tel que, pour tout $x \in K$, $\phi v(x) = v'(f(x))$.

Exemples

(i) Sur un corps des séries formelles $k((t))$, on définit la valuation d'une série α comme la plus grande puissance n telle que $\alpha = t^n\beta$, $\beta \in k[[t]]$. Le groupe de valuation est alors isomorphe à $\mathbb{Z}$.

(ii) La valuation p-adique sur $\mathbb{Q}$ ou sur son complété $\mathbb{Q}_p$ est également une valuation de groupe $\mathbb{Z}$.

Proposition 1.1 *Soit (K, v) un corps valué.*
- $v(1) = 0$
- *Pour tout x, $v(-x) = v(x)$.*
- *Si $v(x) \neq v(y)$, $v(x + y) = \min\{v(x), v(y)\}$*

Démonstration.- $v(1) = v(1.1) = v(1) + v(1)$ donc $v(1) = 0$

Pour le deuxième point, il suffit de voir que $v(-1) = 0$. Or $v(-1)+v(-1) = v(1) = 0$. Comme le groupe de valuation est sans torsion, $v(-1) = 0$.

Enfin, supposons $v(x) < v(y)$. Alors $v(x+y) = v(x)+v(1+yx^{-1})$. Il suffit donc de prouver que si $v(z) > 0$, $v(1+z) = 0$. Or $0 = v(1) = v(1+z-z) \geq \min\{v(1+z), v(-z)\}$, donc $v(1 + z)$ vaut nécessairement 0. □

Soit (K, v) un corps valué. Notons $A_v = \{x \in K | v(x) \geq 0\}$ et $M_v = \{x \in K | v(x) > 0\}$. La proposition précédente montre que A_v est un sous-anneau de K dont M_v est l'unique idéal maximal.

Définition 1.4 *A_v est l'anneau de valuation de (K, v).*

Le corps $\overline{K} = A_v/M_v$ est appelé **corps résiduel** *de K.*

1.2 Anneaux de valuation

On se donne dans cette partie un corps valué (K, v).

Proposition 1.2 *A_v vérifie la propriété suivante :*

$$\forall x \in K^* \ \ x \in A_v \ \text{ ou } x^{-1} \in A_v \quad (\star)$$

Réciproquement, tout anneau vérifiant ces propriétés définit une et une seule valuation sur K.

On en déduit en particulier qu'un anneau de valuation est local et intégralement clos.

Démonstration.- Cette propriété est évidemment vérifiée par un anneau de valuation. Inversement, soit A vérifiant ces propriétés. On vérifie alors facilement que le groupe fractionnaire G de A est l'ensemble des $A.x$ (tout idéal de type fini est principal), totalement ordonné par inclusion. Soit v l'application $x \to A.x$. Alors v est une valuation d'anneau A et de groupe $(G, \subset)$.

Si $x^n + \ldots + c_0 = 0$ et $x^{-1} \in A_v$, en multipliant par x^{-n+1}, on trouve immédiatement $x \in A_v$ donc A_v est intégralement clos. Il est local car l'ensemble des éléments non-inversibles de A_v forment l'idéal M_v. □

Théorème 1

Soit (K, v) un corps valué et L une extension de K. Alors il existe une valuation w de L qui prolonge v.

Démonstration.- On va démontrer qu'il existe un anneau de valuation de L convenable, c'est à dire un anneau $A \subset L$ vérifiant $(\star)$ tel que $A \cap K = A_v$.

Soit A un sous-anneau de L local et intégralement clos maximal tel que $K \cap A = A_v$ (obtenu grâce au lemme de Zorn) et soit $x \in L$. On suppose $x \notin A$. Par maximalité $A[x] \cap K \neq A_v$, il existe donc $P(x) \in K$, $v(P(x)) < 0$. Écrivons $P(x) = c_n x^n + \ldots + c_0$. En posant $\alpha = P(x)$:

$$Q(x^{-1}) = (1 - \alpha^{-1} c_0) x^{-n} + \alpha^{-1}(c_1 x^{-n+1} + \ldots + c_n) = 0$$

Or comme $v(\alpha) < 0$, $v(1 - \alpha^{-1} c_0) = 0$ donc $1 - \alpha^{-1} c_0$ est inversible dans A, donc x^{-1} est annulé par le polynôme unitaire $(1 - \alpha^{-1} c_0)^{-1} Q(t) \in A[t]$. A est intégralement clos, donc $x^{-1} \in A$.

A est donc l'anneau d'une valuation sur L, soit w. Alors w prolonge v, à isomorphisme près, car pour $y \in K$, $w(y) \geq 0$ si et seulement si $y \in A \cap K = A_v$, et donc l'application $v(y) \mapsto w(y)$ est un morphisme de groupes ordonné bien défini strictement croissant. □

Définition 1.5 Soient v et v' deux valuations de K. On définit l'ordre suivant (modulo l'identification des valuations équivalentes) :

$$v \leq v' \Leftrightarrow A_v \supseteq A_{v'}$$

On dit alors que v est **moins fine** *que v'.*

Théorème 2

L'ensemble des valuations moins fines que v est totalement ordonné et en correspondance biunivoque avec les idéaux premiers de A_v : à tout idéal premier P, on associe la valuation v_P d'anneau A_P et d'idéal maximal $PA_P = P$.

Démonstration.- Soit v' moins fine que v, donc $A = A_v \subset A_{v'}$. Soit P l'ensemble des éléments de A_v qui ne sont pas inversibles dans $A_{v'}$; $P = M_{v'} \cap A_v$ est un idéal de A_v, premier comme $M_{v'}$. Ainsi $A_P \subset A_{v'}$. Par ailleurs, si $x \in A_{v'}$, $v(x) < 0$, $x^{-1} \in A$ est inversible dans $A_{v'}$ donc $x^{-1}, x \in A_P$. Ainsi $A_P = A_{v'}$. On voit facilement que $P \subset PA_P$. Inversement, si $x \in PA_P$, $v(x) > 0$ car $x^{-1} \notin A_P \supset A$ donc $x \in P$.

Réciproquement, toute localisation A_P de A définit un anneau de valuation car $x \notin A_P$ implique $x \notin A$ implique $x^{-1} \in A \subset A_P$.

Enfin montrons que les idéaux premiers d'un anneau de valuation sont totalement ordonnés par inclusion, ce qui prouvera que deux valuations moins fines que v sont comparables. Soient P, P' deux idéaux premiers de A, on suppose $x \in P$, $x \notin P'$. Alors si $y \in P'$, $v(y) > v(x)$ (sinon x est multiple de y dans A donc $x \in P'$), donc $y \in P$. □

Corollaire 2 *Tout anneau de K contenant un anneau A de valuation est un anneau de valuation de la forme A_P.*

Deux valuations de K admettent un infimum. Elles admettent un supremum si et seulement si elles sont comparables.

Démonstration.- Soit $A \subset B \subset K$. Alors il est clair que B est un anneau de valuation (il vérifie $(\star)$) moins fine que celle d'anneau A, donc $B = A_P$.

Si A, A' sont les anneaux de v et v', alors AA' est le plus petit anneau contenant A et A' donc la valuation d'anneau AA' est l'infimum de v et v'.

Enfin si il existe un anneau de valuation B contenu dans A et A', alors A et A' sont de la forme B_P et $B_{P'}$, donc comparables. La réciproque est évidente. □

1.3 Théorème d'approximation

On s'intéresse dans cette section au problème suivant : étant données $v_1 \dots v_n$ des valuations sur K, $\alpha_1 \in v_1(K) \dots \alpha_n \in v_n(K)$, existe-t-il z tel que $v_i(z) = \alpha_i$ pour tout i. On montrera un résultat plus faible que le théorème d'approximation que l'on peut trouver dans [R1], mais suffisant pour la suite.

Définition 1.6 Deux valuations sont dites indépendantes si leur infimum est égal à la valuation triviale et si elles sont non-triviales.

Lemme 1.1 Soient v, v' deux valuations de K, A, A' leurs anneaux de valuation, $w = v \wedge v'$, et $A_w = A_P = A'_{P'}$, $M_w = P = P'$ est le plus grand idéal premier de A contenu dans M' (et le plus grand idéal premier de A' contenu dans M par symétrie).

Démonstration.- Il est clair que $P = P' = M_w$. Soit $P_1 \supset P$ un idéal premier de A inclus dans M'. Comme $A_{P_1} \subset A_P$, on va montrer que A_{P_1} contient A', donc $A_{P_1} = A_P$ puis $P = P_1$. Soit $x \in A'$. On n'a pas $x^{-1} \in P_1$, sinon $x^{-1} \in M'$ donc $x \notin A'$. Donc $A' \subset A_{P_1}$, c'est à dire $AA' = A_P \subset A_{P_1}$. □

Remarquons que si $w \leq v$, on a une surjection canonique de $v(K)$ sur $w(K)$ (si l'anneau de v est A et A_P celui de w, à $v(x)$ on associe $w(x)$, c'est bien défini car si $w(x) = 0$, $x \in A - M \subset A_P - P$). Ainsi, $w(x)$ est l'image de $v(x)$ donc v définit w pour toute valuation moins fine.

On note généralement $w = v_P$

Lemme 1.2 Soient v, v' des valuations incomparables de K, et $(\alpha, \alpha') \in v(K) \times v'(K)$. Si $w = v \wedge v'$, on suppose $w(\alpha) = w(\alpha') = 0$ (w désigne par abus de langage la projection canonique sur $w(K)$). Alors il existe $x \in K$ tel que $v(x) \leq \alpha$ $v'(x) \geq \alpha'$.

Démonstration.- On peut supposer $\alpha < 0$ et $\alpha' > 0$ ($A \not\subset A'$ donc il existe $x \in A$, $v'(x) < 0$ et de même $y \in A'$, $v(y) < 0$. Ainsi si $z = x^{-1}y$, $\alpha = v(z) < 0$ et

$\alpha' = v'(z) > 0$, et z est une unité de A_w car x et y en sont, donc le couple ainsi construit satisfait les conditions de l'énoncé).

On va montrer qu'il existe y tel que $v'(y) \geq \alpha'$ et $v(y) \leq 0$, par symétrie il existera z tel que $v'(z) \leq 0$ et $v(z) \geq -\alpha$. Ainsi $x = yz^{-1}$ conviendra.

Soit $a \in K$ tel que $v'(a) = \alpha'$.

Supposons par l'absurde que $J = \{x \in K | v'(x) \geq \alpha'\} \subset M$. J est un idéal de A' contenant a. Soit P' le radical de J, c'est à dire $P' = \{y \in K | \exists n\, y^n \in J\}$.

Alors $J \subset P' \subset M$ et P' est un idéal premier de A' (si $nv'(xy) \geq \alpha'$, et par exemple $v'(x) \geq v'(y)$, alors $2nv'(x) \geq \alpha'$).

Or d'après le lemme précédent et comme v et v' sont indépendantes, tout idéal de A' contenu dans M est contenu dans l'idéal de w. En particulier, $w(a) > 0$, ce qui est absurde. □

Théorème 3

Soient $v_1 \dots v_n$ des valuations deux à deux incomparables, et $(\alpha_1 \dots \alpha_n) \in v_1(K) \times \dots \times v_n(K)$ tels que $v_1 \wedge v_i(\alpha_1) = v_1 \wedge v_i(\alpha_i) = 0$ pour $i > 1$. Alors il existe x tel que $v_1(x) \leq \alpha_1$ et $v_i(x) \geq \alpha_i$ si $i > 1$.

Démonstration.- On note A_i l'anneau de v_i, M_i l'idéal de v_i. Il existe pour tout i un idéal $P_i \subset A_1$ tel que P_i soit l'idéal de la valuation $v_1 \wedge v_i$. Ces idéaux sont distincts de M_1, et complètement ordonnés par inclusion donc il existe x non-inversible dans A_1 qui n'est dans aucun des P_i. On a montré ainsi que l'on pouvait supposer $\alpha_1 < 0$ (quitte à poser $\alpha_1 = v(x^{-1})$), et de la même façon, on peut bien sûr supposer $\alpha_i > 0$ pour $i > 1$.

Le théorème est vrai pour $n = 2$ d'après ce qui précède. Procédons par récurrence et supposant avoir démontré le lemme au rang $n-1$, démontrons-le au rang n.

Par hypothèse de récurrence, il existe a et b tels que $v_1(a), v_1(b) \leq \alpha_1$, et $v_i(a) \geq \alpha_i$ si $1 < i < n$, $v_i(b) \geq \alpha_i$ si $2 < i \leq n$. On va distinguer les cas selon le signe de $v_s(a)$ et $v_2(b)$. Remarquons que par symétrie on peut supposer $v_1(a) < v_1(b)$ (quitte à changer b en b^2 s'il y a égalité).

Si $v_n(a) \geq 0$ et $v_2(b) \geq 0$, $x = ab$ convient naturellement.

Si $v_n(a) \geq 0$ et $v_2(b) < 0$, posons $x = \frac{ab}{b+1}$. On vérifie :

$$v_1(x) = v_1(a) \leq \alpha_1$$

$$v_2(x) = v_2(a) \geq \alpha_2$$

$$v_i(x) = v_2(a) + v_2(b) \geq v_i(b) \geq \alpha_i \ (i \in \{3 \dots n\})$$

Si $v_n(a) < 0$ et $v_2(b) \geq 0$, il est clair que $x = \frac{ab}{a+1}$ convient.

Enfin si $v_n(a) < 0$ et $v_2(b) < 0$, posons $x = \frac{ab}{a+b+1}$. On vérifie :

$$v_1(x) = v_1(b) \leq \alpha_1 \text{ car } v_1(a) < v_1(b)$$

$$v_2(x) = v_2(a) \geq \alpha_2$$

$$v_i(x) = v_2(a) + v_2(b) \geq v_i(b) \geq \alpha_i \ (i \in \{3 \dots n-1\})$$

$$v_n(x) = v_n(b) \geq \alpha_n$$

Ceci conclut la preuve. □

Nous démontrons maintenant deux corollaires utiles pour la suite :

Corollaire 3.1 *Si $v_1 \dots v_n$ sont deux à deux incomparables, il existe x tel que $v_1(x) = 0$ et $v_i(x) > 0$ pour tout $i > 1$.*

Démonstration.- D'après le théorème d'approximation, il existe y_i tel que $v_i(y_i) < 0$ et $v_j(y_i) > 0$ pour tout $i \neq j$. Formons $y = \sum_{i>1} y_i$. Alors $v_1(y) > 0$ et $v_i(y) = v_i(y_i) < 0$ pour tout $i > 1$. Considérons l'élément $x = (1+y)^{-1}$. Alors $v_1(x) = -v_1(1) = 0$ tandis que $v_i(x) = -v_i(y) > 0$ pour tout $i > 1$. x convient. □

Corollaire 3.2 *Soient A et A_i $(i = 1 \dots n)$ des anneaux de valuations d'un même corps. On suppose $\bigcap A_i \subset A$. Alors il existe i tel que $A_i \subset A$.*

Démonstration.- En effet, dans le cas contraire on peut supposer A et les A_i deux à deux incomparables (quitte à éliminer les j tels qu'il existe $i \neq j$, $A_i \subset A_j$ ou $A \subset A_j$). Soient v et v_i les valuations correspondant respectivement à A et aux A_i. Alors d'après la preuve précédente, il existe x tel que $v(x) < 0$ et $v_i(x) \geq 0$, i.e. $x \in \bigcap A_i$ et $x \notin A$. □

1.4 Corps henselien, henselisation

On s'intéresse ici aux prolongements d'une valuation dans une extension algébrique.

Proposition 1.3 *Soit $\widetilde{K}$ une extension algébrique de (K, v) un corps valué.*

Alors tout prolongement $\widetilde{v}$ de v à $\widetilde{K}$ est à valeurs dans le groupe divisible engendré par $v(K)$.

Démonstration.- Soit $x \in \widetilde{K}$ et $P(t) = \sum_i a_i t^i$ son polynôme minimal sur K. Comme $P(x) = 0$, il existe $i \neq j$ tels que $\widetilde{v}(a_i x^i) = \widetilde{v}(a_j x^j)$ ce qui prouve que $\widetilde{v}(x) = \frac{v(a_i) - v(a_j)}{j-i}$. □

Proposition 1.4 *Deux valuations distinctes prolongeant une même valuation v d'un corps K à une extension algébrique sont incomparables.*

Démonstration.- Soient $A' \subset A$ deux anneaux de valuations comparables prolongeant la même valuation de K. Alors il existe un idéal premier P de A tel que $A' = A_P$ et P est l'idéal maximal de A_P. De plus comme on a un prolongement, $P \cap K = M \cap K$, où M désigne l'idéal maximal de A. Soit $x \in M$. Notons v la valuation correspondant à A. Alors il existe n tel que $v(x^n) \in v(K)$, on peut donc trouver u inversible dans A tel que $ux^n \in M \cap K = P \cap K$. Ainsi $ux^n \in P$ donc $x \in P$ car l'idéal P est premier et $P = M$, $A = A'$. □

Théorème 4

Soit $\widetilde{K}$ une extension algébrique de (K,v) et $\widetilde{v}$ un prolongement de v à $\widetilde{K}$. Alors tout prolongement de v est de la forme $\widetilde{v}\circ\sigma$, $\sigma\in Gal(\widetilde{K}|K)$.

Démonstration.- On peut supposer $\widetilde{K}$ normale, quitte à se placer dans l'extension normale engendrée par K. On suppose dans un premier temps que $\widetilde{K}$ est une extension finie.

Il est clair que $\widetilde{v}\circ\sigma$ est une valuation, d'anneau $\sigma^{-1}(A_{\widetilde{v}})$.

De plus $\bigcap_\sigma A_{\widetilde{v}\circ\sigma}$ est la clôture intégrale de A_v dans L.

En effet, si $x\in L$ est entier sur A_v, $P(t)=t^n+a_1t^{n-1}+\ldots+a_n\in A_v[t]$ un polynôme annulateur de x, et $\widetilde{v}(\sigma x)<0$, $\widetilde{v}(P(\sigma x))=nv(x)$ ce qui est contradictoire car $P(\sigma x)=0$.

Réciproquement, si $x\in\bigcap_\sigma A_{\widetilde{v}\circ\sigma}$, les coefficients de $\prod_\sigma(t-\sigma x)$ sont dans $K\cap A_{\widetilde{v}}=A_v$ donc x est bien entier sur A_v.

Soit A' l'anneau d'une valuation v' prolongeant v, alors $\bigcap_\sigma A_{\widetilde{v}\circ\sigma}\subset A'$. D'après le second corollaire du théorème 3, il existe σ tel que $A_{\widetilde{v}\sigma}\subset A'$ donc $\widetilde{v}\circ\sigma$ est plus fine que v', et ces deux valuations sont donc égales d'après le théorème 1.4.

Supposons maintenant $\widetilde{K}$ de degré infini et v' une valuation de prolongeant v. Considérons la famille (L,ρ) avec $L\subset\widetilde{K}$ une extension normale de K, $\rho\in\mathrm{Gal}(L|K)$ et $v'_{|L}=\widetilde{v}_{|L}\circ\rho$. Cette famille est inductive, elle admet un élément maximal (K',σ) et $K'=\widetilde{K}$ sinon on choisit $x\in\widetilde{K}-K'$ et on applique le cas fini à l'extension normale engendrée par x sur K', contredisant la maximalité de K'. □

Soit $p(t)\in A_v[t]$ un polynôme. Soit $\overline{p}(t)\in\overline{K}[t]$ le polynôme dont les coefficients sont les résidus des coefficients de p modulo M_v. Si $p(x)=0$ dans A_v, on a aussi $\overline{p}(\overline{x})=0$ dans $\overline{K}$. Réciproquement, un corps valué sera dit henselien ou corps de Hensel s'il vérifie la propriété suivante :

Lemme de Hensel *Pour tout polynôme $p\in A_v[t]$ et $\overline{x}\in\overline{K}$ racine simple de $\overline{p}$, il existe $y\in A_v$ racine simple de p telle que $\overline{y}=\overline{x}$.*

On a la caractérisation suivante :

Théorème 5

Soit (K,v) un corps valué. Alors il y a équivalence entre :
(i) *v se prolonge de façon unique à toute extension algébrique de K*
(ii) *Si $p(t)\in A_v[t]$ irréductible, $\overline{p}(t)$ est soit constant, soit de même degré que $p(t)$ et multiple d'une puissance d'un polynôme irréductible sur $\overline{K}[t]$.*
(iii) *Pour tout polynôme $p(t)\in A_v[t]$ et toute factorisation $\overline{p}(t)=u(t)v(t)$ dans $\overline{F}[t]$ telle que $\overline{q}$ et $\overline{r}$ soient premiers entre eux, il existe une factorisation $p(t)=q(t)r(t)$ dans $F[t]$, vérifiant $\overline{q}=u$, $\overline{r}=v$ et $\deg q=\deg u$.*
(iv) *K est henselien.*
(v) *Si $p(t)=t^n+a_1t^{n-1}+\ldots+a_n\in A_v[t]$, $a_1\notin M_v$, $a_i\in M_v$ $(i>1)$, p admet une racine simple de résidu a_1.*

Démonstration.- **(i)⇒(ii)** Soit K' une clôture algébrique de K, v' l'unique prolongement de v et $p \in A_v[t]$ irréductible sur K. On peut écrire $p(t) = \prod_i (at - b_i)$. On se ramène très facilement au cas où $a = 1$ et $v(b_i) = \beta \neq 0$ (les b_i sont conjugués). Si (ii) était faux, on pourrait écrire $\overline{p}$ comme le produit de deux facteurs premiers entre eux. Or les K-automorphismes de K' induisent des $\overline{K}$-isomorphismes de $\overline{K}'$, donc chaque $\overline{b}_i$ est racine des deux facteurs, ce qui contredit que ces facteurs soient premiers entre eux.

(ii)⇒(iii) Il suffit d'écrire f en produit de polynômes irréductibles pour aboutir au résultat.

(iii)⇒(iv), (iv)⇒(v) sont immédiats.

(v)⇒(i) Par contraposée, on peut supposer qu'il existe K' extension galoisienne de K (i.e. normale séparable de degré fini) avec $v_1, \ldots, v_s$ $(s > 1)$ les différentes extensions de v. D'après le premier corollaire au théorème 3, il existe $a \in K'$ avec $v_1(a) = 0$ et $v_j(a) > 0$. On peut de plus supposer que a est laissé fixe par tous les σ tels que $v_1 \circ \sigma = v_1$ (quitte à se placer dans l'extension galoisienne fixée par ces automorphimes). Ainsi pour tout $\sigma \in \mathrm{Gal}(K'|K)$, $\sigma(a) = a$ ou $\sigma(a)$ est dans M_{v_1}. Le polynôme minimal de a est donc de la forme de (v), et n'a pas de racine dans K (a n'est pas dans K, ayant des valuations différentes par les v_i). □

On montre maintenant que tout corps valué est contenu dans un corps henselien. Plus précisément :

Théorème 6

Soit (K, v) un corps valué. Il existe un corps henselien $(\tilde{K}, \tilde{v})$ extension algébrique de (K, v) tel que pour tout autre extension algébrique henselienne (L, w) contenant (K, v), il existe un isomorphisme de $(\widetilde{K}, \widetilde{v})$ dans (L, w). Un tel corps sera appelé une henselisation de (K, v). Une henselisation est une extension normale, unique à isomorphisme près.

Démonstration.- Soit $\widehat{K}$ une clôture algébrique séparable de K et soit G son groupe de Galois sur K. Soit $\widehat{v}$ une valuation de $\widehat{K}$ prolongeant v et définissons :

$$H = \{g \in G | \widehat{v} \circ g = \widehat{v}\} \quad , \quad \widetilde{K} = \widehat{K}^H \quad , \quad \widetilde{v} = \widehat{v}_{|\widetilde{K}}$$

Soit $L \subset \widehat{K}$ une extension algébrique de $\widetilde{K}$. D'après le théorème 4, toute valuation w de L prolongeant $\widetilde{v}$ est de la forme $\widehat{v}_{|L} \circ \sigma = \widehat{v}_{|L}$. On a donc unicité du prolongement et $\widetilde{K}$ est henselien.

Soit L, w une extension henselienne de K, v, que l'on supposera d'abord algébrique séparable, donc $L \subset \widehat{K}$. La valuation de L est donc de la forme $w = \widehat{v} \circ \rho$, $\rho \in \mathrm{Gal}(\widehat{K}|K)$. Comme L est henselien, si $g \in \mathrm{Gal}(\widehat{K}|L)$, $\widehat{v} \circ \rho \circ g = \widehat{v} \circ \rho$ donc $\mathrm{Gal}(\widehat{K}|L) \subset \rho^{-1} H \rho$. Ceci prouve que $\rho^{-1}(K) \subset L$.

Dans le cas général, on remarque que si L est henselien, sa clôture séparable est henselienne. □

Remarque : En particulier, l'henselisation de K a le même groupe de valuation que K, voir [R1]

2 Théories complètes et modèles saturés

Dans cette partie on considére $\mathcal{L}$ un langage quelconque.

2.1 Saturation

Définition 2.1 Soit $\mathcal{M}$ une $\mathcal{L}$-structure et $X \in M^I$. On notera $\mathcal{M}_X$ l'expansion de $\mathcal{M}$ dans le langage $\mathcal{L}_I = \mathcal{L} \cup \{c_i | i \in I\}$ et où c_i est interprété par x_i.

Remarque : Si $X \subset M$, on peut aussi parler de $\mathcal{M}_X$ où on identifie X à l'élément diagonal de M^X. Si β est un ordinal, et $X = (x_\lambda)_{\lambda<\beta}$, on note parfois $(M, x_\lambda)_{\lambda<\beta}$ pour $\mathcal{M}_X$ (en général quand on fait varier β).

Définition 2.2 Soit C un ensemble de variables libres, $\mathcal{M}$ une $\mathcal{L}$-structure.

Un type $\Sigma(C)$ de $\mathcal{M}$ est un ensemble maximal, consistant (i.e. finiment réalisé dans $\mathcal{M}$), de formules à variables libres dans C. On dit qu'un type $\Sigma(C)$ est réalisé dans $\mathcal{M}$ si il existe $a \in M^C$ vérifiant pour tout $\sigma(c_1 \dots c_n) \in \Sigma$, $\mathcal{M} \models \sigma(a_{c_1} \dots a_{c_n})$.

Si C est fini de cardinal n, on parle de n-type.

Remarque : L'hypothèse de maximalité n'est pas essentielle, car tout ensemble consistant de formules peut être inclus dans un ensemble maximal consistant d'après le lemme de Zorn.

Les modèles saturés permettent de réaliser, au sens strict (et non pas finiment), tout type, plus précisément :

Définition 2.3 Soit $\mathcal{M}$ une $\mathcal{L}$-structure et α un cardinal. On dit que $\mathcal{M}$ est un modèle α-saturé si pour tout cardinal $\beta < \alpha$, et pour tout $X \in M^\beta$, $\mathcal{M}_X$ réalise tout 1-type de $\mathcal{M}_X$.

$\mathcal{M}$ est dit saturé si il est $|M|$-saturé.

Proposition 2.1 *Si α est infini, on a les deux propriétés suivantes :*

1) $\mathcal{M}$ est α-saturé si et seulement si pour tout cardinal $\beta < \alpha$, $X \in M^\beta$, $\mathcal{M}_X$ est α-saturé.

2) $\mathcal{M}$ est α-saturé si et seulement si pour tout cardinal $\beta < \alpha$, $X \in M^\beta$, $\mathcal{M}_X$ réalise tout ensemble de formules $\Sigma(C)$ à variables libres dans C et consistant, tel que $|C| \leq \alpha$.

3) Enfin, si $\mathcal{M}$ est α-saturé, et $\mathcal{L}' \subset \mathcal{L}$, alors $\mathcal{M}$ est α-saturé en tant que $\mathcal{L}'$-structure.

Démonstration.- 1)Supposons $\mathcal{M}$ α-saturé. Soit $\beta' < \alpha$ et $Y \in M^{\beta'}$. Alors le cardinal de $\beta + \beta'$ est plus petit que α donc tout 1-type de $\mathcal{M}_{X.Y}$ est réalisé dans $\mathcal{M}$, donc $\mathcal{M}_X$ est α-saturé. La réciproque est évidente.

2) Quitte à l'inclure dans un ensemble maximal consistant, on peut supposer que $\Sigma(C)$ est un type de $\mathcal{M}_X$.

Notons $C = \{c_\lambda\}_{\lambda<\alpha'}$ avec $\alpha' \leq \alpha$, et $C_\gamma = \{c_\lambda\}_{\lambda<\gamma}$. Soit $\Sigma_\gamma = \Sigma \cap \mathcal{L}_{C_\gamma}$ (formules de Σ à variables libres dans C_γ). Alors $\Sigma_0 = \mathrm{Th}(\mathcal{M})$ et $\Sigma_{\alpha'} = \Sigma$.

On va montrer que si Σ_γ est réalisé par Y_γ dans $\mathcal{M}_X$, il existe y_γ tel que $Y_\gamma.y_\gamma$ réalise $\Sigma_{\gamma+1}$. Par induction, ceci permet de conclure.

Comme $\mathcal{M}_{X.Y_\beta}$ est α-saturé, il suffit de montrer que $\Sigma_{\gamma+1}$ est un 1-type de $\mathcal{M}_{X\ .Y_\beta}$. Par compacité, il suffit de voir qu'un sous-ensemble fini de $\Sigma_{\gamma+1}$ est consistant. Par maximalité, en réalisant la conjonction, on peut même se ramener à une seule formule $\sigma(\overline{c}, x_\beta)$.

Comme Σ est maximal consistant, $\exists x\, \sigma(\overline{c}, x)$ est dans Σ donc dans Σ_γ. Par définition de la consistance, on en déduit que σ est consistant donc réalisé dans $\mathcal{M}_{X.Y_\beta}$.

3) C'est évident. □

Les propositions suivantes montrent des propriétés de cardinalité sur les modèles α-saturés.

Proposition 2.2 *1) Si $\mathcal{M}$ est α-saturé et infini, alors $|M| \geq \alpha$.*
2) $\mathcal{M}$ est fini si et seulement si il est α-saturé pour tout α.

Démonstration.- 1) Supposons $\alpha > |M|$. L'ensemble des formules $\Sigma(v) = \{v \neq a\}_{a\in M}$ est réalisable par saturation et complétude (car M est infini) mais pas dans $\mathcal{M}_M$, donc $\mathcal{M}$ n'est pas α-saturé.

2) Il suffit de montrer que si $\mathcal{M}$ est fini et α un cardinal, $\mathcal{M}$ est α-saturé (la réciproque a été prouvée ci-dessus). Or soit $\beta < \alpha$, $A \in M^\beta$ et $\Sigma(v)$ un 1-type de $\mathcal{M}_A$. Si Σ n'était pas réalisé dans $\mathcal{M}$, il existerait pour tout $b \in M$ une formule $\sigma_b \in \Sigma$ telle que $\mathcal{M} \not\models \sigma_b(b)$. Alors la formule $\forall x\, \neg(\bigwedge_b \sigma_b)$ est dans $\mathrm{Th}(\mathcal{M}_A)$, donc $\{\sigma_b(v)\}$ n'est pas consistant, ce qui est contradictoire. □

2.2 Caractérisation des théories complètes

Lemme 2.1 [Lemme du va-et-vient] Soient $\mathcal{M}$ et $\mathcal{M}'$ deux modèles α-saturés élémentairement équivalents, et $\beta \leq \alpha$ un cardinal infini. Soient $X \in M^\beta$ et $Y \in M'^\beta$. Alors il existe $\overline{X} \in M^\beta$ et $\overline{Y} \in M'^\beta$ dont les supports contiennent respectivement ceux de X et Y et tels que $\mathcal{M}_{\overline{X}} \equiv \mathcal{M}'_{\overline{Y}}$

Démonstration.- Soit $Z \in M^\beta$ une énumération de $X \cup Y$. On supposera toujours par symétrie $z_\gamma \in X$. On notera $X_\gamma = (x_\lambda)_{\lambda<\gamma}$. Supposons $\mathcal{M}_{\overline{X}_\gamma} \equiv \mathcal{M}'_{\overline{Y}_\gamma}$ et construisons $\overline{x}_\gamma$ et $\overline{y}_\gamma$ par induction tels que $\mathcal{M}_{\overline{X}_{\gamma+1}} \equiv \mathcal{M}'_{\overline{Y}_{\gamma+1}}$. Soit $\overline{x}_\gamma = z_\gamma$. Alors soit $\Sigma(v)$ l'ensemble des formules satisfaites par $\overline{x}_\gamma$ dans $\mathcal{M}_{X_\gamma}$. Par hypothèse d'induction, il existe $\overline{y}_\gamma$ qui réalise $\Sigma(v)$ dans $\mathcal{M}'_{\overline{Y}_\beta}$.

Ainsi $\mathcal{M}_{\overline{X}_{\beta+1}} \equiv \mathcal{M}'_{\overline{Y}_{\beta+1}}$ et les familles $\overline{X}$ et $\overline{Y}$ satisfont par construction les conditions de l'énoncé du lemme. □

Lemme 2.2 Soit $\mathcal{M}$ une $\mathcal{L}$-structure, α un cardinal. On suppose $|\mathcal{L}| \leq$

$\alpha \leq |M| \leq 2^\alpha$. Alors il existe une extension élémentaire $\mathcal{M}'$ de $\mathcal{M}$ telle que si $X \in M^\beta$, $\beta \leq \alpha$, $\mathcal{M}'$ réalise tout 1-type $\Sigma(v)$ de $\mathcal{M}_X$.

Démonstration.- Comme $|M| \leq 2^\alpha$, il y a au plus 2^α $X \in M^\beta$ $\beta \leq \alpha$. Comme $|\mathcal{L} \cup \{c_x\}_{x \in X}| \leq \alpha$, l'ensemble des formules $F(\mathcal{L} \cup \{c_x\}_{x \in X})$ est de cardinalité inférieure à α également, donc il y a pour chaque X au plus 2^α 1-types. On introduit alors une nouvelle constante $c_{X\Sigma}$ pour chaque $\beta \leq \alpha$, $X \in M^\beta$ et chaque 1-type $\Sigma(v)$. On obtient donc un nouveau langage $\mathcal{L}'$ de cardinalité inférieure à 2^α. Soit la théorie suivante de $\mathcal{L}' \cup \mathcal{L}_M$:

$$T = \bigcup_{\Sigma, X} \Sigma(c_{X\Sigma}) \cup \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$$

Un modèle de T, réduit à $\mathcal{L}$, sera une extension élémentaire de $\mathcal{M}$ qui vérifie la propriété souhaitée.

Il suffit donc de montrer que T est consistante, avec le théorème de compacité. Soit $T' \subset T$ fini. Alors T' ne contient qu'un nombre fini de constantes du type $c_{\Sigma,X}$ notées $c^1, \dots c^n$ correspondant aux formules $\sigma_1 \dots \sigma_n$ et aux ensembles $X^1, \dots X^n$. Quitte à faire des conjonctions, on suppose que les c^i sont deux à deux distincts. Par consistance, chaque Σ est finiment réalisable donc chaque $\sigma(c_i)$ est réalisé dans $\mathcal{M}$. Ainsi T est consistante. □

Lemme 2.3 Soit $\alpha \geq |\mathcal{L}|$ et $\mathcal{M}$ une $\mathcal{L}$-structure de cardinalité $|M| \leq 2^\alpha$ infinie. Il existe une extension élémentaire de $\mathcal{M}$ de cardinalité inférieure à 2^α α^+-saturée.

Démonstration.- On va construire une chaîne d'extensions élémentaires selon le lemme précédent. Définissons par induction $\mathcal{M}_0 = \mathcal{M}$, si $\beta < \alpha^+$, est limite, $\mathcal{M}_\beta = \bigcup_{\gamma<\beta} \mathcal{M}_\gamma$ et pour tout cardinal successeur $\beta+1$, $\mathcal{M}_{\beta+1}$ est une extension élémentaire de $\mathcal{M}_\beta$ construite selon le lemme précédent.

Soit $\mathcal{M}' = \bigcup_{\beta<\alpha^+} \mathcal{M}_\beta$ et $X \in M'^\gamma$, $\gamma \leq \alpha$. Pour tout $\lambda \leq \gamma$, choisissons β_λ tel que $x_\lambda \in M_{\beta_\lambda}$. Comme α^+ est régulier, $\beta = \cup_{\lambda \leq \alpha} \beta_\lambda < 2^\alpha$ (en effet son cardinal est $|\beta| = \sup(|\beta_\lambda|, |\gamma|) \leq \alpha$).

Il s'en suit que $X \in (M_\beta)^\gamma$ et tout 1-type de $\mathcal{M}'_X$ est réalisé dans $\mathcal{M}_{\beta+1}$ donc dans $\mathcal{M}'$. □

Ces lemmes nous conduisent au théorème d'isomorphisme suivant, qui caractérise les théories complètes :

Théorème 7

On suppose l'hypothèse du continu. Soit T une théorie sur un langage dénombrable. Alors T est complète ssi deux modèles saturés de T de cardinalité ω_1 sont isomorphes.

Démonstration.- Supposons T complète. Si $\mathcal{M}$ et $\mathcal{M}'$ sont des modèles saturés de T, ils sont élémentairement équivalents. D'après le lemme, il existe X et Y dont les supports sont respectivement M et M' et tels que $\mathcal{M}_X \equiv \mathcal{M}'_Y$. On en déduit donc un isomorphisme entre $\mathcal{M}$ et $\mathcal{M}'$ en posant $f(x_\lambda) = y_\lambda$.

Réciproquement, supposons T non-complète. Alors elle admet deux modèles dénombrables $\mathcal{M}$ et $\mathcal{M}'$ non élémentairement équivalents. Or d'après ce qui précède, il existe $\tilde{\mathcal{M}} \equiv \mathcal{M}$ et $\tilde{\mathcal{M}}' \equiv \mathcal{M}'$ des modèles saturés de cardinalité ω_1, qui ne sont donc pas élémentairement équivalents, donc encore moins isomorphes. □

3 Théorie des modèles des corps valués

L'objectif de cette section est de démontrer le théorème suivant :

Théorème 8 (Ax-Kochen-Ershov)

Soient F, G deux corps valués henseliens. On suppose $\overline{F}$ de caractéristique nulle et $\overline{F} \equiv \overline{G}$, $v(F) \equiv v(G)$. Alors $F \equiv G$.

On supposera l'hypothèse du continu, il suffit alors pour démontrer ce résultat de supposer F et G saturés de cardinalité ω_1 et de montrer que $F \simeq G$

L'idée de la preuve, d'après [CK], est la suivante :

On plonge les corps résiduels $\overline{F}$ et $\overline{G}$ dans F et G respectivement, et on en déduit un isomorphisme $f_0 : F_0 \simeq G_0$ entre des sous-corps valués de F et G. Puis on construit deux suites croissantes d'isomorphismes de sous-corps valués de F et G tels que $f_\alpha : F_\alpha \simeq G_\alpha$ et $F = \bigcup_\alpha F_\alpha$, $G = \bigcup_\alpha G_\alpha$.

Remarque : On suppose donc l'hypothèse du continu dans cette preuve. Le résultat en est indépendant, mais celle-ci permet d'alléger la preuve, en se ramenant à démontrer l'existence d'un isomorphisme.

3.1 Résultats préliminaires

3.1.1 Langage des corps valués

Soit $\mathcal{L}_0 =< 0, 1, +, ., -, ^{-1} >$ le langage des corps, $\mathcal{A}$ l'ensemble des axiomes des corps dans ce langage (on prend généralement la convention $0^{-1} = 0$).

Le langage le plus économique pour décrire un corps valué est le langage $\mathcal{L}_1 = \mathcal{L}_0 \cup \{A\}$, où A est un symbole de prédicat représentant l'anneau de valuation. On travaillera pour la suite dans ce langage canonique.

Les axiomes de la théorie des corps valués dans ce langage sont :

$$\mathcal{A}_v = \mathcal{A} \cup \{-1 \in A\} \cup \{\forall x, y \in A(x.y \in A \wedge x+y \in A))\} \cup \{\forall x(x \in A \vee x^{-1} \in A)))\}$$

La proposition 1.2 de la partie 1 montre que les modèles de $\mathcal{A}_v$ sont des corps valués d'anneau A.

Soit ϕ_n l'énoncé :

$$\begin{array}{lll} \forall a_1 \in A \ldots \forall a_n \in A & (\exists y & ((y^n + a_1 y^{n-1} + \ldots a_n)^{-1} \notin A \\ & & \wedge (n y^{n-1} + (n-1) a_1 y^{n-2} + \ldots a_{n-1})^{-1} \in A - \{0\}) \\ & \Rightarrow \exists x & (x^n + a_1 x^{n-1} + \ldots a_n) = 0) \end{array}$$

Les axiomes de la théorie des corps valués henséliens sont :

$$\mathcal{A}_h = \mathcal{A}_v \cup \{\phi_n\}_{n>0}$$

On peut définir le langage plus intuitif $\mathcal{L}_2 = \mathcal{L} \cup \{v, \leq, V, \phi, \overline{K}\}$ qui précise la valuation v, le groupe de valuation $(V, \leq)$, le corps résiduel $\overline{K}$ et la surjection canonique ϕ. On va montrer rapidement que dans ce langage, apparemment plus riche, toute formule sur les corps valués est équivalente à une formule de $\mathcal{L}_1$, et réciproquement :

- $x \in A$ est équivalent à $v(1) \leq v(x)$
- $v(x) \leq v(y)$ s'exprime par $y/x \in A$
- L'égalité de deux éléments dans V revient à dire que le rapport de leurs antécédents est inversible dans A
- Une égalité $\overline{x} = \overline{y}$ dans $\overline{K}$ est équivalente à $x - y = 0$ ou $(x-y)^{-1} \notin A$.

En particulier, la théorie du corps résiduel et du groupe de valuation (dans les langages respectifs des anneaux et des groupes ordonnés) peut s'exprimer sous forme d'axiomes du premier ordre dans $\mathcal{L}_1$. *Ainsi, le corps résiduel et le groupe de valuation d'un corps valué ont au moins la même saturation que celui-ci.*

3.1.2 Plongement du corps résiduel

Proposition 3.1 *Soit K un corps hensélien, de corps résiduel de caractéristique nulle. Alors il existe un sous-corps K_0 de K et inclus dans A_v tel que la surjection canonique ϕ induise un isomorphisme $\phi : K_0 \simeq \overline{K}$.*

Remarque : L'exemple de $\mathbb{Q}_p$, dont le corps résiduel n'a pas la même caractéristique, montre qu'il n'est pas toujours possible de plonger $\overline{K}$ dans K.

Démonstration.- Si $\overline{K}$ est de caractéristique nulle, alors v est nulle sur $\mathbb{Z}$ donc $\mathbb{Q} \subset A_v$, et on en déduit que la famille $\{k \subset A_v | k \to \overline{k}$ isomorphisme$\}$ contient $\mathbb{Q}$. Ordonnée par inclusion, elle est naturellement inductive. Soit K_0 un élément maximal d'après le lemme de Zorn. On va prouver que $\overline{K_0} = \overline{K}$. Soit $x \in A_v$, $v(x) = 0$. Supposons par l'absurde $\overline{x} \notin \overline{K_0}$ et cherchons à contredire la maximalité de $\overline{K_0}$.

Si $\overline{x}$ est transcendant sur $\overline{K_0}$, x est transcendant sur K_0 donc $K_0(x) \simeq \overline{K_0}(\overline{x}) \subset A_v$ car $v(x) = 0$.

Sinon, soit P un polynôme de K_0 tel que $\overline{P}$ est le polynôme minimal de $\overline{x}$ sur $\overline{K_0}$. Il s'agit ici de trouver un élément y de A_v, $\overline{y} = \overline{x}$ et P polynôme minimal de y sur K_0. Comme $\overline{K}$ est de caractéristique nulle, $\overline{x}$ est racine simple de $\overline{P}$. D'après le lemme de Hensel, il existe $y \in K$, $\overline{y} = \overline{x}$, tel que $P(y) = 0$. Soit Q le polynôme minimal de y sur K_0 Q divise P, et $\overline{Q}$ annule $\overline{x}$ donc $\deg Q \geq \deg P$ et $Q = P$. C'est ce qu'il fallait démontrer. □

3.1.3 Cross-sections

Définition 3.1 Soit (K, v) un corps valué, de groupe de valuation Γ. Une cross-section est une section s de la suite exacte :

$$0 \to U \to K^* \to \Gamma \to 0$$

où U désigne le groupe des unités de A_v.

Si une telle section existe, le groupe de valuation peut être identifié à un sous-groupe de K^* supplémentaire de U. La question de l'existence d'une section est donc celle de l'existence de supplémentaires dans un groupe sans torsion.

Définition 3.2 Un sous-groupe A de B est dit **pur** *si pour tout $a \in A$ et pour tout $n \in \mathbb{Z}$, n divise a dans B ssi n divise a dans A.*

Lemme 3.1 Soit B abélien et $A \subset B$ un sous-groupe pur tel que B/A soit de type fini. Alors A admet un supplémentaire.

Démonstration.- Par classification des groupes abéliens de type fini, on peut écrire $B/A = \bigoplus < \overline{z}_i >$, où les $\overline{z}_i$ sont d'ordre fini k_i ou infini et $k_i = 0$. Comme $k_i z_i \in A$ et A pur dans B, il existe $y_i \in A$ tels que $k_i z_i = k_i y_i$. Posons $z'_i = z_i - y_i$. Vérifions que $B = A \oplus \sum < z'_i >$. Comme $\overline{z'_i} = \overline{z}_i$, il faut simplement montrer que $\sum < z'_i > \cap A = 0$. Soit x dans l'intersection ; alors $x = \sum l_i z_i$, et comme $\overline{x} = 0$, k_i divise l_i. Or par définition, $k_i z'_i = 0$ donc $x = 0$. □

Proposition 3.2 *Soit K un corps valué saturé. Alors K admet une cross-section.*

Démonstration.- On va montrer qu'il existe V tel que $K^* = U \oplus V$ et il s'en suivra $v : V \simeq \Gamma$. V sera construit comme le noyau d'une projection sur U, i.e. une application h qui prolonge à K^* l'application identique de U.

Soit $\{x' \mid x \in K^*\}$ un nouvel ensemble de constantes, qui seront interprétées par $h(x)$. On va prouver la consistance d'une théorie qui dit exactement que h est une projection sur U.

Soit plus précisément la théorie suivante (que l'on peut inclure dans un type de K grâce au lemme de Zorn) :

$$T = \{\sum_{K^*} m_x x' = \sum_{U} n_u u \mid m \in \mathbb{N}^{(K^*)}, n \in \mathbb{N}^{(U)}, \sum_{K^*} m_x x = \sum_{U} n_u u\}$$

Par saturation et compacité, il suffit de voir que tout sous-ensemble fini de T est consistant avec la théorie du groupe K^*. Soit $T_0 \subset T$ fini, et $x_1 \dots x_n \in K^*$ tels que seuls les x'_i apparaissent dans T_0.

Alors définissons B le sous-groupe de K^* engendré par les x_i sur U. D'après le lemme précédent, il existe un sous-groupe C de B tel que $U \oplus C = B$. Soit π la projection sur U, alors posons $x'_i = \pi(x_i)$. T_0 est donc réalisé. □

3.2 Démonstration du théorème d'Ax-Kochen-Ershov

Énumérons $F \cup G = \{x_\alpha\}_{\alpha<\omega_1}$. F et G étant supposés saturés, on peut identifier les groupes de valuation à des sous-groupes des groupes multiplicatifs, notés $v(F)$ et $v(G)$, en vertu de ce qui précède.

Appelons $\mathcal{L}$ le langage $\mathcal{L}_1$ enrichi de la section v.

On va construire une suite croissante de $\mathcal{L}$-isomorphismes $(f_\alpha : F_\alpha \simeq G_\alpha)$ vérifiant :

- $x_\beta \in F_\alpha$ (resp. G_α)si $\beta < \alpha$ et $x_\beta \in F$ (resp. G).
- F_α et G_α sous-corps valués algébriquement clos respectivement dans F et G (°).
- $v(F_\alpha)$ et $v(G_\alpha)$ sont dénombrables et en tant que groupes ordonnés :

$$(v(F), x)_{x\in v(F_\alpha)} \equiv (v(G), f_\alpha(x))_{x\in v(F_\alpha)} \quad (*)$$

D'après la proposition 3.1, il existe $F_0 \subset F$ et $G_0 \subset G$ tels que $F_0 \simeq \overline{F} \simeq \overline{G} \simeq G_0$ (l'isomorphisme $\overline{F} \simeq \overline{G}$ provenant de la saturation).

$f_0 : F_0 \simeq G_0$ convient, car $v(F_0) = 0$, et $(v(F), 0)$ et $(v(G), 0)$ sont élémentairement équivalents (car isomorphes par saturation), enfin ces corps sont algébriquement clos dans F : si $x \in F$, $P \in F_0[X]$ polynôme minimal de x, on voit facilement que $v(x) = 0$ (v est nulle sur F_0^*), et en passant modulo M_v on en déduit que P admet une racine dans F_0, donc que $x \in F_0$.

Par induction, supposons $f_\alpha : F_\alpha \simeq G_\alpha$ construit, et construisons $f_{\alpha+1}$. Par symétrie de la construction on pourra toujours supposer que $x_\alpha \in F$.

Si $x = x_\alpha \in F_\alpha$, on prend $f_{\alpha+1} = f_\alpha$. Sinon, par hypothèse d'induction, F_α étant algébriquement clos dans F, x est transcendant sur F_α.

Le lemme suivant nous sera très utile par la suite :

> Lemme 3.2 Soit F_0 un corps henselien d'équicaractéristique nulle avec cross-section, F_1 un sous-corps valué et F_1' sa clôture algébrique dans F_0. On suppose que le corps résiduel de F_1 est le même que celui de F_0 (à isomorphisme canonique près).
>
> Alors $v(F_1')$ est pur dans $v(F)$.
>
> Si de plus $v(F_1) = v(F_1')$, alors F_1' est une henselisation de F_1.
>
> Réciproquement, une henselisation de F_1 a le même groupe de valuation que F_1.

Démonstration.- Si $v(x^n) \in F_1'$, $v(x) \in F_1'$ car le corps F_1' est algébriquement clos.

La deuxième partie du lemme découle du fait qu'un corps henselien d'équicaractéristique nulle n'admet pas d'extension immédiate algébrique.

En effet, posons F_2 une henselisation de F_1, $F_1 \subset F_2 \subset F_1'$, et soit $x \in F_1'$ tel que $v(x) \in v(F_2)$. Alors il existe $a \in F_2$ tel que $v(ax) = 0$. Posons $p(t) = t^n + c_1 t^{n-1} + \ldots + c_n$ le polynôme minimal de ax. Si A désigne l'anneau de valuation de F_2, $p(t) \in A[t]$ (les coefficients sont des fonctions symétriques des conjugués de ax, qui sont tous dans A).

On peut de plus supposer $c_1 = 0$ quitte à remplacer ax par $ax - c_1/n$. Considérons le résidu de p, c'est une puissance d'un polynôme irréductible, mais comme il admet $\overline{x}$ pour racine, il est de la forme $\overline{p}(t) = (t + \overline{a})^n$. Ainsi $\overline{c}_1 = n\overline{a} = 0$ donc comme le corps résiduel est de caractéristique nulle, $\overline{a} = 0$. Par ailleurs $\overline{c}_n = \overline{a}^n = 0$ mais par ailleurs

$v(c_n) = \sum_\sigma v(\sigma x) = nv(x) = 0$ car F_2 henselien. Donc $\overline{c}_n \neq 0$, ce qui constitue une contradiction.

Le dernier point découle de la remarque suivant le théorème 5. □

Remarque : On a prouvé au passage que si K est henselien d'équicaractéristique nulle, K' une extension algébrique de même corps résiduel et $z \in K' - K$, il existe $a \in K$ tel que $v(z-a) \notin v(K)$.

On traitera maintenant successivement deux cas particuliers avant d'expliquer comment construire $F_{\alpha+1}$.

Premier cas : $v(F_\alpha(x)) \subset F_\alpha$.

Lemme 3.3 Dans les hypothèses de ce cas, s'il existe $y \in G$ tel que pour tout $a \in F_\alpha$ $f_\alpha(v(x-a)) = v(y - f_\alpha(a))$, alors f_α peut être étendu à un isomorphisme $f'_\alpha : F_\alpha(x) \simeq G_\alpha(y)$.

Démonstration.- On va naturellement poser $f'_\alpha(x) = y$. Désignons par F' (resp. G') une clôture algébrique de F (resp. G), qui peut être munie d'une valuation prolongeant celle de F (resp. G). Soit aussi F'_α (resp. G'_α) la clôture de F_α (resp. G_α) dans F' (resp. G'). f_α peut donc se prolonger en $f' : F'_\alpha \simeq G'_\alpha$ isomorphisme de corps, mais aussi isomorphisme de corps valués car il y a unicité du prolongement d'une valuation sur une extension algébrique d'un corps henselien. C'est aussi un $\mathcal{L}$-isomorphisme car F'_α et G'_α contiennent leur groupe de valuation d'après le théorème 1.3.

Or pour tous $b \in F_\alpha(x)$ et $z \in F'_\alpha - F_\alpha$, il existe $a \in F_\alpha$ tel que $v(b-a) \neq v(z-a)$ d'après la remarque consécutive au lemme 3.2, puisque $v(b-a) \in v(F_\alpha)$ par hypothèse.

Il suffit de montrer que pour tout polynôme unitaire irréductible $P \in F_\alpha[x]$,

$$v(f_\alpha(P)(y)) = f_\alpha(v(P(x)))$$

Par hypothèse, ceci est vérifié pour les polynômes de degré au plus 1. Si $\deg P \geq 2$, soit $z \in F'_\alpha - F_\alpha$ une racine de P et a tel que $v(x-a) \neq v(z-a)$. Montrons que $v(y - f'(z)) = v(x-z)$. On a comme $v(x-a) \neq v(z-a)$,

$$v(x-z) = v(x-a+a-z) = \min(v(x-a), v(z-a))$$
$$= \min(v(y-f_\alpha(a)), v(f'(a-z))) = v(y - f'(a) + f'(a-z)) = v(y-f'(z))$$

Ainsi ceci prouve que y est transcendant sur G_α et que l'isomorphisme de corps f'_α prolongeant f_α est un isomorphisme de corps valués. □

Pour trouver $y \in G$ vérifiant la propriété du lemme, on utilise la saturation de G. Comme $v(F_\alpha(x))$ est dénombrable, il existe un sous-ensemble $A \subset F_\alpha$ dénombrable tel que pour tout $b \in F_\alpha$ il existe $a \in A$ tel que $v(x-a) = v(x-b)$.

Par saturation, pour trouver y tel que $v(y - f(a)) = v(x-a)$ pour tout $a \in A$, il suffit de montrer cette propriété pour A' fini.

Supposons donc A' fini et $b \in A'$ tel que $c = v(x-b)$ maximale.

On a $v(b-nc-a) \geq \min(v(b-x), v(nc), v(x-a)) = v(x-a)$ et il y a égalité pour tous les n sauf au plus un, sinon $v(x-a) = c$ et $v(c) = v((n-m)c) \geq \min(v(b-nc-a), v(b-mc-a)) > v(c)$. Ainsi pour n assez grand, $y = f_\alpha(b-nc)$ convient.

Il existe donc y tel que si $a \in A$ $v(y - f_\alpha(a)) = v(x - a)$. Si $b \in F_\alpha$, comme le corps résiduel de F_α est le même que celui de $F_\alpha(x)$, il existe b' tel que $v(x-b) < v(x-b')$. On peut supposer $b' \in A$, et ainsi :

$$v(x-b) = \min(v(x-a), v(b'-b)) = \min(v(y-f_\alpha(a)), v(f_\alpha(b-b'))) = v(y-f_\alpha(a))$$

Une fois que l'isomorphisme $f'_\alpha : F_\alpha(x) \simeq G_\alpha(y)$ est obtenu, il peut s'étendre à leurs clôtures algébriques dans F et G, qui sont des henselisations puisque ce sont des extensions henseliennes immédiates, d'après le lemme 3.2.

Soit donc $f_{\alpha+1} : F_{\alpha+1} \simeq G_{\alpha+1}$. Cet isomorphisme vérifie les conditions de l'induction, car $v(F_{\alpha+1}) = v(F_\alpha)$ dans ce cas.

Second cas : $x \in v(F)$

Dans ce cas, la condition sur le groupe de valuation demandera une vérification attentive dans la construction.

Comme $v(F_\alpha)$ est dénombrable, par saturation, il existe $y \in v(G)$ tel que :

$$(v(F), x, a)_{a \in v(F_\alpha)} \equiv (v(G), y, f_\alpha(a))_{a \in v(F_\alpha)}$$

(considérer la théorie de $(v(F), x, a)_{a \in v(F_\alpha)}$ comme un type en x et consistant avec la théorie de $(G, b)_{b \in v(G_\alpha)}$, où G_α est ordonné comme F_α grâce à la bijection f_α).

Soit X le sous groupe de $v(F)$ engendré par $v(F_\alpha)$ et x, et Y le sous groupe de $v(G)$ engendré par $v(G_\alpha)$ et y. Alors X et Y sont dénombrables. On a également $v(F_\alpha(x)) = X$. En effet si $P(t) = c_n t^n + \ldots + c_0$ ($c_i \in F_\alpha$), l'ensemble des $c_i x^i$ admet un minimum absolu, sinon on peut écrire $x^{r-s} = v(c_s c_r^{-1})$, bien que x soit transcendant sur F_α. Donc si $v(c_r x^r)$ minimal, $v(P(x)) = v(c_r) + rv(x) \in X$.

Ainsi $F_\alpha(x)$ et $G_\alpha(y)$ contiennent leurs groupe de valuation et y est transcendant sur G_α ; l'isomorphisme de corps $\tilde{f} : F_\alpha(x) \simeq G_\alpha(y)$ est donc un $\mathcal{L}$-isomorphisme.

Cet isomorphisme peut s'étendre en un $\mathcal{L}$-isomorphisme $f'_\alpha : F'_\alpha \simeq G'_\alpha$ où F'_α et G'_α sont des henselisations de $F_\alpha(x)$ et $G_\alpha(y)$ contenues dans leurs clôtures algébriques respectives dans F et G (puisque celles-ci sont henseliennes, bien que non nécessairement isomorphes). Etant des extensions immédiates, ce sont bien des sous-$\mathcal{L}$-structures de F et G, respectivement.

De plus, $(v(F), c)_{c \in X} \equiv (v(G), \tilde{f'_\alpha}(c))_{c \in X}$ car tout énoncé de $(v(F), c)_{c \in X}$ est équivalent à un énoncé de $(v(F), x, a)_{a \in v(F_\alpha)}$, donc les deux structures sont élémentairement équivalentes car $(v(F), x, a)_{a \in v(F_\alpha)} \equiv (v(G), y, f_\alpha(a))_{a \in v(F_\alpha)}$.

Mieux, si $\overline{X}$ et $\overline{Y}$ sont les sous-groupes purs (dénombrables) engendrés par X et Y dans $v(F)$ et $v(G)$, $(v(F), c)_{c \in \overline{X}} \equiv (v(G), h(c))_{c \in \overline{Y}}$ (où h est l'unique prolongement de $\tilde{f}_{|X}$ à $\overline{X}$) : tout énoncé $\sigma(y')$ sur l'élément $y' = \frac{x'}{n}$, $x' \in X$ est équivalent à l'énoncé $\exists y\, (ny = x' \wedge \sigma(y))$ car le groupe est sans torsion.

Comme $\overline{X}$ et $\overline{Y}$ sont algébriques sur F_α et G_α, les extensions $F''_\alpha = F'_\alpha(\overline{X})$ et $G''_\alpha = G'_\alpha(\overline{Y})$ sont elles aussi algébriques. Ce sont des extension valuées qui contiennent leur groupe de valuation.

Pour étendre f'_α à ces extensions, il suffit de montrer qu'elles sont isomorphes

en tant que corps (par le théorème 5). Soit P à coefficients dans F'_α tel que $P(x_1, \ldots, x_n) = 0$. Montrons que :

$$f'_\alpha(P)(h(x_1), \ldots, h(x_n)) = 0$$

Les x_i sont à coefficient près des racines d'une même puissance de x donc on voit qu'il suffit de travailler avec P à une seule variable (car $(v(F), c)_{c\in\overline{X}} \equiv (v(G), h(c))_{c\in\overline{Y}}$), puis qu'il suffit de calculer le polynôme minimal P d'une racine n-ième de x^k, soit z et montrer que son image par f'_α annule $h(z)$. On va montrer qu'il est de la forme $P(t) = t^m - z^m$. En effet, comme $z^n = x^k$, il est clair que $P(t) = \prod_{i=1}^{n}(t - \zeta_i z)$, où les ζ_i sont des racines n-ièmes de l'unité (dans une extension algébrique de F'_α convenable). Ainsi $P(t) = t^m + c_1 z t^{m-1} + \ldots + c_m z^m$, où les c_i sont des combinaisons symétriques des ζ_i, donc en particulier algébriques sur $\mathbb{Q}$. Comme $z \in F''_\alpha$, $c_i \in F''_\alpha$ aussi et comme v est nulle sur $\mathbb{Q}$, d'après la proposition 1.3, si $c_i \neq 0$, $v(c_i) = 0$ donc $v(c_i z^i) = v(z^i) = z^i$. En particulier, si $c_i \neq 0$, $v(c_i z^i) = v(z^i) = z^i$ donc comme F'_α une $\mathcal{L}$-structure, $z^i \in F'_\alpha$. En particulier le polynôme $t^i - z^i$ annule z dans F'_α, tout en étant de degré inférieur à m le degré de z sur F'_α. On en déduit nécessairement $i = m$ et $P(t) = t^m - z^m$. Il ne reste plus qu'à montrer que $h(z^m) = f_\alpha(z^m)$. Mais comme $z^m \in F'_\alpha$, $v(z^m) \in v(F'_\alpha) = v(F_\alpha(x)) \subset F_\alpha(x)$, et comme x est transcendant sur F_α, z^m est nécessairement une puissance *entière* de x (c'est x^k si on a choisi k et n premiers entre eux). Comme on a justement choisi $f_\alpha(x) = h(x) = y$, on a donc bien $h(z^m) = f_\alpha(z^m)$ et $f_\alpha(P)(h(z)) = 0$.

Ainsi, $v(F''_\alpha)$ et $v(G''_\alpha)$ étant purs dans $v(F)$ et $v(G)$, leurs clôtures algébriques dans F et G sont des henselisations, elles sont donc isomorphes par $f_{\alpha+1} : F_{\alpha+1} \simeq G_{\alpha+1}$. Cet isomorphisme est un $\mathcal{L}$-isomorphisme (car il commute avec v) qui vérifie par construction toutes les conditions souhaitées.

Cas général

Appliquons le second cas particulier afin d'obtenir $f^0 : F^0 \simeq G^0$ prolongeant f_α et vérifiant (°) et (*) avec $v(F_\alpha(x)) \in F^0$. En itérant ce procédé un nombre dénombrable de fois, on en déduit qu'il existe une suite croissante $f^n : F^n \simeq G^n$ d'isomorphismes tels que $v(F^n(x)) \subset v(F^{n+1})$. Posons $F' = \bigcup_{n<\omega} F^n$, $G' = \bigcup_{n<\omega} G^n$. Alors par construction $v(F'(x)) = v(F')$ et l'isomorphisme naturel $f' : F' \simeq G'$ vérifie (°) et (*).

Maintenant, le premier cas, appliqué à f' permet de conclure.

Ainsi, on a construit $f = \bigcup_{\alpha<\omega_1} f_\alpha$ isomorphisme de corps valués entre F et G.

Notation : Pour la suite, on notera $\mathcal{A}_0$ la théorie :

$$\mathcal{A}_0 = \mathcal{A}_h \cup \{v(n) = 0\}_{n>0}$$

Le théorème d'Ax-Kochen-Ershov dit exactement que si T_1 est une théorie complète de corps, et T_2 une théorie complète de groupes ordonnés (exprimés dans $\mathcal{L}_1$), alors $\mathcal{A}_0 \cup T_1 \cup T_2$ est complète (montrer sa consistance relève d'une construction facile).

Exemple : Si k est algébriquement clos, $k((t))$ est élémentairement équi-

valent au corps des germes de fonctions méromorphes au voisinage de 0 sur $\mathbb{C}$.

Corollaire 8 *Soit σ un énoncé dans le langage des corps valués. Alors il existe un ensemble fini de couples (σ_i, τ_i) d'énoncés du langage des corps et des groupes ordonnés (respectivement), tels que pour tout corps K hensélien d'équicaractéristique nulle :*

$$K \models \sigma \text{ si et seulement si il existe } i \text{ tel que } \overline{K} \models \sigma_i \text{ et } \Gamma \models \tau_i$$

Démonstration.- On notera T_V la théorie des corps valués henséliens d'équicaractéristique nulle dans le langage des corps valués.

Soit X l'ensemble des énoncés sur le corps résiduel (dans le langage des corps valués), Y l'ensemble des énoncés sur le groupe de valuation, et Z la clôture de $X \cup Y$ par conjonction et disjonction. On trouvera $\tau \in Z$ équivalent à σ dans T_V. Posons Z_1 l'ensemble des conséquences de σ et T_V dans Z.

On va montrer que Z_1 implique σ dans T_V. En effet, dans le cas contraire, $\{\neg\sigma\} \cup Z_1 \cup T_V$ est consistante, et admet un modèle $\mathcal{M}$. Soit $T = \mathrm{Th}(\mathcal{M}) \cap Z$. D'après le théorème d'Ax-Kochen-Ershov, T est une théorie consistante complète. Donc T démontre $\neg\sigma$ modulo la théorie T_V. Comme T est clos par conjonction, il existe $\tau' \in T$, tel que dans T_V, $\tau' \Rightarrow \neg\sigma$, i.e. $\neg\tau' \in Z_1 \subset T$ ce qui contredit la consistance de T.

Ainsi (en utilisant toujours la clôture par conjonction), il existe une formule τ de Z_1 qui implique σ, donc dans la théorie des corps valués, $\tau \Leftrightarrow \sigma$.

On peut alors montrer que τ est équivalente à une disjonction finie d'énoncés σ_i, τ_i comme dans l'énoncé, ce qui permet de conclure. □

Remarque : Le résultat est faux si on suppose que la caractéristique du corps résiduel est finie.

Ainsi, deux corps d'équicaractéristique $p > 0$ dont corps résiduels et groupe de valuation sont élémentairement équivalents ne le sont pas nécessairement, comme le prouve l'exemple suivant :

Soit F la clôture algébrique de $\mathbb{F}_p$ et $H = F((t))^{\mathbb{Q}}$ l'ensemble des séries à support bien ordonné dans $\mathbb{Q}$ et à coefficients dans F. H est valué henselien (car algébriquement clos) de groupe $\mathbb{Q}$ et de corps résiduel F. Soit aussi $H' = \bigcup_n F((t^{1/n!}))$. H' est un corps henselien (comme réunion de corps henseliens) de mêmes groupe de valuation et corps résiduel que H. Pourtant H' n'est pas algébriquement clos, puisque $\sum t^{1-1/p^n} \notin H'$ est solution de $x^p = t^{p-1}(x-1) \in H'[x]$.

Sous des hypothèses plus fortes que le caractère henselien, on peut toutefois montrer des résultats du même type que le principe d'Ax-Kochen-Ershov pour l'équicaractéristique finie.

Le cas de caractéristique différentes (corps résiduel de caractéristique finie pour un corps de caractéristique nulle) est mentionné à la partie 5 (principe d'Ax-Kochen-Ershov pour les corps formellement p-adiques, théorème 14).

4 Élimination des quantificateurs

On travaille dans cette partie avec le langage $\mathcal{L}_1$ des corps valués.

4.1 Définitions et critère d'élimination des quantificateurs

Définition 4.1 Soit $\mathcal{M}$ une $\mathcal{L}$-structure, et $X \subset M^n$. On dit que X est définissable si il existe une formule à $n+k$ variables libres σ et $\overline{a} \in M^k$ tels que :

$$X = \{\overline{x} \in M^n | \mathcal{M} \models \sigma(\overline{x}, \overline{a})\}$$

X sera dit définissable sans quantificateurs *si on peut de plus choisir σ sans quantificateurs.*

On sait souvent caractériser algébriquement les ensembles définissables sans quantificateurs : ce sont les ensembles constructibles de la topologie de Zariski pour la théorie des corps, les réunions finies d'intervalles pour la théorie des ordres, etc.

Définition 4.2 Une $\mathcal{L}$-structure $\mathcal{M}$ admet l'élimination des quantificateurs si sur $\mathcal{M}$ toute formule est équivalente à une formule sans quantificateurs, en particulier tout ensemble définissable est définissable sans quantificateurs.

Une théorie T admet l'élimination des quantificateurs si tout modèle $\mathcal{M}$ de T admet l'élimination des quantificateurs, en particulier toute formule est équivalente à une formule sans quantificateurs dans T.

Le théorème suivant donne une condition nécessaire et suffisante à l'élimination des quantificateurs.

Théorème 9

Soit T une $\mathcal{L}$-théorie.
T admet l'élimination des quantificateurs si et seulement si quels que soient A $\mathcal{L}$-structure, $\mathcal{M}$, $\mathcal{N}$ modèles de T et $\mathcal{L}$-extensions de A, $\overline{a} \in A^n$ et $\psi(\overline{v}, w)$ formule sans quantificateurs, s'il existe $m \in M$ tel que $\mathcal{M} \models \psi(\overline{a}, m)$, il existe $n \in N$ tel que $\mathcal{N} \models \psi(\overline{a}, n)$.

Démonstration.- Si T admet l'élimination des quantificateurs, la formule $\exists w\, \psi(\overline{v}, w)$ est équivalente à une formule sans quantificateurs, donc la propriété à vérifier est immédiate.

Réciproquement, posons $\phi(\overline{v}) = \exists w\, \psi(\overline{v}, w)$. On peut supposer que $T \cup \{\exists \overline{v}\, \phi(\overline{v})\}$ est consistant (sinon $\phi(\overline{v})$ est T-équivalente à $\overline{v} \neq \overline{v}$), et soit $\Sigma(\overline{v})$ l'ensemble des formules $\sigma(\overline{v})$ sans quantificateurs T-conséquences de $\phi(\overline{v})$ (i.e. telles que T démontre $\forall \overline{v}\, \phi(\overline{v}) \Rightarrow \sigma(\overline{v})$). Soit $\mathcal{L}' = \mathcal{L} \cup \{\overline{c}\}$. On va montrer que $T' = T \cup \Sigma(\overline{c}) \cup \{\neg\phi(\overline{c})\}$ n'est pas consistant

Supposons par l'absurde T' consistante. Il existe $(M, \overline{c})$ modèle de T'. Soit A la sous-$\mathcal{L}$-structure de $\mathcal{M}$ engendrée par $\overline{c}$. Construisons $\mathcal{N}$ contenant A modèle de

$T \cup \{\phi(\overline{c})\}$. Il suffit de voir que $\mathrm{Diag}(A) \cup T \cup \{\phi(\overline{c})\}$ est consistant (où $\mathrm{Diag}(A)$ désigne l'ensemble des formules *sans quantificateurs* satisfaites par A).

$\mathrm{Diag}(A)$ est clos par conjonction, il suffit par compacité de montrer que tout énoncé de $\mathrm{Diag}(A)$ est consistant avec $T \cup \{\phi(\overline{c})\}$. Or A est engendrée par $\overline{c}$, donc tout énoncé du diagramme (simple) de A est équivalent à un énoncé sans quantificateurs sur $\overline{c}$. Or par définition, si $\sigma(\overline{c})$ sans quantificateurs n'est pas consistant avec $T \cup \{\phi(\overline{c})\}$, $\neg\sigma(\overline{c}) \in \Sigma(\overline{c}) \subset \mathrm{Diag}(A)$.

L'existence des deux structures $\mathcal{M}$ et $\mathcal{N}$ constitue une contradiction (l'un réalise $\phi(\overline{v})$, l'autre non). Par compacité et cloture par conjonction, il existe donc $\sigma(\overline{c}) \in \Sigma(\overline{c})$ tel que $T \vdash (\sigma(\overline{c}) \Rightarrow \phi(\overline{c}))$. Par variations des constantes, on a donc :

$$T \vdash \forall \overline{v}\ (\exists w\ \psi(\overline{v}, w) \Leftrightarrow \sigma(\overline{v})$$

On en déduit par induction sur la complexité que toute formule est T-équivalente à une formule sans quantificateurs. Soient $\phi_1(\overline{v})$, $\phi_2(\overline{v})$, $\phi(\overline{v}, w)$ des formules, respectivement T-équivalentes à $\sigma_1(\overline{v})$, $\sigma_2(\overline{v})$, $\sigma(\overline{v}, w)$. Alors :

- $\phi_1(\overline{v}) \wedge \phi_2(\overline{v})$ est T-équivalente à $\sigma_1(\overline{v}) \wedge \sigma_2(\overline{v})$.
- $\neg\phi_1(\overline{v})$ est T-équivalente à $\sigma_1(\overline{v})$.
- $\exists w \phi(\overline{v}, w)$ est T-équivalente à $\exists w \sigma(\overline{v}, w)$ donc à une formule sans quantificateurs.

Donc T admet l'élimination des quantificateurs. □

4.2 Corps valués algébriquement clos

L'objectif de cette section est de prouver que la théorie des corps valués non-trivialement et algébriquement clos admet l'élimination des quantificateurs (corollaire 10.1). Ce résultat peut aussi se déduire de la modèle complétude de la théorie, prouvée par A. Robinson dans [Ro].

Remarquons que les corps valués algébriquement clos de valuation non-triviale sont modèles de la théorie du premier ordre suivante (où $\mathcal{A}_v$ désigne la théorie des corps valués) :

$$T = \mathcal{A}_v \cup \{\exists x\ \neg x \in A\} \cup \{\forall a_1 \ldots \forall a_n\ \exists x\ x^n + a_1 x^{n-1} + \ldots + a_n = 0\}_{n \geq 0}$$

Dans un premier temps, nous allons montrer deux propriétés du corps résiduel et du groupe de valuation d'un corps algébriquement clos.

Lemme 4.1 Soit (K, v) un corps valué algébriquement clos. Alors $\overline{K}$ est algébriquement clos.

Démonstration.- Pour tout $\overline{p}(t) \in \overline{K}[t]$ unitaire non constant, il existe $p(t) \in A_v[t]$ unitaire non constant de résidu $\overline{p}(t)$, admettant une racine dans K donc dans A_v (qui est intégralement clos), donc le résidu de cette racine est racine de $\overline{p}(t)$. □

Lemme 4.2 Soit (K, v) un corps valué algébriquement clos. Alors $v(K)$ est un groupe ordonné divisible.

Démonstration.- Soit $v(x) \in v(K)$. Alors x admet une racine n-ième, soit y. Donc $n(v(y)) = v(x)$, ce qui prouve que $\frac{1}{n}v(x) \in v(K)$ Le groupe $v(K)$ est donc divisible. □

Les résultats d'élimination des quantificateurs découleront du théorème suivant :

Théorème 10

Soient (E, v) un corps valué algébriquement clos, $L \subset E$ un sous-corps algébriquement clos. On suppose que la valuation de L n'est pas triviale.
Soit $\psi(v_1 \dots v_n, w)$ une formule sans quantificateurs et $u_1 \dots u_n \in L$.
On suppose qu'il existe $x \in E$ tel que $E \models \phi(u_1 \dots u_n, x)$.
Alors il existe $y \in L$ tel que $L \models \phi(u_1 \dots u_n, y)$.

Démonstration.- La démonstration se déroule en plusieurs étapes, elle consiste à "approximer" x par un élément de L.

Premières simplifications

Toute formule sur x étant équivalente à une formule sur x^{-1} (car $(x^{-1})^{-1} = x$), on peut supposer que $v(x) \geq 0$.

Il nous faut caractériser les ensembles définis par des formules sans quantificateurs de $\mathcal{L}_1$. En utilisant la forme normale disjonctive, et sachant qu'une disjonction est satisfaite si et seulement si au moins un de ses termes est satisfait, on se ramène au cas où $\phi(u_1 \dots u_n, v)$ est une conjonction de formules atomiques et de négations de formules atomiques. Comme tout terme est une fraction rationnelle en v, il existe des polynômes $P, P_1, \dots, P_k$ et des fractions rationnelles $R_1 \dots R_n$, tous à coefficients dans L, tel que $L \models \psi(u_1 \dots u_n, y)$ si et seulement si les conditions suivantes sont réalisées :

1. $P(y) = 0$
2. $P_i(y) \neq 0$ pour tout $i \in \{1 \dots k\}$
3. $v(R_j(y)) \,\square_j\, 0$ pour tout $j \in \{1 \dots n\}$ (où $\square_j$ désigne soit $\leq$ soit $>$)

On trouvera donc $y \in L$ réalisant ces conditions (sachant que x les satisfait dans E).

Si le polynôme P est non-nul, comme L est algébriquement clos, $x \in L$ et donc $y = x$ convient. On supposera dans la suite que $x \notin L$ et $P = 0$.

Ecrivons $R_j(t) = \lambda_j \prod_{\beta \in L}(t - \beta)^{n^j_\beta}$ ($\lambda_j \in L$). Il est important de voir que $B = \{\beta \in L | \sum_j |n^j_\beta| \neq 0\}$ est *fini*. Quitte à agrandir B en lui adjoignant les racines des P_i, on est donc ramené à trouver $y \in L$ *non dans* B (condition 2) et tel que $v(R_j(y)) \,\square_j\, 0$ pour tout $j \in \{1 \dots n\}$ (condition 3).

Il existe une partition de $B = B_0 \cup B_+ \cup B_-$ avec $B_0 = \{\beta \in B | v(\beta) = v(x)\}$, $B_+ = \{\beta \in B | v(\beta) > v(x)\}$, $B_- = \{\beta \in B | v(\beta) < v(x)\}$. Comme on a supposé $v(L)$ non-trivial et $v(x) \geq 0$, quitte à rajouter à B un élément de valuation strictement négative, on peut supposer que $B_- \neq \emptyset$.

Premier cas : $B_0 = B_+ = \emptyset$.

Alors pour tout j, $v(R_j(x)) = v(\lambda_j) + \sum_\beta n^j_\beta v(\beta)$. Soit $\mu = \max v(B_-) \in v(L)$ et soit $y \in L$ tel que $v(y) > \mu$. Alors de même $v(R_j(y)) = v(\lambda_j) + \sum_\beta n^j_\beta v(\beta) = v(R_j(x))$ donc y convient.

Second cas : $B_+ \neq \emptyset$ et $B_0 = \emptyset$.

Soit Y l'ensemble des $y \in L$ tels que $\max v(B_-) < v(z) < v(\min B_+)$. Sur Y, les conditions $v(R_j(y)) \,\square_j\, 0$ sont équivalentes à :

$$\sum_{\beta \in B_+} n_\beta^j v(x) \,\square_j\, - \sum_{\beta \in B_-} n_\beta^j v(\beta) - v(\lambda_j)$$

On définit ainsi un intervalle de $v(E)$ à extrêmités dans $v(L)$, soit I. Posons aussi $\mu = \max B_-$ et $\nu = \min B_+$. Soit $I' = I \cap]\mu, \nu[\cap [0, +\infty[$. Si $v(y) \in I'$ et $y \in L$, y convient. Mais I' est à extrêmités dans $v(L)$, de la forme $(v(a), v(b))$, et $v(x) \in I'$, donc $v(a) \leq v(x) \leq v(b)$. Si $y = \sqrt{ab} \in L$, $v(y)$ est donc dans I', et convient donc (la densité de $v(L)$ suffit pour montrer que $v(L) \cap I' \neq 0$).

Troisième cas : $B_0 \neq \emptyset$ et pour tout $\beta \in B_0$, $v(x - \beta) \in v(L)$.

Soit $\alpha = \max_{\beta \in B_0} v(x - \beta) \in v(L)$, β_0 en lequel ce maximum est atteint, et $u \in L$ tel que $v(u) = \alpha$. Le corps résiduel de L étant algébriquement clos donc infini, on peut trouver z dans l'anneau de valuation de L dont le résidu soit différent des résidus de $(\beta - \beta_0)u^{-1})$, pour les $\beta \in B_0$ tels que $v(x - \beta) = \alpha)$. Posons $y = \beta_0 + uz \in L$ et vérifions $v(x - \beta) = v(y - \beta)$ pour tout $\beta \in B$:

- Si $\beta \in B_+ \cup B_-$, il est clair que $v(y - \beta) = v(x - \beta)$.
- Si $\beta \in B_0$ et $v(x - \beta) < \alpha$, $v(y - \beta) = v(\beta_0 - x + uz + x - \beta) = v(x - \beta)$.
- Si au contraire $\beta \in B_0$ et $v(x - \beta) = \alpha = v(x - \beta_0)$, alors $v(y - \beta) = v(uz + \beta_0 - \beta) = v(u) + v(z - (\beta - \beta_0)u^{-1}) = v(u) = v(x - \beta)$ car le résidu de z est par construction différent du résidu de $(\beta - \beta_0)u^{-1}$, donc $v(z - (\beta - \beta_0)u^{-1}) = 0$.

Quatrième cas : $B_0 \neq \emptyset$ et il existe $\beta_0 \in B_0$, $v(x - \beta_0) \notin v(L)$.

On peut remarquer que $v(x - \beta_0)$ est maximale parmi les $\{v(x - \beta)\}_{\beta \in B_0}$. En effet, $v(x - \beta) = v(x - \beta_0 - (\beta - \beta_0))$ donc si $v(x - \beta) > v(x - \beta_0)$, c'est que $v(x - \beta_0) = v(\beta - \beta_0) \in v(L)$, ce qui est absurde.

Notons $B_* = \{\beta \in B_0 | v(x - \beta) < v(x - \beta_0)\}$. On vient de montrer que si $\beta \in B_*$, $v(x - \beta) \in v(L)$. De plus on peut toujours supposer que $B*$ est non vide, quitte à ajouter $u\beta_0$ à B, avec $v(u) = 0$ et $u \neq 1$ (par infinité du corps résiduel). Soit $\gamma = \max_{\beta \in B_*} v(x - \beta) \in v(L)$ et $\alpha = v(x - \beta_0)$. Alors $\gamma < \alpha$.

On va chercher y de la forme $y(u, z) = \beta_0 + uz$, avec $z \in L$, $v(z) > \gamma$ suffisamment proche de $v(x - \beta_0)$, et $u \in L$ tel que $v(u) = 0$. Si $v(z) > \gamma \geq v(x)$, on a $v(x - \beta) = v(y - \beta) \in v(L)$ pour tout $\beta \in B_+ \cup B_- \cup B_*$. Si $v(z) \leq \delta = \min_{v(x-\beta)=\alpha} v(\beta - \beta_0)$, alors $v(y - \beta) = v(z)$ pour une infinité de u, comme dans le troisième cas. De la même façon que dans le second cas, les conditions $R_j(y) \,\square_j\, 0$ définissent un intervalle de $v(E)$ auquel il faut et il suffit qu'appartienne $v(z) \in]\gamma, \delta]$, et cet intervalle intersecté avec $]\gamma, \delta]$ est non-vide car il contient $v(x - \beta_0)$. On choisit $z \in L$ tel que $v(z)$ soit dans cet intervalle, puis $u \in L$ tel que $v(y - \beta) = v(z)$ pour tout β tel que $v(x - \beta) = \alpha$.

Cette démonstration se comprend particulièrement bien si l'on considère que L et E sont des corps de séries formelles. □

Corollaire 10.1 *La théorie des corps valués algébriquement clos de valuation non-triviale T admet l'élimination des quantificateurs.*

Démonstration.- On utilise la caractérisation de l'élimination des quantificateurs du théorème 9. Soient (F, v) et (G, v') deux corps valués algébriquement clos contenant un même sous-corps K (c'est à dire une sous-$\mathcal{L}_1$-structure). Soit aussi $\psi(v_1 \dots v_n, w)$ une formule sans quantificateurs et $u_1 \dots u_n \in K$. Supposons qu'il existe $x \in F$ tel que $F \models \phi(u_1 \dots u_n, x)$.

Si la valuation de K n'est pas triviale, d'après le théorème 10, il existe y dans la cloture algébrique L de K dans F tel que $L \models \psi(u_1 \dots u_n, y)$.

Or L est isomorphe à la cloture algébrique L' de K dans G (qui est algébriquement clos) en tant que corps, donc en tant que corps valué d'après le théorème 5, donc il existe $y' \in L' \subset G$ qui satisfait la même formule que x,

Si la valuation est triviale sur K, il existe un élément $a \in F - K$ et un élément $b \in G - K$ tels que $v(a) > 0$ et $v'(b) > 0$. $K(a) \subset F$ et $K(b) \subset G$ sont naturellement isomorphes en tant que corps valués. De plus, d'après le théorème 10, il existe y dans la clôture algébrique L de $K(a)$ dans F tel que $L \models \psi(u_1 \dots u_n, y)$. De la même façon que précédemment, L est isomorphe à la clôture algébrique de $K(b)$ dans G, donc il existe $y' \in L' \subset G$ tel que $L' \models \psi(u_1 \dots u_n, y')$ donc comme ψ est sans quantificateurs, $G \models \psi(u_1 \dots u_n, y')$.

On a donc prouvé que la théorie des corps valués algébriquement clos admettait l'élimination des quantificateurs. □

Ce résultat, antérieur au principe d'Ax-Kochen-Ershov, ne présente pas de restriction liée à la caractéristique. On peut obtenir un nouveau résultat de complétude en ajoutant des hypothèses sur celle-ci :

Corollaire 10.2 *Si on fixe la caractéristique ainsi que celle du corps résiduel, la théorie T est complète.*

Démonstration.- Soient F et G deux modèles de T qui de plus ont même caractéristique et même caractéristique résiduelle.

Plaçons nous d'abord dans la situation d'équicaractéristique. Soit K le sous-corps premier de F, K' celui de G. $K = K' = \mathbb{Q}$ ou $\mathbb{F}_p$ à isomorphisme près. Par ailleurs il existe, respectivement dans F et dans G, a et b de valuation strictement positive, tels que $K(a)$ est isomorphe $K'(b)$. On en déduit un isomorphisme entre L et L' leurs clotures algébriques respectives. Soit ϕ un énoncé de $\mathcal{L}_1$, que l'on peut supposer sans quantificateurs d'après le corollaire précédent. Alors $F \models \phi$ ssi $L \models \phi$ ssi $L' \models \phi$ ssi $G \models \phi$. Donc F et G sont élémentairement équivalents.

Le cas où F est de caractéristique nulle et de caractéristique résiduelle p non-nulle est un peu différent. On note toujours K et K' les sous-corps premiers respectifs de F et de G, ils sont isomorphes (en tant que corps) à $\mathbb{Q}$. Or la seule valuation de $\mathbb{Q}$ dont le corps résiduel soit de caractéristique p est la valuation p-adique (vérification immédiate). Donc, si L, L' désignent les clôtures respectives de K dans F et K' dans G, elles sont isomorphes (en tant que corps valués). On conclut comme dans le premier cas. □

Beaucoup d'autres résultats d'élimination des quantificateurs plus difficiles ont été démontrés depuis les années 60, dont date le théorème d'Ax-Kochen-Ershov. Ils font cependant toujours appel à des langages contenant strictement $\mathcal{L}_1$. On montre en effet dans [EQ] que si une théorie de corps valués admet l'élimination des quantificateurs dans $\mathcal{L}_1$, *elle définit nécessairement la classe des corps valués algébriquement clos.*

5 Applications aux corps p-adiques

Les corps des p-adiques $\mathbb{Q}_p$ donnent lieu à un grand nombre d'applications de la théorie présentée ci-avant, on essaiera d'en présenter quelques unes.

5.1 La conjecture d'Artin

La similitude entre $\mathbb{F}_p((t))$ et $\mathbb{Q}_p$ a donné lieu à des questions de transport de propriétés algébriques de l'un vers l'autre. La conjecture d'Artin dit précisément que la dimension diophantienne de $\mathbb{Q}_p$ (non calculée jusqu'à présent) est égale à celle de $\mathbb{F}_p((t))$.

On verra dans la suite en quoi le théorème d'Ax-Kochen-Ershov permet de formaliser le parallèle entre les propriétés de ces deux ensembles de corps locaux, en particulier dans le cas de la dimension diophantienne.

5.1.1 Dimension diophantienne de $\mathbb{F}_p((t))$

Définition 5.1 Un corps K est de classe $C_i(d)$ si tout polynôme homogène de degré d à $n > d^i$ variables présente un zéro non-trivial.

La dimension diophantienne d'ordre d d'un corps K est la borne inférieure des i tels que $K \in C_i(d)$.

La dimension diophantienne d'un corps K est la borne inférieure des i tels que pour tout d, $K \in C_i(d)$.

Théorème 11

Pour tout $d \geq 2$, $\mathbb{F}_p((t)) \in C_2(d)$.

Démonstration.- Cela résulte du lemme suivant :

Lemme 5.1 [Théorème de Chevalley-Warning] Soient $q = p^r$, et (P_i) une famille finie de polynômes à n variables sur $\mathbb{F}_q$, tels que $\sum \deg P_i < n$. Soit X l'ensemble des zéros communs aux P_i dans $(\mathbb{F}_q)^n$. Alors p divise $|X|$.

Posons $Q = \prod(1-(P_i)^{q-1})$. Alors Q est la fonction caractéristique de X et modulo p, $|X| = \sum_{x\in(\mathbb{F}_q)^n} Q(x)$.

Q est de degré inférieur (strictement) à $n(q-1)$ donc il est combinaison linéaire de monômes $x_1^{\alpha_1}\dots x_n^{\alpha_n}$ où pour ou moins un i, $\alpha_i < q-1$.

On va prouver que pour $\alpha < q-1$ $S_\alpha = \sum_{x\in\mathbb{F}_q} x^\alpha = 0$, ce qui permettra de conclure en observant que $\sum_{x\in(\mathbb{F}_q)^n} x_1^{\alpha_1}\dots x_n^{\alpha_n} = S_{\alpha_1}\dots S_{\alpha_n}$.

Pour $\alpha = 0$, le résultat est évident. Sinon, comme le groupe $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$, il existe $y \in \mathbb{F}_q^*$ tel que $y^\alpha \neq 1$. Ainsi $S_\alpha = \sum x \in \mathbb{F}_q^* yx = yS_\alpha$ d'où $S_\alpha = 0$.

Soit maintenant $P(x)$ un polynôme homogène à $n > d^2$ variables de $\mathbb{F}_p((t))[x]$. En multipliant par une puissance de t, on se ramène à $P(x) \in F_p[[t]][x]$. Écrivons $P(x) = P_0(x) + tP_1(x) + \dots$ et soit pour tout k $P_{(k)} = \sum_0^k P_i$. On va prouver que pour tout k il existe une racine de $P_{(k)}$ dans $\mathbb{F}_p[t]$. Écrivons :

$$P_{(k)}(x_0 + tx_1 + \ldots + t_m x_m) = \sum_0^{k+dm} Q_i(x_0 \ldots x_m)$$

Chaque x_i représente un n-vecteur de $\mathbb{F}_p$, chaque Q_i est de degré au plus d.

Pour appliquer le théorème de Chevalley-Warning, il suffit donc que $d(k+dm) < nm$ soit $d^2(1+\frac{k}{dm}) < n$, ce qui est vrai pour m assez grand.

On en déduit l'existence d'une suite $(y_i) \in (\mathbb{F}[[t]]^*)^n$ telle que $v(P(y_i)) \geq i$ pour tout i. P est homogène, on peut donc supposer que pour tout i un des résidus des coordonnées de y_i est non-nul. Comme $F[[t]])^n$ est compact pour la topologie de la valuation, on peut supposer que $y = \lim y_i$ existe. Alors y est non-nul car une de ses coordonnées a un résidu non-nul, et par continuité de P, $P(y) = 0$. □

Remarque : 2 est bien la dimension diophantienne de $\mathbb{F}_p((t))$, pour une preuve de ce résultat voir [R2].

5.1.2 Conjecture d'Artin sur $\mathbb{Q}_p$

On démontre dans cette section le résultat suivant :

Théorème 12

Soit $d \geq 2$. $\mathbb{Q}_p$ est de classe $C_2(d)$ pour tous p sauf un nombre fini.

On remarque que la classe $C_i(d)$ est définissable par un énoncé du premier ordre. En effet dire que tout polynôme homogène vérifiant $n > d^i$ a un zéro non-trivial est équivalent à dire que tout polynôme homogène de degré $n_0 = E(d^i) + 1$ a un zéro non-trivial. Désignons par $N_1 \ldots N_K$ les multientiers de poids d. $K \in C_i(d)$ si et seulement si :

$$K \models \forall a_{N_1} \ldots \forall a_{N_K}\, \exists x_1 \ldots \exists x_{n_0}\, (\bigvee_1^{n_0} x_{n_i} \neq 0) \wedge (\sum_1^K a_{N_k} x^{N_k} = 0)$$

Le théorème résulte en fait du résultat plus général suivant :

Théorème 13

Soit σ un énoncé du premier ordre, alors $\mathbb{F}_p((t)) \models \sigma$ ssi $\mathbb{Q}_p \models \sigma$ sauf pour un nombre fini de p, dépendant de σ.

Démonstration.- D'après le corollaire 8.**1**, il existe σ_i des énoncés sur le groupe de valuation et τ_i des énoncés sur le corps résiduel, tels que dans la théorie des corps valués henséliens d'équicaractéristique nulle, $(\sigma \Leftrightarrow \bigvee_i(\sigma_i \wedge \tau_i))$. Mais une preuve formelle n'utilise qu'un nombre fini des axiomes de la caractéristique nulle du corps résiduel, donc cette équivalence est vraie pour tout corps valué henselien dont le corps résiduel a caractéristique assez grande. Par ailleurs, $\mathbb{F}_p((t))$ et $\mathbb{Q}_p$ ont même corps résiduel et groupe de valuation, donc $\mathbb{F}_p((t)) \models \bigvee_i(\sigma_i \wedge \tau_i)$ ssi $\mathbb{Q}_p \models \bigvee_i(\sigma_i \wedge \tau_i)$. Ainsi pour p assez grand, $\mathbb{F}_p((t)) \models \sigma$ ssi $\mathbb{Q}_p \models \sigma$. □

Ainsi, pour tout d, il existe un ensemble fini X_d tel que $\mathbb{Q}_p$ soit de classe $C_2(d)$ si $p \notin X_d$. On sait peut de choses sur les ensembles X_d, mais il s'avère toutefois que les dimensions diophantiennes de tous les $\mathbb{Q}_p$ sont strictement supérieures à 2.

Dans la suite de cette partie, en raison notamment de la similitude de certains avec ce qui précède, on ne présentera plus de démonstration rigoureuse des faits énoncés.

Les résultats énoncés montrent la grande similitude algébrique entre les corps formellement p-adiques et les corps réels clos : complétude, nullstellensatz, élimination des quantificateurs, et similitude topologique des ensembles définissables.

5.2 Corps formellement p-adiques

Définition 5.2 Un corps henselien de caractéristique nulle et dit formellement p-adique si son groupe de valuation est élémentairement équivalent à $\mathbb{Z}$ et si son corps résiduel est fini.

Exemple : Toute extension de degré fini de $\mathbb{Q}_p$ est formellement p-adique.

Remarque : La classe des corps formellement p-adiques de corps résiduel fixé $\mathbb{F}_q$ est axiomatisable, par la théorie suivante :

$$\begin{aligned} T_q = \quad & \mathcal{A}_h \\ \cup \quad & \{\exists u_1 \dots \exists u_q((\textstyle\bigwedge_1^q (u_i \in A \wedge u_i^{-1} \in A)) \\ & \qquad \wedge \forall x((x \in A \wedge x^{-1} \in A) \Rightarrow (\textstyle\bigvee_1^q (x - u_i)^{-1} \notin A - \{0\}))))\} \\ \cup \quad & \{\exists y\, ((y \notin A \wedge \forall x(x \notin A \Rightarrow yx^{-1} \in A)) \\ & \qquad \wedge \forall x \exists z \exists r(x = z^n r \wedge r \in A \wedge ry^n \notin A))\}_{n>0} \end{aligned}$$

Principe d'Ax-Kochen-Ershov pour les corps formellement p-adiques

La version du théorème d'Ax-Kochen-Ershov portait sur les corps henseliens d'équicaractéristique nulle. Il n'existe pas de résultat général sur les autres configurations entre les caractéristiques du corps et du corps résiduel.

Pour les corps formellement p-adiques, on dispose cependant du théorème suivant :

Théorème 14

Soient F, G deux corps valués henseliens. On suppose $\overline{F}$ **fini** *et $\overline{F} \equiv \overline{G}$, $v(F) \equiv v(G)$. Alors $F \equiv G$. Si de plus $F \subset G$, G est une extension élémentaire.*

Remarques

(i) Dans ce cas, l'élémentaire équivalence entre les corps résiduels se traduit immédiatement par un isomorphisme (deux structures élémentairement équivalentes finies sont isomorphes, puisque saturées).

(ii) Ce résultat montre que la théorie T_q (q fixé) est complète. En particulier, toutes les extensions de $\mathbb{Q}_p$ *de degré résiduel fixé* sont élémentairement équivalentes (à $\mathbb{Q}_p$ si ce degré est 1). Ceci prouve aussi que la théorie de $\mathbb{Q}_p$ est également décidable.

5.3 Nullstellensatz sur $\mathbb{Q}_p$

Il est bien connu que sur un corps réel clos, les fractions rationnelles ne prenant que des valeurs positives sont sommes de carrés, c'est le Nullstellensatz réel.

Par analogie, il est possible de caractériser les fractions rationnelles sur un corps p-adique à valeurs dans l'anneau de valuation.

Définition 5.3 Soit K un corps formellement p-adique d'anneau A. Une fonction entière définie est une fraction rationnelle f de $K(x_1, \ldots, x_n)$, telle que pour tout $(y_1 \ldots y_n) \in K^n$ non pôle de f, $f(y_1, \ldots, y_n) \in A$.

Remarque : Par continuité, il est facile de voir qu'une fonction entière-définie n'a pas de pôle, cela découle aussi du théorème suivant.

Théorème 15

Soit K un corps formellement p-adique d'anneau A. Définissons :

$$\gamma = \frac{1}{p((X^p - X) - (X^p - X)^{-1})}$$

$$R = A[\gamma(K(x_1, \ldots, x_n)] \text{ et } T = \{1 + pr\}_{r \in R}$$

Alors l'anneau R' des fonctions entières définies à n variables est le localisé de R en T, $R' = R_T$

Démonstration.- (D'après [Ch])

Il est très simple de vérifier que $R_T \subset R'$.

La théorie des modèles fournit une démonstration agréable de la réciproque, dont nous présentons informellement les principales étapes.

Comme A est intégralement clos, il en va de même pour R'.

Montrons d'abord que R' est la clôture intégrale de R_T. Cela résulte du fait (admis) que si r n'est pas entier sur R_T, $K(x_1, \ldots, x_n)$ admet une p-valuation v telle que $v(r) < 0$. Ensuite on montre qu'une henselisation L de $K(x_1, \ldots, x_n)$ est un corps formellement p-adique.

D'après le théorème 14, L est une extension élémentaire de K. Or la fonction r est définissable sur K. En particulier, la propriété pour r d'être entière définie sur K se dit par la formule ϕ, à paramètres dans K, suivante :

$$\forall a_1 \ldots \forall a_n \, r(a_1, \ldots, a_n) \in A$$

Comme $K \models \phi$ et que L est une extension élémentaire de K, $L \models \phi$, donc en particulier $v(r(x_1, \ldots, x_n)) \geq 0$. Mais $r(x_1, \ldots, x_n) = r$, et on a choisi $v(r) < 0$, ce qui constitue une contradiction.

Enfin, un argument purement algébrique montre que R_T est intégralement clos, donc $R_T = R'$. □

5.4 Élimination des quantificateurs pour $\mathbb{Q}_p$, applications

Soit $\mathcal{L}_1$ le langage des corps valués, dans lequel on a montré que la théorie des corps algébriquement clos admettait l'élimination des quantificateurs.

On sait qu'il n'existe pas d'autre théorie qui admette l'élimination des quantificateurs dans $\mathcal{L}_1$. En rajoutant un nombre dénombrable d'autres prédicats (définissables dans $\mathcal{L}_1$ avec quantificateurs), on peut prouver une élimination des quantificateurs pour les corps p-adiques.

Soit $\mathcal{L}_Q = \mathcal{L}_1 \cup \{P_n\}_{n>1}$. $\mathbb{Q}_p$ est une $\mathcal{L}_Q$-structure, si chaque P_n représente l'ensemble des racines n-ièmes de $\mathbb{Q}_p^*$.

Macintyre a prouvé dans [Ma] le résultat suivant :

Théorème 16

Dans $\mathcal{L}_Q$, $\mathbb{Q}_p$ admet l'élimination des quantificateurs.

Dans [PR], on démontre le résultat plus général suivant :

Théorème 17

La théorie des corps formellement p-adiques admet l'élimination des quantificateurs.

Corollaire 17 *Tout ensemble définissable infini de $\mathbb{Q}_p$ admet un intérieur non-vide.*

Démonstration.- Un ensemble définissable s'obtenant comme intersection et union finies d'ensembles définis par des formules atomiques ou des négations de formules atomiques, il suffit de s'intéresser aux formules atomiques (ou leurs négations) définissant un ensemble infini. Or pour toute fraction rationnelle R (ayant un nombre fini de pôles que l'on néglige) :

- $R(x) = 0$ définit un ensemble fini tandis que $R(x) \neq 0$ définit un ouvert ;
- $\{R(x) \in A\}$ est ouvert, $\{R(x) \notin A\}$ est ouvert également ;
- $\{R(x) \in P_n\}$ est ouvert (par continuité, car P_n est ouvert). Son complémentaire, privé des zéros de R, est également ouvert.

Une récurrence immédiate montre donc que tout ensemble définissable infini est réunion d'un ouvert non-vide et d'un ensemble fini, donc est d'intérieur non-vide. □

Ceci amène à des développements en intégration p-adique, voir par exemple [De].

6 Conclusion

Les principales applications du théorème d'Ax-Kochen-Ershov et les résultats d'élimination des quantificateurs portent sur les corps p-adiques (ou, un peu plus généralement, les corps formellement p-adiques). C'est que cette classe de corps soulève à la fois des problèmes plus complexes que des classes très générales comme les corps algébriquement clos, tout en étant proche de problèmes intéressants, puisqu'elle est le support de la théorie des nombres.

Historiquement, la notion de valuation est d'abord apparue pour traiter justement des problèmes de théorie des nombres. Il n'est donc pas surprenant d'avoir un nombre important de résultats sur les corps de nombres p-adiques.

Il serait cependant incohérent de subordonner toute la théorie des valuations à la théorie des nombres, de multiples domaines de recherche sont ouverts sur d'autres classes de corps valués, mais dans la plupart des cas la théorie des modèles n'apporte pas des résultats aussi spectaculaires que ceux présentés ici.

Références

[R1] P. Ribenboim, **Théorie des valuations**, Les Presses de l'Université de Montréal, *Montréal 1964*

[R2] P. Ribenboim, **L'Arithmétique des corps**, Hermann, *Paris, 1972*

[CK] C.C. Chang et H.J. Keisler, **Model theory**, North Holland, *Amsterdam, 1973*

[Ch] G. Cherlin, **Model Theoretic Algebra-Selected Topics**, Springer Verlag, *Berlin-Heidelberg-New York 1976, LNM n°521*

[Ro] A. Robinson, **Complete theories**, North-Holland, *Amsterdam,1956*

[EQ] A. Macintyre, K. McKenna, L. Van den Dries, **Elimination of Quantifiers in Algebraic Structures**, Advances in Math. 47, *1983, pp.74-87*

[PR] A. Prestel et P. Roquette, **Formally p-adic fields**, Springer Verlag, *Berlin, 1984, LNM n° 1050*

[Ma] A. Macintyre, **On definable subsets of p-adic fields**, J. Symbolic Logic 41, *1976*

[De] J. Denef, **On the evaluation of certain p-adic integrals**, Séminaire de Théorie des Nombres, *Paris 1983-84*, Progress in Mathematics 59 (1985), 25-47, Birkhäuser.