Cours de M2 - Théorie des Modèles des corps valués
Zoé Chatzidakis, printemps 2008

# 1 Préliminaires algébriques sur les valuations

**1.1. Rappel : groupes ordonnés**. Un *groupe ordonné* est un groupe $(G, *, ^{-1}, e)$ muni d'un ordre total $<$ qui est compatible avec la loi de groupe, c'est-à-dire, si $g < h$ et $u$ sont dans $G$ alors $g * u < h * u$ et $u * g < u * h$. On vérifie facilement qu'un groupe ordonné est sans torsion, et que si $g > 1$ alors $g^{-1} < 1$. [Si $1 < g$, alors, en multipliant par $g$ sur la gauche, on obtient $g < g^2$, puis $g^2 < g^3$, etc. ; de même, en multipliant par $g^{-1}$, on obtient $g^{-1} < 1$.] Si la loi de groupe est commutative, on utilise en général la notation additive : $(G, +, -, 0, <)$.

**1.2. Définition**. Soit $R$ un anneau intègre. Une valuation $v$ sur $R$ est une application $v : R \to \Gamma \cup \{\infty\}$, où $(\Gamma, +, 0, <)$ est un groupe abélien ordonné, satisfaisant, pour tout $a, b \in R$ et $\gamma \in \Gamma$ :

(i) $v(a) = \infty \iff a = 0$.

(ii) $v(a + b) \geq \min\{v(a), v(b)\}$.

(iii) $v(ab) = v(a) + v(b)$.

(iv) $\gamma < \infty$. On pose $\gamma + \infty = \infty$.

Notons que l'on a nécessairement $v(1) = v(-1) = 0$ (car $1 = 1^2 = (1)^2$ et par (iii)), et que la valuation $v$ s'étend de manière unique au corps des fractions $K$ de $R$, en posant $v(a/b) = v(a) - v(b)$ pour $a, b \in R$, $b \neq 0$. Le groupe $v(K^\times)$ est appelé le *groupe de valeurs de* $v$

**1.3. Rappel : entiers, anneaux intégralement clos**. Si $R$ est un anneau intègre, contenu dans un corps $K$, on dit qu'un élément $a \in K$ est *entier* sur $R$ s'il existe un polynôme unitaire $f(T) \in R[T]$ tel que $f(a) = 0$. Cette condition est en fait équivalente à : l'anneau $R[a]$ est un $R$-module de type fini. En effet, en tant que $R$-module, $R[a] = \sum_{i \in \mathbb{N}} Ra^i$ ; il sera de type fini si et seulement s'il existe $n$ tel que $a^n \in \sum_{i=0}^{n-1} Ra^i$, c'est à dire, s'il existe $b_0, \ldots, b_{n-1} \in R$ tels que $a^n = \sum_{i=1}^{n-1} b_i a^i$.

Cela permet par exemple de montrer que si $a$ est entier sur $R$ et $b$ est entier sur $R[a]$, alors tous les éléments de $R[a, b]$ sont entiers sur $R$.

Par contre on voit bien que $1/2$ n'est pas entier sur $\mathbb{Z}$ : $\mathbb{Z}[1/2] = \sum_{i \in \mathbb{N}} \mathbb{Z}2^{-i}$, et $\mathbb{Z}2^{-(i+1)}$ contient proprement $\mathbb{Z}2^{-i}$.

**1.4. Quelques propriétés faciles**. Soit $(K, v)$ un corps valué.

(1) $v(1) = v(-1) = 0$. Si $v(a) < v(b)$ alors $v(a + b) = v(a)$.

(1') Si $v(a_1 + \cdots + a_n) > \min\{v(a_i) \mid 1 \leq i \leq n\}$ alors il existe $i \neq j$ tels que $v(a_i) = v(a_j)$. Cette condition est en particulier vérifiée si $\sum a_i = 0$ et les $a_i$ ne sont pas tous nuls.

(2) Posons
$$\mathcal{O}_v = \{a \in K \mid v(a) \geq 0\}, \qquad \mathcal{M}_v = \{a \in K \mid v(a) > 0\}.$$
Alors $\mathcal{O}_v$ est un sous-anneau de $K$ (appelé l'*anneau de valuation* de $v$) et $\mathcal{M}_v$ est un idéal maximal de $\mathcal{O}_v$.

(3) On a : si $v(a) \leq v(b)$ alors $b/a \in \mathcal{O}_v$. Les idéaux de $\mathcal{O}_v$ forment une chaine (ordonnée par inclusion), qui est en correspondance avec les segments finaux de $\Gamma^{>0} \cup \{\infty\}$.

(4) L'anneau $\mathcal{O}_v$ est *intégralement clos*, c'est-à-dire, si $a \in K$ est racine d'un polynôme unitaire à coefficients dans $\mathcal{O}_v$, alors $a \in \mathcal{O}_v$.

*Démonstration.* (1) On a $v(1) = v(1^2) = v((-1)^2) = 2v(1) = 2v(-1)$, donc $v(1) = v(-1) = 0$. Pour la deuxième assertion, on a $v(a) = v((a+b) - b) \geq \min\{v(a+b), v(b)\}$, ce qui entraîne que $v(a) = v(a+b)$.

(1') Pour $n = 2$, c'est tout simplement la contraposée du (1). On montre facilement par induction sur $n$ que si $v(a_1) < v(a_2) < \ldots < v(a_n)$ alors $v(\sum a_i) = v(a_1)$.

(2) Par (1) il est clair que $\mathcal{O}_v$ est un anneau, et que $\mathcal{M}_v$ est un idéal de $\mathcal{O}_v$. On remarque que les éléments de $\mathcal{O}_v \setminus \mathcal{M}_v$ sont précisément ceux ayant valuation 0, et que leurs inverses sont dans $\mathcal{O}_v$. $\mathcal{M}_v$ est donc nécessairement maximal.

(3) $v(b/a) = v(b) + v(a^{-1}) = v(b) - v(a) \geq 0$. Si $I$ est un idéal de $\mathcal{O}_v$, soit $C(I) = v(I)$. Notons que si $a \in I$, alors tous les éléments $b$ avec $v(b) \geq v(a)$ sont aussi dans $I$. $C(I)$ est donc un segment final de $\Gamma^{>0} \cup \{\infty\}$, qui détermine complètement $I$, puisque $I = \{a \in \mathcal{O}_v \mid v(a) \in C(I)\}$.

(4) Soit $f(T) = \sum_{i=0}^{n} a_i T^i$ un polynôme sur $\mathcal{O}_v$, avec $a_n = 1$, et supposons $v(a) < 0$. Alors, puisque les $a_i$ sont dans $\mathcal{O}_v$, on a $nv(a) < v(a_i) + iv(a)$ pour $i = 0, \ldots, n-1$. Donc $\min\{v(a_i a^i) \mid i = 0, \ldots, n-1\} > nv(a)$, et $v(f(a)) = nv(a)$. Cela entraîne que $f(a) \neq 0$ : aucun élément de $K \setminus \mathcal{O}_v$ ne peut être entier sur $\mathcal{O}_v$.

**1.5. Valuations équivalentes**. Soit $K$ un corps et $v_1 : K \to \Gamma_i \cup \{\infty\}$, $i = 1, 2$, deux valuations sur $K$. Les valuations $v_1$ et $v_2$ sont *équivalentes* s'il existe un isomorphisme (de groupes ordonnés) $f : v_1(K^\times) \to v_2(K^\times)$ tel que $v_2 = f \circ v_1$. En fait, nous considèrerons toujours les valuations à équivalence près.

**1.6. Définition, notation**. Le corps $\mathcal{O}_v/\mathcal{M}_v$ est appelé le *corps résiduel de $K$ (pour la valuation $v$)*. Je le noterai $k_v$. L'application $\mathcal{O}_v \to k_v$ est appelée l'application *résiduelle* et je la noterai res ou $\mathrm{res}_v$. On pourrait l'étendre à $K$ tout entier en posant $\mathrm{res}\,(K \setminus \mathcal{O}_v) = \infty$, ce qui nous donnerait une *place* sur $K$.

Il arrivera aussi que nous considérions plusieurs corps valués contenus les uns dans les autres, et dans ce cas il sera utile d'utiliser une notation qui précise le corps. Si $(K, v)$ est un corps valué, nous utiliserons donc indifféremment $\mathcal{O}_v$ ou $\mathcal{O}_K$ pour l'anneau de valuation, $\mathcal{M}_v$ ou $\mathcal{M}_K$ pour son idéal maximal, $k_v$ ou $k_K$ pour le corps résiduel, et enfin $\Gamma_v$ ou $\Gamma_K$ dénotera $v(K^\times)$.

**1.7. Quelques exemples connus**

(1) **Les valuations sur** $\mathbb{Q}$. Soit $v$ une valuation sur $\mathbb{Q}$. Alors $\mathcal{O}_v$ contient $\mathbb{Z}$, et $\mathcal{M}_v \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ pour un nombre premier $p$, ou bien (0). Si $\mathcal{M}_v \cap \mathbb{Z} = 0$, cela veut dire que tous les éléments de $\mathbb{Z}$ sont inversibles dans $\mathcal{O}_v$, et donc que $\mathcal{O}_v = \mathbb{Q}$, i.e., la valuation $v$ est triviale sur $\mathbb{Q}$ (la valuation *triviale* sur un corps $K$ est celle ayant comme groupe de valeurs (0)). Supposons maintenant que $\mathcal{M}_v \cap \mathbb{Z} = p\mathbb{Z}$. Cela entraîne que si $a$ est un entier, alors $v(a)$ égale l'exposant de la plus grande puissance de $p$ divisant $a$. Cela nous donne que si $a \in \mathbb{Q}$ s'écrit $p^n r$ où $n \in \mathbb{Z}$, et $r$ est une fraction dont le numérateur et dénominateur sont premiers à $p$, nous avons $v(a) = n$. Le groupe de valeurs de $v$ est donc isomorphe à $\mathbb{Z}$, son corps résiduel à $\mathbb{F}_p$ (le corps à $p$ éléments). La valuation $v$ est appelée la *valuation $p$-adique* sur $\mathbb{Q}$.

(2) **Les valuations sur** $K(t)$. Soit $K$ un corps, $t$ un élément transcendant sur $K$. De la même façon que dans (1), on montre que les valuations sur $K(t)$ dont l'anneau de valuation contient $K[t]$, sont : la valuation triviale ; pour chaque polynôme irréductible unitaire $p(t)$, la valuation $v_{p(t)}$ sur $K(t)$ définie par $v(p(t)) = 1$.

Notons que si $K$ n'est pas algébriquement clos, alors il existe un polynôme $p(t) \in K[t]$ qui est irréducible et de degré $> 1$. Le corps résiduel de la valuation $v_{p(t)}$ sera alors une extension de $K$ (de degré $\deg(p(t))$).

Si $p(t)$ est de degré 1, alors $p(t)$ sera de la forme $t-a$ pour un $a \in K$, et la valuation associée sera aussi parfois notée $v_a$. Il existe aussi une valuation *à l'infini* : celle définie par $v(t^{-1}) = 1$. Son anneau de valuation est $K[t^{-1}]$, et si $f(t) \in K[t]$, alors $v_\infty(f(t)) = \deg(f(t))$.

(3) **Les séries formelles**. Plus généralement, considérons le corps $K((t))$ des séries, dont les éléments sont les séries $\sum_{i \geq i_0} a_i t^i$, où les indices $i_0$ et $i$ sont dans $\mathbb{Z}$. On additionne et multiplie ces séries comme si elles étaient des polynômes en $t, t^{-1}$, c'est-à-dire :

$$\sum_{i \geq i_0} a_i t^i + \sum_{i \geq j_0} b_i t^i = \sum_{i \geq \inf\{i_0, j_0\}} (a_i + b_i) t^i, \qquad \sum_{i \geq i_0} a_i t^i \sum_{i \geq j_0} b_i t^i = \sum_{k \geq i_0 + j_0} \sum_{i+j=k} a_i b_j t^k.$$

On vérifie que c'est bien un anneau. Le produit de deux séries est bien défini, car étant donné un entier $k$, l'ensemble des entiers $i$ et $j$ satisfaisant $i + j = k$, $i \geq i_0$ et $j \geq j_0$, est fini. Si $a_{i_0} \neq 0$, on définit alors $v(\sum_{i \geq i_0} a_i t^i) = i_0$. L'anneau des séries ne faisant intervenir que des puissances non-négatives de $t$ est noté $K[[t]]$. On remarque que si $f \in K[[t]]$ s'écrit $1 - tu$, où $u \in K[[t]]$, alors l'élément

$$g = 1 + (tu) + (tu)^2 + \cdots + (tu)^n + \cdots$$

est dans $K[[t]]$, et de plus $fg = 1$. Tout élément $a$ de $K((t))$ s'écrit $a = c(1-tu)t^{v(a)}$, où $c \in K$ et $u \in K[[t]]$, et aura donc un inverse $(c^{-1}(1-tu)^{-1}t^{-v(a)})$ dans $K((t))$. L'anneau de valuation de $K((t))$ est donc $K[[t]]$, son corps résiduel est $K$.

(4) **Les séries de Puiseux**. Pour chaque $n > 0$ on choisit une racine $n$-ième $t^{1/n}$ de $t$ (dans une clôture algébrique), de telle façon que $(t^{1/mn})^n = t^{1/m}$. On peut alors former le corps $\bigcup_{n \in \mathbb{N}} K((t^{1/n}))$, et y définir une valuation qui prolonge celle de $K((t))$. Ce corps est appelé le corps des séries de *Puiseux* sur $K$. Si $K$ est algébriquement clos de caractéristique 0, alors

$\bigcup_{n\in\mathbb{N}} K((t^{1/n}))$ sera algébriquement clos. Mais ce résultat est faux si la caractéristique de $K$ est positive : si elle égale $p$, alors l'équation $X^p - X = t^{-1}$ n'a pas de solution dans $\bigcup_{n\in\mathbb{N}} K((t^{1/n}))$ (intuitivement, une telle solution devrait s'écrire $\sum_{i>0} t^{1/p^i}$).

**1.8. Définition** Remarquez que dans les exemples 1, 2 et 3, le groupe des valeurs est isomorphe à $\mathbb{Z}$. Dans ce cas, on dira que la valuation est *discrète*. Dans l'exemple 3, la valuation $v$ est *triviale sur* $K$. Dans l'exemple 4, le groupe des valeurs est $\mathbb{Q}$ (on a évidemment $v(t^{1/n}) = 1/n$). Voici un autre exemple, avec un groupe de valeurs quelconque.

Soient $\Gamma$ un groupe abélien ordonné, et $K$ un corps. On considère l'algèbre de groupe $K[\Gamma]$, qui est engendrée par l'ensemble $t^\gamma$, $\gamma \in \Gamma$, soumis aux relations

$$\sum_\gamma c_\gamma t^\gamma \sum_\delta d_\delta t^\delta = \sum_\varepsilon \sum_{\gamma+\delta=\varepsilon} c_\gamma d_\delta t^\varepsilon.$$

Sur $K[\Gamma]$, on définit la valuation par : $v(\sum_\gamma c_\gamma t^\gamma) = \inf\{\gamma \mid c_\gamma \neq 0\}$, puis on étend au corps des fractions $K(\Gamma)$ de $K[\Gamma]$. Le groupe des valeurs est bien sûr $\Gamma$.

**1.9. Valeurs absolues**. Soit $(K, v)$ un corps valué, et supposons que son groupe de valeur $\Gamma$ est archimédien. Il existe donc un plongement de $\Gamma$ dans le (groupe additif ordonné) $\mathbb{R}$, et nous identifierons $\Gamma$ avec un sous-groupe de $\mathbb{R}$. On choisit $r \in \mathbb{R}$, $r > 1$, et on définit alors, pour $a \in K$, $|a|_v = r^{-v(a)}$ (et $|0|_v = 0$). Les propriétés de la valuation $v$ se traduisent alors de la façon suivante :

(i') $|a|_v = 0 \iff a = 0$.

(ii') $|a + b|_v \leq \max\{|a|_v, |b|_v\}$.

(iii') $|ab|_v = |a|_v|b|_v$.

Si $v$ est la valuation $p$-adique sur $\mathbb{Q}$ (ou sur sa complétion $\mathbb{Q}_p$), on prend en général $r = p$ et on obtient la valeur absolue $p$-adique.

**1.10. Un peu de théorie des modèles : le langage à trois sortes**. Dans quel langage allons-nous parler des corps valués? Il en existe plusieurs, qui sont équivalents à bi-interprétabilité près. Le plus simple est le langage des anneaux, augmenté par un prédicat unaire $\mathcal{O}$ pour l'anneau de valuation. Le plus naturel est le langage à trois sortes que nous avons implicitement utilisé pour définir les corps (ou anneaux) valués, et je vais tout d'abord parler de celui-ci.

Les structures que nous considèrerons sont des structures $\mathcal{K} = (K, \Gamma, k)$ à trois sortes, c'est-à-dire, trois univers disjoints, les variables et constantes viennent avec une étiquette de sorte. $K$ est l'univers de la sorte "corps", $\Gamma$ celui de la sorte "groupe" et $k$ celui de la sorte "corps résiduel". Bien évidemment, au corps valué $(K, v)$ nous associerons la structure $(K, \Gamma_v, k_v)$, où $\Gamma_v$ est le groupe de valeurs de $K$. La notation est un peu trompeuse : en fait l'univers de la sorte "groupe" contiendra aussi l'élément $\infty$, qui ne fait pas partie du groupe.

De plus, nous avons dans le langage les symboles usuels de fonctions et constantes pour le corps $K$ (c'est-à-dire, $\{+, -, \cdot, 0, 1\}$), ceux pour le corps $k$, et ceux pour le groupe ordonné $\Gamma$

$(\{+,-,0,<,\infty\})$. Nous avons aussi deux symboles de fonctions : res : $\mathcal{O}_v \to k$ et $v : K \to \Gamma \cup \{\infty\}$, qui sont interprétés par l'application résiduelle et par la valuation.

Il existe une théorie dont les modèles sont exactement ceux provenant d'un corps valué. Ses axiomes sont $\forall\exists$, notez que vous êtes obligés de dire que les applications $v$ et res sont surjectives. Ma définition n'est pas tout à fait correcte, car la fonction res n'est pas partout définie. Si ça vous ennuie, vous pouvez aussi définir res comme prenant la valeur 0 sur $K \setminus \mathcal{O}_v$.

Comme je l'ai dit, chaque variable vient avec une étiquette de sorte; pour être précis, ce serait donc bien d'utiliser des lettres différentes pour des variables de sortes différentes. J'utiliserai des lettres latines pour les variables du corps et du corps résiduel, et des lettres grecques pour celles du groupe de valeurs. En cas de risque de confusion entre les variables des deux corps, je préciserai la sorte : l'énoncé $\forall x \in k\ \exists y \in K\ \mathrm{res}\, y = x \wedge v(y) \geq 0$ exprime que l'application res définit une surjection de $\mathcal{O}_v$ sur $k_v$.

En fait, on peut aussi penser à $\mathcal{K}$ comme à une structure au sens usuel (c'est-à-dire, avec un seul univers) : son univers est la réunion disjointe de $K$, $\Gamma \cup \{\infty\}$ et de $k_v$, et on a trois relations unaires qui définissent respectivement $K$, $\Gamma \cup \{\infty\}$ et $k_v$. Et bien sûr toutes les autres fonctions, relations et constantes introduites ci-dessus. Cela devrait vous convaincre qu'il n'y a aucune différence entre une logique avec 3 sortes, et la logique usuelle du premier ordre.

**1.11. D'autres langages pour les corps valués**. Il existe des langages plus simples dans lesquels on peut étudier les corps valués. Au niveau du pouvoir d'expression, tous ces langages sont équivalents.

Le premier langage est obtenu en ajoutant un prédicat unaire $\mathcal{O}$ au langage des anneaux $\{+,-,\cdot,0,1\}$. Si $K$ est un corps valué avec valuation $v$ et anneau de valuation $\mathcal{O}_v$, le prédicat $\mathcal{O}$ sera interprété par $\mathcal{O}_v$. structures

Le deuxième langage, parfois appelé $\mathcal{L}_{\mathrm{div}}$, est obtenu en ajoutant au langage des anneaux un symbole binaire $|$ (div - abréviation de "divise"), qui est interprété dans la corps valué $(K, v)$ par : $a|b \iff ba^{-1} \in \mathcal{O}_v \iff v(a) \leq v(b)$.

Notons que l'anneau $\mathcal{O}_v$ est définissable dans la $\mathcal{L}_{\mathrm{div}}$-structure $K$, par la formule $1|x$.

Au lieu de s'intéresser aux corps valués, nous pourrions aussi bien regarder les anneaux de valuation : à partir d'un anneau de valuation $\mathcal{O}$, on retrouve bien évidemment son corps des fractions, et donc la structure du corps avec un prédicat pour un sous anneau. Il reste maintenant à montrer que ces langages sont "équivalents".

**1.12. Retrouver le corps valué à partir de l'anneau de valuation**. On va montrer comment, à partir de l'anneau $\mathcal{O}_v$, retrouver le corps $K$ et la valuation $v$. Tout d'abord le corps $K$ : c'est tout simplement le corps des fractions du domaine $\mathcal{O}_v$. Ensuite, $\mathcal{M}_v$ est l'idéal des éléments non inversibles de $\mathcal{O}_v$. Nous connaissons donc déjà $k_v$ : c'est le quotient $\mathcal{O}_v/\mathcal{M}_v$, ainsi que l'application res. Les éléments inversibles de $\mathcal{O}_v$ (c'est-à-dire, $\mathcal{O}_v \setminus \mathcal{M}_v$) forment un sous-groupe multiplicatif de $K^\times$, que nous noterons $\mathcal{O}_v^\times$, et on voit très facilement que le quotient $K^\times/\mathcal{O}_v^\times$ est naturellement isomorphe à $\Gamma$. Nous définissons donc $v : K^\times \to K^\times/\mathcal{O}_v^\times$ comme étant la projection naturelle, et posons $v(a) \leq v(b) \iff ba^{-1} \in \mathcal{O}_v$.

**1.13. Rappels sur les structures définissables**. Soient $\mathcal{L}$ et $\mathcal{L}'$ des langages, $M$ une $\mathcal{L}$-structure et $N$ une $\mathcal{L}'$-structure. On dit que la $\mathcal{L}'$-structure $N$ est *définissable* dans la $\mathcal{L}$-structure

$M$ s'il existe $k$ et un sous-ensemble définissable $S$ de $M^k$ (c'est-à-dire, il existe une $\mathcal{L}$-formule $\varphi(x_1, \ldots, x_k)$ telle que $S$ est l'ensemble des $k$-uplets de $M$ qui satisfont $\varphi$), et une bijection $F : N \to S$ telle que, pour tout entier $n$ :

- Si $R$ est un symbole de relation $n$-aire de $\mathcal{L}'$, alors l'image par $F$ des uplets de $N^n$ qui satisfont $R$ est définissable dans $M$. Nous dénoterons par $R^*$ cet ensemble.
- Si $f$ est un symbole de fonction $n$-aire de $\mathcal{L}'$, alors l'image par $F$ du graphe de $f$ est définissable dans $M$. Nous dénoterons par $f^*$ la fonction $S^n \to S$ dont le graphe est cet ensemble.
- Pour chaque symbole de constante $c$ de $\mathcal{L}'$, le $k$-uplet $F(c)$ est définissable dans $M$.

**1.14. Exercice**. Supposons que $N$ est $\emptyset$-définissable. Montrez que pour toute $\mathcal{L}'$-formule $\varphi(x_1, \ldots, x_n)$ il existe une $\mathcal{L}$-formule $\varphi^*(y_1, \ldots, y_n)$, où les $y_i$ sont des $k$-uplets de variables, et telle que, pour tout $n$-uplet $(a_1, \ldots, a_n)$ de $N$ on a

$$N \models \varphi(a_1, \ldots, a_n) \iff M \models \varphi^*(F(a_1), \ldots, F(a_n)).$$

On prouve d'abord, par induction sur la complexité, que si $t(x_1, \ldots, x_n)$ est un terme du langage $\mathcal{L}'$, alors l'image par $F$ du graphe de $(x_1, \ldots, x_n) \mapsto t(x_1, \ldots, x_n)$, est définissable dans $M$. Puis on montre le résultat pour les formules atomiques, puis pour les formules sans quantificateurs. Ensuite, par induction sur la compléxité des formules, pour les formules arbitraires. La preuve est longue et ennueyeuse, vous pouvez tout simplement le faire pour l'exemple de l'exercice 1.15. Puis vous persuader que c'est vrai en général.

**1.15. Exercice**. Montrez que le corps des complexes $\mathbb{C}$ est définissable dans le corps $\mathbb{R}$.

**1.16. Rappel sur les structures interprétables**. Soient $\mathcal{L}$ et $\mathcal{L}'$ des langages, $M$ une $\mathcal{L}$-structure, $N$ une $\mathcal{L}'$-structure. On dit que $N$ est *interprétable* dans $N$ s'il existe un sous-ensemble définissable $S$ de $M^k$, et un sous-ensemble définissable $E$ de $S^2$ qui définit une relation d'équivalence sur $S$, et une bijection $F$ de $N$ sur l'ensemble des classes d'équivalence de $S$ modulo $E$, tels que :

- pour tout symbole $n$-aire de relation $R$ de $\mathcal{L}'$, l'ensemble des uplets $(a_1, \ldots, a_n)$ de $S^n$ tels que $(F^{-1}(a_1/E), \ldots, F^{-1}(a_n/E)) \in R$, est définissable dans $M$.
- pour tout symbole $n$-aire de fonction $f$ de $\mathcal{L}'$, l'ensemble des uplets $(a_1, \ldots, a_n, b)$ de $S^{n+1}$ tels que $f(F^{-1}(a_1/E), \ldots, F^{-1}(a_n/E)) = F^{-1}(b/E)$ est définissable dans $M$.
- pour tout symbole $c$ de constante de $\mathcal{L}'$, l'ensemble $F(c)$ est définissable dans $M$.

**1.17. Exercice**. Montrez que si $N$ est interprétable dans $M$, alors pour toute $\mathcal{L}'$-formule $\varphi(x_1, \ldots, x_n)$ il existe une $\mathcal{L}$-formule $\varphi^*(y_1, \ldots, y_n)$, où chaque $y_i$ est un $k$-uplet de variables, telle que, pour tout $n$-uplet $(b_1, \ldots, b_n)$ d'éléments de $S$, on a

$$N \models \varphi(F^{-1}(a_1/E), \ldots, F^{-1}(a_n/E)) \iff M \models \varphi^*(b_1, \ldots, b_n).$$

Même remarque que pour les structure définissables : la preuve est longue et ennuyeuse, vous pouvez vous contenter de la faire pour l'exemple donné dans l'exercice 1.18.

**1.18. Exercice**. Montrez que si $R$ est un anneau intègre commutatif, alors son corps des fractions $K$ est interprétable dans $R$.

**1.19. Exercice**. Soit $(K, v)$ un corps valué. Montrez que la structure $\mathcal{K}$ à 3 sortes qui lui est associée est interprétable dans l'anneau $\mathcal{O}_v$ (son langage étant celui des anneaux : $\{+, -, \cdot, 0, 1\}$).

**1.20. La topologie**. Soit $(K, v)$ un corps valué, de groupe de valeur $\Gamma$, et soient $a \in K$, $\gamma \in \Gamma$. Les ensembles

$$B(a, \gamma) = \{b \in K \mid v(b - a) > \gamma\} \quad \text{and} \quad \bar{B}(a, \gamma) = \{b \in K \mid v(b - a) \geq \gamma\}$$

sont appelés la *boule ouverte* (resp. *fermée*) *de centre a et rayon* $\gamma$.

En prenant pour base d'ouverts les boules ouvertes, on définit sur $K$ une topologie. Notez que les opérations du corps sont continues pour cette topologie. Si $a, b \in K$ et $\gamma \in \Gamma$, alors on a

$$B(a, \gamma) = B(b, \gamma) \iff b \in B(a, \gamma) \iff B(a, \gamma) \cap B(b, \gamma) = \emptyset.$$

La preuve est laissée en **exercice**. Cela entraine que les boules ouvertes sont aussi fermées pour la topologie, et que les boules fermées sont ouvertes pour la topologie.

**1.21. Complétions**. Rappelons qu'un espace muni d'une métrique est *complet* ssi toute suite de Cauchy a une limite. Dans le cas d'un corps valué avec groupe de valeurs archimédien (qu'on peut donc supposer contenu dans $\mathbb{R}$), cette propriété se traduit de la façon suivante : le corps valué $K$ est complet ssi, pour toute suite suite $(a_n)_{n\in\mathbb{N}}$ telle que pour tout $N$ il existe $M$ tel que quelque soit $m \geq M$, $v(a_{m+1} - a_m) > N$, alors il existe $a \in K$ tel que $lim_{n\to\infty} v(a - a_n) = \infty$.

On peut l'exprimer aussi en termes de boules : $K$ est complet ssi toute chaîne décroissante de boules ouvertes non vides dont les rayons tendent vers l'infini a une intersection non vide. (On pourrait tout aussi bien prendre des boules fermées).

Quand le groupe de valeurs du corps n'est pas archimédien, nous introduirons d'autres notions.

**1.22. Exercice**. Vérifiez que la définition que j'ai donnée coïncide avec la définition usuelle de corps métrique complet.

**1.23. Exemples de corps complets**.

Il est clair que $K((t))$, donné dans l'exemple 1.7(2) est complet. On peut d'ailleurs montrer que c'est la complétion de $K(t)$. Par contre, $\mathbb{Q}$ muni de la valuation $p$-adique n'est pas complet, tout simplement pour des raisons de cardinalite. En effet, soit $(b_n)_{n\in\mathbb{N}}$ une suite d'entiers de $\{0, \ldots, p-1\}$. A partir de $(b_n)$ nous pouvons définir une suite de Cauchy $(a_n)$, en posant tout simplement $a_n = \sum_{i=0}^{n-1} b_i p^i$. La limite d'une telle suite s'écrira intuitivement $b = \sum_{i\in\mathbb{N}} b_i p^i$, et si

$(b'_n)$ est une autre suite, alors il existe $N$ tel que si $m \geq N$ alors $\sum_{0\leq i\leq m} b_i p^i \not\equiv \sum_{0\leq i\leq m} b'_i p^i$ : soit $N$ le plus petit entier tel que $b_N \neq b'_N$. Comme il y a $2^{\aleph_0}$ telles suites (rappel : $2^{\aleph_0} = p^{\aleph_0} = \aleph_0^{\aleph_0}$), et que $\mathbb{Q}$ est dénombrable, $\mathbb{Q}$ ne peut être complet. Notons que le contre-exemple auquel on pense tout de suite n'en est pas un : la suite $(a_n)$ définie par $a_n = \sum_{i=0}^{n-1} p^i$ a pour limite $(1-p)^{-1}$. En effet, pour tout $n$, on a $a_n(1-p) \equiv 1 \bmod p^n$ ; c'est-à-dire, pour tout $n$, pour tout $m > n$, $a_m(1-p) \equiv 1 \bmod p^n$ ; la limite $a$ devra donc satisfaire $a(1-p) \equiv 1 \bmod p^n$ pour tout $n$. Et donc, $a = (1-p)^{-1}$.

De la même façon qu'on construit $\mathbb{R}$ à partir de $\mathbb{Q}$ en utilisant les suites de Cauchy, on peut construire la complétion de $\mathbb{Q}$ pour la valuation $p$-adique de la façon suivante : Un *entier $p$-adique* est une suite $(a_n)_{n\in\mathbb{N}}$ d'entiers satisfaisant

$$0 \leq a_n < p^n \quad \text{et} \quad a_{n+1} \equiv a_n \mod p^n$$

pour tout $n \in \mathbb{N}$. Les opérations d'anneau s'étendent facilement : si $(a_n)_n$, $(b_n)_n$ et $(c_n)_n$ sont de telles suites alors

$$\begin{aligned} (a_n)_n + (b_n)_n = (c_n)_n \quad &\Longleftrightarrow \quad \forall n\ a_n + b_n \equiv c_n \bmod p^n, \\ (a_n)_n (b_n)_n = (c_n)_n \quad &\Longleftrightarrow \quad \forall n\ a_n b_n \equiv c_n \bmod p^n. \end{aligned}$$

L'ensemble de ces suites, muni des deux opérations définies ci-dessus, est un anneau, appelé l'anneau des *entiers $p$-adiques*, et noté $\mathbb{Z}_p$. On a $v((a_n)_n) = \inf\{n \mid a_n = 0\}$, et $\mathbb{Z}$ est dense pour la topologie. Le corps $\mathbb{Q}_p$ des nombres $p$-adiques est le corps des fractions de $\mathbb{Z}_p$, il est noté $\mathbb{Q}_p$, et on a $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.

Une autre façon de décrire $\mathbb{Z}_p$ est tout simplement comme la limite inverse des anneaux $\mathbb{Z}/p^n\mathbb{Z}$, les flèches $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ étant tout simplement *réduction modulo $p^n$*.

**1.24. Compacité**. La représentation des éléments de $\mathbb{Z}_p$ comme des sommes $\sum_{i=0}^{\infty} b_i p^i$, $b_i \in \{0, 1, \ldots, p-1\}$ nous donne un homéomorphisme $\mathbb{Z}_p \to \{0, 1, \ldots, p-1\}^{\aleph_0}$, et montre que $\mathbb{Z}_p$ est compact.

Par contre $\mathbb{Q}_p$ n'est pas compact, car il est la réunion des boules ouvertes $B(0; -n)$, $n \in \mathbb{N}$).

De la même façon, on peut montrer que si $K$ est un corps **fini**, alors $K[[t]]$ est compact (et $K((t))$ n'est pas compact). Cette propriété de compacité de l'anneau de valuation est une conséquence de la finitude du corps résiduel, et n'est plus vérifiée si $K$ est infini : $K[[t]]$ est une union infinie de boules ouvertes de rayon 0 (indexée par les éléments du corps résiduel).

**1.25. Ensembles bien ordonnés**. Soit $(I, <)$ un ensemble totalement ordonné. $I$ est *bien ordonné* s'il satisfait l'une des deux propriétés équivalentes suivantes :

(1) Tout sous-ensemble non vide de $I$ a un plus petit élément.

(2) Toute suite strictement décroissante d'éléments de $I$ est finie.

**1.26. Lemme** Soit $\Gamma$ un groupe abélien ordonné, et soient soient $I$ et $J$ des sous-ensembles de $\Gamma$ qui sont bien-ordonnés. Soit $k \in \Gamma$. Alors l'ensemble des paires $(i, j) \in I \times J$ telles que $i + j = k$ est fini.

*Démonstration.* Si $i + j = k = i' + j'$ et $i < i'$ alors $j > j'$. Si notre ensemble de paires est infini, alors l'ensemble des premières coordonnées est infini, contenu dans $I$. En prenant le premier élément, puis le deuxième, etc., on en extraint une suite infinie, appelons-la $(i_n)$ ; alors $k - i_n = j_n$ est strictement décroissante, ce qui contredit la propriété du bon ordre de $J$.

**1.27. Lemme**. Soit $\Gamma$ un groupe abélien ordonné, et soient $I$ et $J$ des sous-ensembles de $\Gamma$ qui sont bien-ordonnés. Montrez que $I + J =_{\text{def}} \{i + j \mid i \in I, j \in J\}$ est bien ordonné.

La preuve de ce lemme est facile, et est laissée en exercice.

**1.28. Lemme**. Soient $\Gamma$ un groupe abélien ordonné, et $I$ un sous-ensemble bien ordonné de $\Gamma$ ne contenant que des éléments $> 0$. Pour chaque $n \in \mathbb{N}$ on définit $nI = \{i_1 + i_2 + \cdots + i_n \mid i_1, \ldots, i_n \in I\}$. Montrez que $\omega I =_{\text{def}} \bigcup_{n\in\mathbb{N}} nI$ est bien ordonné, et que pour tout $\gamma \in \Gamma$, il n'existe qu'un nombre fini de suites finies d'éléments de $\Gamma$ dont la somme égale $\gamma$.

Ce lemme est connu sous le nom de *Lemme de Neumann*. Sa preuve est assez longue et plus difficile. On montre d'abord le résultat en supposant que $\Gamma$ est archimédien (facile). Puis dans le cas général, pour chaque $a > 0$ on considère $[a] = \{b \in \Gamma \mid \exists n \in \mathbb{N}\ a/n < b < na\}$ (la *classe archimédienne de a dans* $\Gamma$). Si $b \in [a]$ alors $[b] = [a]$, chaque classe est convexe et close par addition. Comme $I$ est bien-ordonné, on peut trouver une suite $(C_\alpha)_{\alpha<\kappa}$ de classes archimédiennes telles que $I \subset \bigcup_{\alpha<\kappa} C_\alpha$. Pour $\alpha \leq \kappa$, on pose $D_\alpha = \bigcup_{\beta<\kappa}$, et, en utilisant une induction sur $\alpha$, on montre alors que chaque $\omega(I \cap D_\alpha)$ satisfait la conclusion du lemme.

**1.29. Séries généralisées - Exercice**. Soit $K$ un corps, et $\Gamma$ un groupe abélien ordonné. On définit l'anneau des séries généralisées $K((\Gamma))$ de la façon suivante. Un élément de $K((\Gamma))$ est une somme $f = \sum_{\gamma\in\Gamma} a_\gamma t^\gamma$, dont le *support*, $Supp(f) = \{\gamma \mid a_\gamma \neq 0\}$ est bien-ordonné. On définit une addition et une multiplication sur $K((\Gamma))$ en posant

$$\sum_\gamma a_\gamma t^\gamma + \sum_\gamma b_\gamma t^\gamma = \sum_\gamma (a_\gamma + b_\gamma) t^\gamma, \quad \sum_\gamma a_\gamma \sum_\gamma b_\gamma = \sum_\gamma (\sum_\delta a_\delta b_{\gamma-\delta}) t^\gamma.$$

On définit une valuation sur $K((\Gamma))$ en posant $v(f) = \inf Supp(f)$, et l'anneau de valuation est noté $K[[\Gamma]]$, ce sont les séries dont le support est non-négatif.

(1) Vérifiez que la somme et le produit de deux éléments de $K((\Gamma))$ sont bien dans $K((\Gamma))$. Il est a peu près clair je pense que les lois d'anneau sont vérifiées, et que $v$ définit bien une valuation.

(2) Montrez que $K((\Gamma)) = K[[\Gamma]](t^\gamma \mid \gamma < 0)$, et que les éléments de valuation 0 sont inversibles dans $K[[\Gamma]]$. Cela montrera que $K((\Gamma))$ est bien un corps. [Où avez-vous utilisé l'hypothèse sur le support des éléments de $K((\Gamma))$?]

**Remarque**. L'algèbre de groupe $K[\Gamma]$ est simplement l'ensemble des éléments de $K[[\Gamma]]$ de support fini.

# 2 Les corps valués algébriquement clos

**2.1. Le langage $\mathcal{L}_{\text{div}}$.** Rappelons que le langage $\mathcal{L}_{\text{div}}$ est obtenu en ajoutant au langage des anneaux $\{+, -, \cdot, 0, 1\}$ un symbole de relation binaire div. Dans un corps valué, ce symbole sera interprété par : $a \operatorname{div} b \iff v(a) \leq v(b)$ (c'est-à-dire, si et seulement si $ba^{-1} \in \mathcal{O}_v$). Il est clair que l'anneau $\mathcal{O}_v$ est alors définissable sans quantificateurs, par la formule $1 \operatorname{div} a$, et que donc la valuation est définissable dans la structure $(K, +, -, \cdot, 0, 1, \operatorname{div})$.

Nous allons montrer que la théorie des corps algébriquement clos valués (de valuation non triviale) élimine les quantificateurs dans le langage $\mathcal{L}_{\text{div}}$. Cela entrainera que les complétions de cette théorie seront obtenues en spécifiant la caractéristique du corps et celle du corps résiduel (cette dernière sera appellée la *caractéristique résiduelle*).

En effet, en notant $n$ la somme $n$-fois du nombre 1 : la caractéristique du corps est $p > 0$ si et seulement $p = 0$, et elle est nulle si et seulement si $p \neq 0$ pour tout $p$. De même, la caractéristique résiduelle est $p > 0$ si et seulement si $\neg(p \operatorname{div} 1)$, et elle est nulle si et seulement si $p \operatorname{div} 1$ pour tout $p$.

La démonstration est faite par une technique de va-et-vient : nous nous plaçons dans deux corps valués algébriquement clos $K$ et $L$ de même caractéristique (de corps et de corps résiduel), et qui sont suffisamment saturés. Nous allons montrer que si $f : A \to B$ est un isomorphisme partiel entre des sous-anneaux dénombrables de $K$ et $L$, et si $a \in K$ alors il existe un isomorphisme partiel $g$ qui étend $f$, a $a$ dans son domaine, et prend ses valeurs dans $L$. Notons que l'ensemble des isomorphismes partiels entre $K$ et $L$ n'est pas vide : leurs sous-corps premiers sont isomorphes en tant que corps valués. Comme nous verrons, la difficulté principale apparaît quand $a$ est algébrique sur $A$, et pour cela nous devons étudier le comportement des extensions de $v$ à la clôture algébrique d'un corps.

## 2.1 Extensions de valuations : résultats d'algèbre commutative

**2.2. Rappels sur les anneaux de valuation**. Soit $R$ un anneau commutatif intègre, et $K$ son corps de fractions. On dit que $R$ est un *anneau de valuation* si pour tout $a \in K^*$, si $a \notin R$, alors $a^{-1} \in R$. On peut vérifier alors que les éléments non inversibles de $R$ forment un idéal, qui est nécessairement maximal, et que les idéaux principaux de $R$ forment une chaîne. [La seule astuce apparaissant dans la vérification est la suivante : supposons $a, b$ non inversibles dans $R$, nous voulons montrer que leur somme est aussi non inversible ; on sait que $a/b$ ou $b/a$ est dans $R$, supposons que ce soit $a/b$ ; alors $a + b = b(1 + a/b)$ ne peut être inversible puisque $b$ ne l'est pas et $1 + a/b \in R$)].

Comme dans 1.12, si $R^\times$ dénote les éléments inversibles de $R$, alors $R^\times$ est un sous-groupe du groupe multiplicatif $K^\times$, et si on écrit la loi de groupe de $K^\times/R^\times$ additivement, on obtient un groupe abélien ordonné $\Gamma$, l'ordre étant défini par $v(a) \geq v(b)$ si et seulement si $ab^{-1} \in R$. Ces résultats sont classiques, les démonstrations peuvent être trouvées par exemple dans le livre *Algebra* de S. Lang.

**2.3. Autres propriétés des anneaux intégralement clos et des extensions intégrales**. Les démonstrations des résultats suivants se trouvent dans le chapitre IX de Lang (Algebra,

chapitre sur les extensions d'anneau). **Tous les anneaux seront commutatifs et intègres**.

**2.4. Proposition**. Soit $R$ un anneau intégralement clos, $P$ un idéal premier de $R$, et $S$ une extension de $R$, dont tous les éléments sont entiers sur $R$. Alors il existe un idéal premier $Q$ de $S$ *au-dessus de* $P$, c'est-à-dire tel que $Q \cap R = P$. De plus, $P$ est maximal si et seulement si $Q$ est maximal.

**2.5.** Rappelons que si $P$ est un idéal premier de $R$, alors le localisé de $R$ en $P$, noté $R_P$, est le sous-anneau du corps des fractions de $R$ qui est engendré au-dessus de $R$ par les inverses des éléments de $R \setminus P$. L'idéal $PR_P$ est donc l'unique idéal maximal de $R_P$, et travaillant dans $S_P$ (le sous-anneau du corps de fractions de $S$ engendré par $S$ et $R_P$), on obtient que les idéaux maximaux de $S_P$ sont exactement ceux qui sont engendrés par des idéaux de $S$ au-dessus de $P$. Notons qu'il peut y en avoir plusieurs.

**Corollaire**. Soient $R$ et $S$ comme ci-dessus, et $\varphi : R \to \Omega$ un morphisme de $R$ dans un corps algébriquement clos $\Omega$. Alors $\varphi$ s'étend à un morphisme $\psi : S \to \Omega$.

*Démonstration.* Appliquer le résultat précédent à $P = Ker(\varphi)$ et utiliser le lemme de Zorn.

**2.6. Proposition**. Soient $R$ un anneau de valuation, $K$ son corps de fractions, $L$ une extension de Galois finie de $K$, et $S$ la *clôture intégrale* de $R$ dans $L$, c'est-à-dire, l'ensemble des éléments de $S$ qui sont entiers sur $R$. Soit $\mathcal{M}$ l'idéal maximal de $R$, $Q$ et $Q'$ des idéaux de $S$ au-dessus de $\mathcal{M}$. Alors

(1) L'anneau $S_Q$ est un anneau de valuation.

(2) Il existe $\sigma \in \mathcal{G}al(L/K)$ tel que $\sigma(Q') = Q$. De plus, les valuations sur $L$ correspondant à $Q$ et à $Q'$ ne sont pas équivalentes.

D'autre part, il est relativement clair que si $R$ est un anneau de valuation de caractéristique $p > 0$, et $S = R[a]$, où $a^p = b \in R$, alors l'idéal maximal $\mathcal{M}$ de $R$ s'étend de manière unique à un idéal maximal $Q$ de $S$ : en effet, les puissances $p$-ièmes des éléments de $S$ sont dans $R$, et on aura donc $s \in Q \iff s^p \in \mathcal{M}$.

Tous ces résultats impliquent alors, étant donné le fait qu'une valuation sur un corps est déterminée (à équivalence près) par son anneau de valuation :

**2.7. Théorème**. Soit $(K, v)$ un corps valué, et $L$ une extension algébrique de $K$ qui est normale. Alors $v$ s'étend à une valuation $w$ sur $L$, et de plus, si $w'$ est une autre valuation de $L$ étendant $v$, alors il existe $\sigma \in \mathrm{Aut}(L/K)$ tel que $w'$ et $w \circ \sigma$ sont équivalentes.

## 2.2 Saturation

**2.8. Saturation, et quelques propriétés**. Soit $\kappa$ un cardinal infini, $T$ une théorie dans un langage $\mathcal{L}$. Si $M$ est une $\mathcal{L}$-structure et $A$ un sous-ensemble de $M$, je d'enote par $\mathcal{L}(A)$ le langage obtenu en ajoutant à $\mathcal{L}$ des symboles de constantes pour les éléments de $A$. $M$ devient naturellement une $\mathcal{L}(A)$-structure : on interprète la constante $a$ par l'élément $a$.

Un modèle $M$ de $T$ est *$\kappa$-saturé* si pour tout sous-ensemble $A$ de $M$ de cardinalité $< \kappa$, et tout ensemble $\Sigma$ de $\mathcal{L}(A)$-formules ayant comme variables libres le $n$-uplet $x$, et qui est *finiment*

*satisfaisable* dans $M$ (c'est-à-dire, pour tout $m$, si $\varphi_1(x), \ldots, \varphi_m(x) \in \Sigma$, il existe un uplet $a$ de $M$ tel que $M \models \bigwedge_i \varphi_i(a)$), alors il existe un $n$-uplet qui *réalise* $\Sigma$, c'est-à-dire qui satisfait toutes les formules de $\Sigma$ dans $M$. Vous verrez les propriétés des modèles saturés plus en détail dans l'autre cours (vous pouvez aussi les trouver dans tous les livres classiques de théorie des modèles : Chang et Keisler, Hodges, Poizat, etc.).

**Théorème**. Soient $M$ une $\mathcal{L}$-structure, $\kappa$ un cardinal infini. Alors $M$ a une extension élémentaire qui est $\kappa$-saturée.

L'intérêt des modèles saturés est qu'ils permettent de satisfaire simultanément des ensembles infinis de formules. Supposons par exemple que $\Sigma$ soit clos par conjonction finie. Le fait qu'il soit finiment satisfaisable s'exprime tout simplement par la conjonction infinie $M \models \bigwedge_{\varphi \in \Sigma} \exists x\ \varphi(x)$. La saturation de $M$ nous permet alors de "sortir le quantificateur existentiel", c'est-à-dire, en fait $M \models \exists x\ \bigwedge_{\varphi \in \Sigma} \varphi(x)$.

Notons que si $|M| = \kappa$ est infini, alors $M$ ne peut-être $\kappa^+$-saturé : en prenant $A = M$, l'ensemble $\Sigma = \{x \neq a \mid a \in M\}$ est finiment satisfaisable dans $M$ mais n'a pas de réalisation dans $M$.

**2.9.** On considère la théorie $T$ du groupe abélien $(\mathbb{Q}, +, -, 0)$. On sait que $T$ est axiomatisée en disant que le groupe est abélien, divisible et sans torsion.

(1) Montrez que $\mathbb{Q}$ n'est pas $\aleph_0$-saturé.

(2) Soit $\kappa$ un cardinal infini. Une fois que vous aurez montré (1), il vous sera facile de caractériser les modèles de $T$ qui sont $\kappa$-saturés.

(3) Est-ce que l'ensemble ordonné $(\mathbb{R}, <)$ est $\aleph_1$-saturé ?

**2.10. Lemme**. Soit $T$ une théorie dans un langage $\mathcal{L}$. **Nous supposerons que $\mathcal{L}$ contient un symbole de constante.** Les trois conditions suivantes sont équivalentes :

(1) $T$ élimine les quantificateurs (c'est-à-dire, toute $\mathcal{L}$-formule $\varphi(x)$, $x$ un uplet de variables, est équivalente modulo $T$ à une formule $\psi(x)$ sans quantificateurs).

(2) Toute formule existentielle avec un seul quantificateur est équivalente modulo $T$ à une formule sans quantificateurs.

(3) Si $M$ et $N$ sont des modèles $\aleph_1$-saturés de $T$, si $A_0 \subset M$ et $B_0 \subset N$ sont dénombrables et tels qu'il existe un isomorphisme (de $\mathcal{L}$-structures) entre les sous-structures $A$ de $M$ et $B$ de $N$ engendrées respectivement par $A_0$ et $B_0$, qui envoie $A_0$ sur $B_0$ (chacun ayant une énumération fixée) et si $c$ est un élément de $M$, alors il existe un isomorphisme $g$ étendant $f$, ayant pour domaine une sous-structure de $M$ contenant $c$, et image contenue dans $N$.

*Démonstration.* (1) $\Rightarrow$ (2) est clair. On montre (2) $\Rightarrow$ (1) par induction sur le nombre de quantificateurs des formules. Grosso modo, (2) nous dit qu'on peut éliminer un quantificateur. On les élimine donc un par un.

(1) $\Rightarrow$ (3). Soient $A_0$, $B_0$, $A$, $B$, $f$ et $a$ comme dans l'hypothèse de (3). La chose importante à remarquer, est que tout élément de $A$ est de la forme $t(\bar{a})$, où $t$ est un $\mathcal{L}$-terme, et $\bar{a}$ est un uplet d'éléments de $A_0$. Le type d'isomorphisme de la $\mathcal{L}$-structure $A$ est donc entièrement décrit par l'ensemble des énoncés sans quantificateurs du langage $\mathcal{L}(A_0)$ qui sont vrais dans $(M, a)_{a\in A_0}$. Il en est de même bien sur pour $B$ et $B_0$, et pour la sous-structure de $M$ engendrée par $c$ et $A$.

Notre hypothèse sur $f$ est donc équivalente au fait que $A_0$ et $B_0$ (avec leur énumération) satisfont exactement les mêmes $\mathcal{L}$-formules sans quantificateurs. Ou encore, si $a \in A_0$ et on interprète dans $N$ la constante $a$ par $f(a)$, alors $f$ est un isomorphisme de $\mathcal{L}(A_0)$-structures. On regarde l'ensemble $\Sigma$ des formules de $\mathcal{L}(A_0)$ qui sont satisfaites par $c$ dans $M$ (cet ensemble s'appelle le *type de a sur* $A_0$, et est noté $tp(a/A_0)$). Notons que $\Sigma$ est clos par conjonction finie, et que toutes ses formules sont de la forme $\varphi(\bar{a}, x)$ pour une $\mathcal{L}$-formule $\varphi$. Par élimination des quantificateurs, puisque $A_0$ et $B_0$ satisfont les mêmes formules sans quantificateurs, nous avons donc que pour toute $\mathcal{L}$-formule $\varphi(\bar{a}, x) \in \Sigma$, comme $M \models \exists x\ \varphi(\bar{a}, x)$, aussi $N \models \exists x\ \varphi(f(\bar{a}), x)$.

Par $\aleph_1$-saturation de $N$, et comme $\Sigma$ est clos par conjonction, il existe donc $d \in N$ qui satisfait toutes les formules de $\Sigma$. Alors l'application qui étend $f$ et envoie $c$ sur $d$ se prolonge à un isomorphisme entre les sous-structures de $M$ et $N$ engendrées par $(A_0, a)$ et $(B_0, b)$ respectivement.

(3) $\Rightarrow$ (2). Supposons qu'il existe une formule $\exists x\ \varphi(y, x)$, $x$ un singleton, $y$ un uplet de variables, qui ne soit pas équivalente modulo $T$ à une formule sans quantificateurs. Il existe donc des modèles de $T$, $M$ et $N$, et des uplets $a$ de $M$ et $b$ de $N$, qui satisfont les mêmes formules sans quantificateurs, mais $M \models \exists x\ \varphi(a, x)$ tandis que $N \models \forall x\ \neg\varphi(b, x)$ [Ceci utilise la compacité, voir 2.12 ci-dessous]. Passant à des extensions élémentaires de $M$ et $N$, nous pouvons supposer que $M$ et $N$ sont $\aleph_1$-saturés. Comme $a$ et $b$ satisfont les mêmes formules sans quantificateurs, il existe un isomorphisme $f$ entre la sous-structure $A$ de $M$ engendrée par $a$ et la sous-structure $B$ de $N$ engendrée par $b$, et qui envoie $a$ sur $b$. Soit $c \in M$ tel que $M \models \varphi(a, c)$. Alors on ne peut trouver un $g$ qui étende $f$, aie $a$ dans son domaine, et image contenue dans $N$, puisque $N \models \forall x\ \neg\varphi(b, x)$.

**2.11. Quelques remarques sur le résultat précédent.**

(1) On aurait pu remplacer (2) par : toute formule existentielle est équivalente modulo $T$ à une formule sans quantificateurs. Mais dans ce cas, il aurait été mieux d'énoncer (3) en prenant pour $c$ un uplet fini (et non un seul élément).

(2) La preuve de (3) implique (2) ci-dessus n'utilise que la $\aleph_0$-saturation de $M$ et $N$. En fait, on voit facilement que l'on peut changer l'énoncé de (3) de la façon suivante : si $\kappa$ est un cardinal infini, $M$ et $N$ des modèles de $T$ $\kappa$-saturés, et si $A_0 \subset M$, $B_0 \subset N$ sont des ensembles de cardinalité $< \kappa$ tels que ...

(3) Que se passe-t-il si $\mathcal{L}$ ne contient aucun symbole de constante ? Supposons que ce soit le cas. Le problème c'est que il n'y a pas d'énoncés sans quantificateurs, donc la théorie $T$ ne peut pas les éliminer. En effet, la définition que j'ai donnée entraîne que si $\varphi$ est un énoncé,

il faut pouvoir trouver un énoncé sans quantificateurs $\psi$ qui lui est équivalent modulo $T$. Donc, de toute façon, $T$ ne peut pas éliminer les quantificateurs, au moins si on prend cette définition. On pourrait relaxer la condition sur $\psi$, en lui permettant d'avoir d'autres variables libres que celles de $\varphi$. Ou bien en ajoutant au langage deux symboles logiques $\top$ et $\bot$. Mais dans les deux cas, il faudrait absolument que $T$ soit complète. Notons que le problème ne se pose vraiment que pour les énoncés. La solution généralement retenue est de permettre à la formule $\psi$ d'avoir plus de variables que $\varphi$. En prenant cette définition moins stricte de l'élimination des quantificateurs, on s'aperçoit alors que même dans ce cas, le théorème reste vrai. Il faut simplement observer que l'application de domaine vide est un isomorphisme entre $\emptyset \subset M$ et $\emptyset \subset N$. Avec cette nouvelle définition de l'élimination des quantificateurs, on montre que la théorie de l'ensemble infini sans structure ($\mathcal{L} = \emptyset$) et que la théorie de l'ensemble ordonné $(\mathbb{Q}, <)$ éliminent les quantificateurs. A dire vrai, j'avais totalement occulté ce problème quand j'ai donné la définition de l'e.q.

(4) On remarque aussi que dans (3), si $M$ et $N$ sont de cardinalité $\aleph_1$, alors on peut, à l'aide d'un va-et-vient, construire un isomorphisme entre $M$ et $N$. En effet, nous prenons deux énumérations $(c_\alpha)_{\alpha<\aleph_1}$ et $(d_\alpha)_{\alpha<\aleph_1}$ de $M \setminus A$ et $N \setminus B$, puis construisons par induction transfinie un système $g_\alpha$ d'isomorphismes entre des sous-structures de $M$ et $N$, avec $f \subset g_\alpha \subset g_\beta$ si $\alpha < \beta$, et tel que le domaine de $g_\alpha$ contienne tous les $c_\gamma$ avec $\gamma < \alpha$ et son image tous les $d_\gamma$ avec $\gamma < \alpha$. La construction de $g_{\alpha+1}$ se fait en deux étapes (le "va" et le "vient") : on utilise (3) pour trouver une application $h_\alpha$ prolongeant $g_\alpha$, et ayant $c_\alpha$ dans son domaine ; puis on utilise (3) de nouveau pour trouver une application $g_{\alpha+1}$ telle que $g_{\alpha+1}^{-1}$ prolonge $h_\alpha^{-1}$ et a $d_\alpha$ dans son domaine.

**2.12. Exercice**. Nous supposons que $T$ est une théorie dans un langage $\mathcal{L}$, que la formule $\varphi(x)$, $x$ un $n$-uplet de variables, n'est pas équivalente modulo $T$ à une formule sans quantificateurs.

(1) Soit $\Delta$ l'ensemble des formules sans quantificateurs en $x$, et soient $a$ et $b$ deux nouveau $n$-uplets de constantes. Montrez que

$$T \cup \{\psi(a) \iff \psi(b) \mid \psi(x) \in \Delta\} \cup \{\varphi(a) \iff \neg\varphi(b)\}$$

est consistante.

(2) Déduisez-en que $T$ a un modèle, dans lequel on peut trouver des $n$-uplets $a$ et $b$ qui satisfont les mêmes formules sans quantificateurs, et tels que $M \models \varphi(a) \wedge \neg\varphi(b)$.

Ce genre de preuve est typique en théorie des modèles : pour prouver quelque chose, on enrichit le langage, on montre qu'une certaine theorie dans ce grand langage est consistante, donc a un modèle, puis on oublie les nouveaux symboles. En général les symboles ajoutés sont des symboles de constantes.

## 2.3 Le résultat principal

**2.13. Quelques propriétés simples des corps valués algébriquement clos**. Notons d'abord que si le corps valué $K$ est algébriquement clos, alors son corps résiduel $k$ l'est aussi, et son groupe de valeurs $\Gamma$ est divisible.

En effet, soit $p(X) \in k[X]$ un polynôme unitaire, et soit $P(X) \in \mathcal{O}_v[X]$ un polynôme unitaire qui relève $p(X)$, c'est-à-dire, tel que le polynôme obtenu en appliquant res aux coefficients de $P(X)$ égale $p(X)$. Puisque $K$ est algébriquement clos, il contient une racine $\alpha$ de $P(X)$ ; comme $P$ est unitaire, $\alpha \in \mathcal{O}_v$ (cf 1.4(4)). Alors $0 = \mathrm{res}\,(P(\alpha)) = p(\mathrm{res}\,(\alpha))$, ce qui montre que $\mathrm{res}\,(\alpha)$ est une racine de $p$.

Soient maintenant $\gamma \in \Gamma$ et $n$ un entier positif. Prenons $a \in K$ tel que $v(a) = \gamma$, et soit $b \in K$ tel que $b^n = a$ ; alors $v(b) = \gamma/n$.

**2.14. Théorème** La théorie des corps valués algébriquement clos et de valuation non triviale élimine les quantificateurs dans le langage $\mathcal{L}_{\mathrm{div}}$.

*Démonstration.* Soient $(K, v)$ et $(L, w)$ des corps algébriquement clos valués $\aleph_1$-saturés, $A \subset K$ et $B \subset L$ des sous-anneaux dénombrables, et $f : A \to B$ un $\mathcal{L}_{\mathrm{div}}$-isomorphisme, $a \in K$.

L'existence même de $f$ nous dit que les corps $K$ et $L$ ont même caractéristique, et même caractéristique résiduelle. De plus, $f$ s'étend uniquement en un isomorphisme entre les corps de fractions de $A$ et $B$, pour simplifier les notations nous les noterons aussi $A$ et $B$. Notons que $f$ induit des isomorphismes (aussi notés $f$) entre le corps résiduel $k_A$ de $A$ et le corps résiduel $k_B$ de $B$, et entre les groupes de valeurs $\Gamma_A$ de $A$ et $\Gamma_B$ de $B$. (En effet, $\Gamma_A \simeq A^\times/\mathcal{O}_A^\times$, et $k_A \simeq \mathcal{O}_A/\mathcal{M}_A$ ; nous avons supposé ici que $A$ est un corps).

**Cas 1**. $a$ est algébrique sur $A$.

Soit $C$ la clôture normale de $A(a)$, et étendons $f$ à un isomorphisme de corps entre $C$ et un sous-corps $D$ de $L$. Alors $g$ envoie l'anneau de valuation $\mathcal{O}_v \cap C$ de $C$ sur un anneau de valuation $R$ de $D$. Comme toutes les valuations sur $D$ qui étendent $w$ sont conjuguées, il existe $\sigma \in \mathrm{Aut}(D/B)$ tel que $\sigma(R)$ coïncide avec l'anneau de valuation $\mathcal{O}_w \cap D$. Alors $\sigma \circ g : C \to D$ est l'isomorphisme désiré.

Plus simple : étendons $f$ à un isomorphisme de corps $g$ entre la clôture algébrique $A^{alg}$ de $A$ et celle de $B$, $B^{alg}$. (Rappel : $A^{alg}$ est l'ensemble des éléments de $K$ qui satisfont une équation non triviale à coefficients dans $A$.) Alors $f(\mathcal{O}_{A^{alg}})$ est un anneau de valuation de $B^{alg}$, dont l'intersection avec $B$ égale l'anneau de valuation de $B$ ; cet anneau définit donc une valuation $v'$ sur $B^{alg}$ qui étend $w$ sur $B$ ; par 2.7, il existe $\sigma \in \mathrm{Aut}(B^{alg}/B)$ tel que alors $v' = w \circ \sigma$. Cela entraîne, pour $a \in A^{alg}$ :

$$v(a) \geq 0 \iff a \in \mathcal{O}_{A^{alg}} \iff f(a) \in \mathcal{O}_{B^{alg},v'} \iff v'(f(a)) \geq \iff w \circ \sigma \circ f(a) \geq 0.$$

Cela montre que $\sigma \circ f$ est un isomorphisme de corps valués.

Le cas 1 montre que nous pouvons étendre $f$ à la clôture algébrique de $A$, et nous supposerons donc que $A$ et $B$ sont algébriquement clos. (Ils seront dénombrables, ce qui nous permettra quand même d'utiliser la $\aleph_1$-saturation).

**Cas 2**. Il existe $c \in A(a)$ tel que $v(c) = \gamma \notin \Gamma_A$.

Comme $A$ est algébriquement clos, $\Gamma_A$ est divisible ; cela entraîne que pour tout $n \in \mathbb{N}^{>0}$, $n\gamma \notin \Gamma_A$ (car $\Gamma_A$ est sans-torsion). Nous avons

$$v(A(c)^\times) = \Gamma_A \oplus \langle\gamma\rangle.$$

Considérons l'ensemble de formules

$$\Sigma(\xi) = \{\xi > \alpha \mid \gamma > \alpha\} \cup \{\xi < \alpha \mid \gamma < \alpha\},$$

ainsi que son image par $f$ :

$$\Sigma^f(\xi) = \{\xi > f(\alpha) \mid \gamma > \alpha\} \cup \{\xi < f(\alpha) \mid \gamma < \alpha\}.$$

Cet ensemble est finiment satisfaisable dans $\Gamma_B$, car $\Gamma_B$ est un ordre dense sans extrémité. Soit $\delta \in \Gamma_L$ satisfaisant toutes les formules de $\Sigma^f(\xi)$. Alors l'application $f : \Gamma_A \oplus \langle\gamma\rangle \to \Gamma_B + \langle\delta\rangle$ est un isomorphisme de groupes ordonnés. En effet, soient $\alpha + m\gamma$ et $\alpha' + m'\gamma$ des éléments de $\Gamma_A \oplus \langle\gamma\rangle$, avec $m \neq m'$. Alors

$$\alpha + m\gamma < \alpha' + m'\gamma \iff \frac{\alpha - \alpha'}{|m' - m|} < \frac{m' - m}{|m' - m|}\gamma,$$

et comme $\Gamma_A$ est divisible, $(\alpha - \alpha')/(m' - m) \in \Gamma_A$. Cela montre deux choses : que $f$ est injective, donc un isomorphisme, et respecte l'ordre.

On montre facilement que si $a_0, \ldots, a_n \in A$, alors les $v(a_i c^i)$ sont tous distincts (si $v(a_i c^i) = v(a_j c^j)$ alors $v(a_i) - v(a_j) = (j - i)\gamma$), ce qui entraîne que $v(\sum_i a_i c^i) = \min\{v(a_i) + i\gamma\}$. La valuation sur $A(c)$ est donc uniquement déterminée par la coupure de $\gamma$ dans $\Gamma_A$, c'est-à-dire, par $\Sigma(\xi)$.

Soit $d \in L$ tel que $v(d) = \delta$. Un tel $d$ existe par $\aleph_1$-saturation. Alors, si $a_0, \ldots, a_n \in A$ et $v(\sum_i a_i c^i) = v(a_j) + j\gamma$, on aura $w(\sum_i f(a_i) d^i) = w(f(a_j)) + jw(d)$, ce qui montre que l'isomorphisme $g : A(c) \to B(d)$ qui prolonge $f$ et envoie $c$ sur $d$ est bien un isomorphisme de corps valués.

Puisque $c \in A(a)$, nous avons $a \in A(c)^{alg}$. Par le cas 1, $f$ se prolonge à $A(c)^{alg}$.

**Cas 3**. Il existe $c \in A(a) \cap \mathcal{O}_v$, $\operatorname{res} c \notin k_A$.

Comme $k_A$ est algébriquement clos, cela entraîne que $\operatorname{res} c$ est transcendant sur $k_A$. Soit $d \in \mathcal{O}_w$ tel que $\operatorname{res} d$ soit transcendant sur $k_B$ (Un tel $d$ existe par $\aleph_1$-saturation de $L$).

Nous allons montrer que si $a_0, \ldots, a_n \in A$, alors $v(\sum_i a_i c^i) = \min\{v(a_i)\}$. En effet, il suffit de le montrer quand les $a_i$ ont tous même valuation, et, divisant par l'un d'entre eux, on peut suppose qu'ils sont tous de valuation 0. Alors $\operatorname{res}(\sum_i a_i c^i) = \sum_i \operatorname{res} a_i (\operatorname{res} c)^i$, et cet élément ne peut être nul, car $\operatorname{res} c$ est transcendant sur $k_A$. Donc $v(\sum_i a_i c^i) = 0$.

On raisonne de la même façon pour la valuation $w$ sur $B(d)$, et cela entraîne que l'isomorphisme d'anneaux $A[c] \to B[d]$ qui prolonge $f$ et envoie $c$ sur $d$ est en fait un isomorphisme d'anneaux valués, et se prolonge à $A(c)$. Comme $a$ est algébrique sur $A(c)$, le cas 1 nous permet de conclure.

**Cas 4**. $A(a)$ a le même corps résiduel que $A$ et le même groupe de valeurs.

Soit $I = \{v(a - c) \mid c \in A\}$. C'est donc un segment initial de $\Gamma_A$, sans élément maximal. La première assertion est évidente (si $v(d) < v(a - c)$ alors $v(a - c + d) = v(d)$), pour la seconde, soit $e \in A$ tel que $v(e) = v(a - c)$. Alors $v((a - c)/e) = 0$, et puisque $A(a)$ a le même corps résiduel que $A$, il existe $d \in A$ tel que $v((a - c)/e - d) > 0$, ce qui entraîne que $v(a - c - de) > v(a - c)$.

Considérons l'ensemble $\Sigma(x)$ de $\mathcal{L}(B)$-formules $\{w(x-f(c)) = w(f(d)) \mid c, d \in A,\ v(a-c) = v(d)\}$. Ici, bien sûr, la formule $v(x) = v(y)$ est une abréviation pour la formule $s \operatorname{div} y \wedge y \operatorname{div} x$. Cet ensemble est finiment satisfaisable dans $N$ : en effet, soient $(c_1, d_1), \ldots, (c_n, d_n) \in A$, et $e \in A$ tel que $v(e-a) > v(a-c_i)$ pour tout $i = 1, \ldots, n$. Alors $v(e-c_i) = v(e-a+a-c_i) = v(a-c_i)$. Puisque $f$ est un $\mathcal{L}_{\mathrm{div}}$-isomorphisme, nous avons donc que $f(e)$ satisfait $w(x - f(c_i)) = w(d_i)$ pour tout $i = 1, \ldots, n$.

Par $\aleph_1$-saturation de $N$, il existe donc un élément $b$ de $N$ qui satisfait toutes les formules de $\Sigma(x)$. Comme $B$ est algébriquement clos, cet élément est transcendant sur $B$, et $f$ se prolonge à un isomorphisme de corps $A(a) \to B(b)$ qui envoie $a$ sur $b$. Il suffit maintenant de montrer que c'est un isomorphisme de corps valués. Soit $P(T) \in A[T]$ un polynôme. Comme $A$ est algébriquement clos, nous avons $P(T) = c\prod_{i=1}^{\deg(f)}(T - a_i)$ pour des éléments $a_i$ et $c$ de $A$. Cela entraîne que $v(P(a)) = v(c) + \sum_{i=1}^{\deg(P)} v(a - a_i)$. Similairement, comme $f(P(a)) = f(c)\prod_{i=1}^{\deg(P)}(b - f(a_i))$, on a $w(f(P(a)) = w(f(c)) + \sum_{i=1}^{\deg(f)} w(b - f(a_i)) = f(v(c)) + \sum_{i=1}^{\deg(P)} f(v(a-a_i))$, ce qui prouve que $f$ définit bien un isomorphisme de corps valués, et donc de $\mathcal{L}_{\mathrm{div}}$-structures.

**2.15. Corollaire**. Les complétions de la théorie des corps valués dans le langage $\mathcal{L}_{\mathrm{div}}$ est obtenue en précisant la caractéristique du corps valué et celle du corps résiduel.

*Démonstration.* Le type d'isomorphisme du sous-anneau d'un corps valué engendré par 1 nous donne la caractéristique du corps ($p = 0$ pour un premier $p$, ou bien $p \neq 0$ pour tout premier), et celle du corps résiduel ($\neg(p \operatorname{div} 1)$ si elle est égale à $p$ ; $p \operatorname{div} 1$ pour tout premier $p$ si elle est nulle).

**2.16. Quelques remarques**.

(1) Le résultat est faux si on n'a pas ajouté à la théorie des corps algébriquement clos valués l'axiome $\exists x\ x \neq 0 \wedge \neg(x \operatorname{div} 1)$. En effet, par exemple si on considère un corps algébriquement clos valué $K$ de valuation non triviale et de caractéristique résiduelle 0, alors la clôture algébrique de $\mathbb{Q}$ dans $K$ est une sous-structure, est un corps algébriquement clos (mais de valuation triviale), et donc $(\mathbb{Q}, v) \not\prec (K, v)$. (J'ai un peu tendance à oublier que la valuation triviale existe, faites attention).

(2) Nous avons vu que les extensions transcendantes sont de trois types (deux à deux incompatibles) : extension du groupe de valeurs (cas 2 ; appelé *purement ramifié*), du corps résiduel (cas 3 ; appelé *purement résiduel*, ou bien aussi *purement inertiel*), ou bien enfin *immédiate* (cas 4). Ces trois types d'extensions se retrouveront aussi dans le cas des extensions algébriques, mais nous aurons dans ce cas des extensions qui mélangent les trois types d'extensions.

**2.17.** La démonstration du théorème montre que en fait, la théorie des corps valués algébriquement clos et de valuation non-triviale admet l'élimination des quantificateurs dans tout langage $\mathcal{L}'$ tel que la $\mathcal{L}'$-structure de $K$ soit définissable dans la $\mathcal{L}_{\mathrm{div}}$-structure $K$, et tel que tout $\mathcal{L}'$-isomorphisme entre des sous-structures induise un isomorphisme de corps valués. On montre facilement le résultat suivant :

**Théorème**. La théorie des structures à trois sortes associées à des corps algébriquement clos valués de valuation non triviale élimine les quantificateurs.

Il faut cependant faire un peu attention : les sous-structures de la structure à 3 sortes associée à un corps valué ne proviennent pas nécessairement d'un corps valué : il est en effet possible que les applications res ou $v$ ne soient pas surjectives dans une sous-structure.

Un des résultats qui en découle, et que je vous conseille d'essayer de montrer, est le suivant :

**2.18. Exercice**. Montrez que la théorie des groupes abéliens divisibles (non triviaux) totalement ordonnés élimine les quantificateurs. Montrez aussi qu'elle est complète.

Dans la preuve, j'ai aussi utilisé implicitement le résultat suivant :

**2.19. Exercice**. Soit $M$ une $\mathcal{L}$-structure, qui est $\kappa$-saturée. Soit $N$ une $\mathcal{L}'$-structure qui est interprétable dans la $\mathcal{L}$-structure $M$. Alors $N$ est $\aleph_1$-saturée.

**2.20. Le langage de Pas**. J. Pas, dans sa thèse, a introduit un langage à 3 sortes un peu différent de celui que nous avons introduits précédemment, et qui lui permet de montrer une élimination des quantificateurs uniforme.

Les corps valués qu'il considère sont des corps valués Henséliens de **caractéristique résiduelle nulle** (et donc aussi de caractéristique nulle). Il suppose que ces corps sont munis d'une *composante angulaire*, c'est-à-dire, d'une application $\overline{\text{ac}}$ du corps dans le corps résiduel, qui satisfait aux conditions suivantes, si $(K, v)$ est un corps valué de corps résiduel $k_v$ :

(i) $\overline{\text{ac}}(0) = 0$.

(ii) La restriction de $\overline{\text{ac}}$ à $K^\times$ définit un morphisme de groupes multiplicatif : $K^\times \to k_v^\times$, qui coïncide avec l'application res sur les éléments de valuation 0.

Notons que nous avons mis une structure additionnelle sur le corps valué $(K, v)$ : l'application $\overline{\text{ac}}$ n'est pas définissable dans $\mathcal{L}_{\text{div}}$.

Le langage de base qu'il considère est le langage à trois sortes : la sorte de corps, la sorte du groupe de valeurs et la sorte du corps résiduel. Chaque sorte vient avec son langage, qui est celui des corps pour les deux corps, et des groupes ordonnés avec un symbole $\infty$, comme dans 1.10. Nous avons aussi les applications $v : K \to \Gamma_v \cup \{\infty\}$ et $\overline{\text{ac}} : K \to k_v$, mais nous n'avons pas l'application res. Cependant elle est définissable : elle coïncide avec $\overline{\text{ac}}$ sur $\mathcal{O}_v^\times$, et est égale à 0 sur $\mathcal{M}_v$. Comme $\mathcal{O}_v$ et $\mathcal{M}_v$ sont définissables, tout va bien. La classe des corps Henséliens de caractéristique nulle avec une composante angulaire forme bien une classe élémentaire dans ce langage.

Le théorème qu'il montre est le suivant :

**Théorème**. La théorie $T_{Pas}$ des corps valués Henséliens de caractéristique résiduelle nulle et ayant une composante angulaire, élimine les quantificateurs de corps.

C'est à dire, étant donnée une formule $\Phi(x, \xi, \bar{u})$, où $x$ est un uplet de variables du corps, $\xi$ de variables du groupe, et $\bar{u}$ de variables du corps résiduel, il existe une formule $\Psi(x, \xi, \bar{u})$, dans laquelle les seules variables quantifiées sont celles de corps résiduel ou de groupe, et qui est équivalente à $\Phi$ modulo $T$.

Ce résultat permet de montrer des résultats d'uniformité sur l'élimination des quantificateurs dans les corps $p$-adiques (bien que ceux-ci ne soient pas dans la classe que nous considérons, mais grâce au théorème d'Ax et Kochen). Je laisse à plus tard la démonstration des résultats de Pas, nous allons d'abord montrer des résultats plus classiques.

**2.21. Exemples**. Soit $\mathbb{C}((t))$ le corps des séries formelles sur $\mathbb{C}$, avec la valuation triviale sur $\mathbb{C}$, et $v(\sum_{i\geq i_0} a_i t^i) = i_0$ si $a_{i_0} \neq 0$. Alors on peut tout simplement définir $\overline{\text{ac}}(\sum_{i\geq i_0} a_i t^i) = a_{i_0}$. C'est-à-dire, le premier coefficient non nul de la série.

En fait, plus généralement, on dit qu'un corps valué $(K, v)$ *a une section* s'il existe un homomorphisme de groupe $s : \Gamma \to K$ tel que $v \circ s = id$. Il est clair que $\mathbb{C}((t))$ a une section : on définit $s(n) = t^n$ pour $n \in \mathbb{Z}$. On peut alors définir une composante angulaire en posant $\overline{\text{ac}}(a) = \text{res}\,(as(-v(a))$ si $a \neq 0$, et $\overline{\text{ac}}(0) = 0$.

Le corps des $p$-adiques a aussi une composante angulaire, puisqu'il a une section (définie par $s(n) = p^n$).

En général. on ne peut pas définir la section à partir de la composante angulaire. En effet, revenons au corps valué $\mathbb{C}((t))$. Nous allons montrer qu'il existe un automorphisme de $\mathbb{C}((t))$ qui fixe $\mathbb{C}$, respecte la valuation et l'application $\overline{\text{ac}}$, mais bouge $t$ (et donc ne preserve pas la section). Soit $u \in \mathbb{C}[[t]]$, et considérons l'élément $w = t(1 + tu)$. Alors $v(w) = v(t) = 1$, et on vérifie facilement que si l'on définit $\varphi(\sum_{i=0}^{\infty} a_i t^i)$ par $\sum_{i=0}^{\infty} a_i w^i$, alors cette application est bien définie, est un isomorphisme d'anneaux valués qui commute avec $\overline{\text{ac}}$, et s'étend à $\mathbb{C}((t))$. Elle envoie $\mathbb{C}(t)$ sur $\mathbb{C}(w)$. Mais comme $\mathbb{C}(w)$ est dense dans $\mathbb{C}((t))$ pour la topologie, et que $\mathbb{C}((t))$ est complet, cela entraîne que ce morphisme est surjectif.

**Bibliographie**.

[AM ]M.F. Atiyah, I.G. MacDonald *Introduction to Commutative Algebra*, Addison-Wesley, Reading, 1969.

[CK ]C.C. Chang, H.J. Keisler, Model theory, North-Holland, Amsterdam 1977 .

[E ]D. Eisenbud, *Commutative Algebra*, Graduate Texts in Math. 150, Springer-Verlag New York, 1995.

[EP ]A.J. Engler, A. Prestel, *Valued fields*, Springer-Verlag 2005.

[H ]W. Hodges, A shorter model theory, Cambridge University Press, 1997.

[L ]S. Lang, *Algebra*, 2nd edition, Addison-Wesley Pub. Co., Menlo Park 1984.

[Mr ]D. Marker, *Model Theory: An Introduction*, Springer-Verlag 2002.

[Mt ]H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Adv. Math. 8, Cambridge University Press, Cambridge, 1986.

[P ]J. Pas, Uniform $p$-adic cell decomposition and local zeta functions, J. reine angew. Math. 399 (1989), 137 – 172.

[Po ]B. Poizat, Cours de Théorie des Modèles, Nur Al-Mantiq Wal-Ma'rifah, Paris 1985.

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

[Ro ]A. Robinson, *Complete Theories*, North Hollan, Amsterdam 1956.

[S ]O.F.G. Schilling, *The Theory of Valuations*, Math. Surveys No 4, A.M.S. Publications, New York 1950.

[Sh ]I.R. Shafarevich, *Basic Algebraic Gemoetry 1 and 2*, 2nd ed., Springer Verlag 1994.

[ZS ]O. Zariski, P. Samuel, *Commutative Algebra Vol. 1 and 2*, Graduate Texts in Mathematics 28, Springer-Verlag New York 1986.

Chang et Keisler, Hodges et Poizat sont de bons livres de référence pour la théorie des modèles. Marker est plus récent, et est plus axé sur la théorie des modèles appliquée. Pour l'algèbre commutative, je consulte souvent Lang (contient toutes les bases d'algèbre), Eisenbud (très complet mais aussi très gros), Zariski et Samuel, Shafarevich. D'autres textes classiques sont ceux de Atiyah et MacDonald (je le trouve parfois un peu concis) et de Matsumura. Pour la théorie des valuations, Ribenboim et Schilling. Il existe aussi une nouvelle version du livre de Ribenboim, assez différente (*Classical theory of valuation*, je crois, publié chez Springer). Tout à fait récent, mais je ne l'ai pas encore regardé à fond, le livre d'Engler et Prestel. A noter : Prestel a aussi un très joli livre sur la théorie des modèles des corps $p$-adiquemenht clos, dans les Springer Lecture Notes.

# 3 Les corps Henséliens. Extensions algébriques de corps valués

## 3.1 Formule de Taylor

**3.1. Formule de Taylor en caractéristique positive**. Soit $K$ un corps de caractéristique 0, $f(X) \in K[X]$. Alors nous avons la formule de Taylor qui nous permet de calculer $f(X+Y)$ :

$$f(X+Y) = \sum_{i=0}^{\deg(f)} \frac{f^{(i)}(X)}{i!} Y^i,$$

où $f^{(i)}(X)$ dénote la $i$-ième dérivée de $f(X)$. En caractéristique $p > 0$, cette formule ne marche pas (si $i \geq p$, alors $i! = 0$), cependant elle a un analogue.

Pour chaque paire d'entiers $i$ et $n$ on définit $D_i(X^n)$ comme étant le coefficient de $Y^i$ dans $(X+Y)^n$, vu comme un polynôme en $Y$. On voit que $D_0(X^n) = X^n$, $D_1(X^n) = nX^{n-1}$, ..., $D_n(X^n) = 1$, et $D_i(X^n) = 0$ pour $i > n$. Ces fonctions sont calculables par récurrence. On pose ensuite, pour $i \in \mathbb{N}$, $a_0, \ldots, a_n \in K$,

$$D_i(\sum_{j=0}^{n} a_j X^j) = \sum_{j=0}^{n} a_j D_i(X^j).$$

L'application $D_i$ définit donc une application $K$-linéaire de $K[X]$ dans $K[X]$, et on vérifie aisément que pour tout $f(X) \in K[X]$ on a

$$f(X+Y) = \sum_{i=0}^{\deg(f)} D_i(f(X)) Y^i.$$

J'appellerai cette formule la formule de Taylor. Si $a \in K$, alors $D_i(f)(a)$ dénotera l'évaluation du polynôme $D_i(f(X))$ en $a$.

## 3.2 Les corps Henséliens

**3.2.** Un corps valué $(K, v)$ est *Hensélien* si, pour tout polynôme $f(T) \in \mathcal{O}_v[T]$ et $a \in \mathcal{O}_v$ tel que $\operatorname{res} f(a) = 0$ et $\operatorname{res} f'(a) \neq 0$, il existe $b \in \mathcal{O}_v$ tel que $f(b) = 0$ et $\operatorname{res} a = \operatorname{res} b$.

**Proposition**. Soit $K$ un corps valué de groupe de valeurs archimédien, et qui est complet. Alors $K$ est Hensélien.

*Démonstration.* Nous allons construire une suite de Cauchy $(a_n)$, et montrer qu'elle converge vers une solution de $f(T) = 0$. On démarre avec $a_0 = a$. Posons $a_1 = a_0 - f(a)/f'(a)$. Puisque $v(f'(a)) = 0$, cet élément est dans $\mathcal{O}_v$ et on a $v(a_1 - a_0) = v(f(a)) =: \gamma$. De plus, en utilisant la formule de Taylor,

$$f(a_1) = f(a) + f'(a)(a_1 - a) + \sum_{n=2}^{\deg(f)} D_n(f)(a)(a_1 - a)^n = \sum_{n=2}^{\deg(f)} D_n(f)(a)(a_1 - a)^n,$$

on obtient que $v(f(a_1)) \geq 2v(a-a_1) = 2\gamma$, car $\gamma > 0$. Comme $\operatorname{res} a = \operatorname{res} a_1$, on a aussi $\operatorname{res} f'(a_1) \neq 0$.

On itère la procédure : supposons que nous ayions trouvé $a_n$ avec $v(f(a_n)) \geq 2^n\gamma$, $\operatorname{res} a_n = \operatorname{res} a$. On prend alors $a_{n+1} = a_n - f(a_n)/f'(a_n)$, et on vérifie que $v(f(a_{n+1})) \geq v(a_{n+1}-a_n)^2 = 2v(f(a_n))$.

Nous avons donc trouvé une suite $(a_n)$ telle que, pour tout $n$, $v(f(a_n)) = v(a_{n+1}-a_n) \geq 2^n\gamma$. Si $m > n$ on a alors que $v(a_m - a_n) = v(a_{n+1} - a_n)$, on peut donc trouver un élément $b \in \mathcal{O}_v$ qui est limite de cette suite. On aura alors $v(f(b)) \geq v(f(a_n))$ pour tout $n$, et comme la suite $v(f(a_n))$ est cofinale dans $\Gamma$ (puisque $\Gamma$ est archimédien), on a $v(f(b)) = \infty$, i.e., $f(b) = 0$.

La technique utilisée pour construire cette suite est appelée une *approximation de Newton.*

**3.3. Remarques**.

(1) Si $b \in \mathcal{O}_v$, alors
$$v(b) > 0 \iff b \in \mathcal{M}_v \iff \operatorname{res}(b) = 0.$$

(2) Soient $(K, v)$ un corps valué, $f(T) \in \mathcal{O}_v[T]$ et $a, b \in \mathcal{O}_v$ tels que $v(f(a)) > v(f'(a)) = 0$, $f(b) = 0$ et $v(b-a) > 0$. Alors $b$ est l'unique élément de $\mathcal{O}_v$ satisfaisant $f(x) = 0$ et $v(x-a) > 0$, et de plus on a $v(b-a) = v(f(a))$.

*Démonstration.* (1) est évident, nous montrons (2). Supposons qu'il existe $c \neq b$ satisfaisant ces conditions. Puisque $b \neq c$, le polynôme $(T-b)(T-c)$ divise $f(T)$ (dans $\mathcal{O}_v[T]$). Quand on applique res aux coefficients de $f(T)$, on obtient donc que $(T - \operatorname{res} b)(T - \operatorname{res} c)$ divise $\operatorname{res}(f)(T)$. Cela entraîne, comme $\operatorname{res} a = \operatorname{res} b = \operatorname{res} c$, que $\operatorname{res}(f'(a)) = 0$, et contredit notre hypothèse. Donc l'élément $b$ est unique.

En utilisant la formule de Taylor on a :
$$0 = f(b) = f(a) + f'(a)(b-a) + \sum_{i=2}^{\deg(f)} D_i(f)(a)(b-a)^i.$$
Comme $v(f'(a)) = 0$ et $v(b-a) > 0$, on a alors que pour tout $i \geq 2$, $v(D_i(f)(a)(b-a)^i) > v(f'(a)(b-a))$, ce qui entraîne $v(f'(a)(b-a)) < v(\sum_{i=2} \deg(f) \frac{D_i(f)(a)}{i!}(b-a)^i)$. Nous avons nécessairement $v(f'(a)(b-a)) = v(f(a))$, ce qui donne le résultat.

## 3.3 Rappels rapides sur la théorie de Galois

**3.4.** Soient $K$ un corps, $0 \neq f(X) \in K[X]$. On dit que $f(X)$ est *séparable* si sa dérivée n'est pas identiquement nulle. Si $K$ est de caractéristique 0, alors tous les polynômes non nuls sonst séparables. Si $K$ est de caractéristique $p > 0$, alors les polynômes non séparables sont exactement ceux qui s'ecrivnet $h(X^p)$, où $h(X) \in K[X]$. On montre aussi que si $f(X) \in K[X]$ alors il existe $m \in \mathbb{N}$ et un polynôme séparable $h(X) \in K[X]$ tels que $f(X) = h(X^{p^m})$.

Si $f(X) \in K[X]$ est irréductible, il engendre un idéal maximal de $K[X]$, et $K[X]/(f(X))$ est un corps. La clôture algébrique de $K$ (dans un grand corps algébriquement clos $L$ le contenant)

est notée $K^{alg}$, et est l'ensemble de tous les éléments (de $L$) qui sont algébriques sur $K$. Les éléments de $K^{alg}$ dont le polynôme minimal sur $K$ est séparable, sont dits *séparables sur* $K$, et ils forment un sous-corps de $K^{alg}$ noté $K^{sep}$. Si $a \in K^{alg}$, alors il existe $m \in \mathbb{N}$ tel que $a^{p^m} \in K^{sep}$. Donc tout automorphisme de $K^{sep}$ s'étend de façon unique à $K^{alg}$ : si $a^{p^m} \in K^{sep}$, on pose $\sigma(a)l$ l'unique élément $b$ de $K^{alg}$ satisfaisant $b^{p^m} = \sigma(a^{p^m})$. Par abus de notation, je dénoterai par $\mathcal{G}al(K^{alg}/K)$ le groupe des automorphismes de $K^{alg}$ qui sont l'identité sur $K$. Si $a \in K^{alg}$, le *polynôme minimal de a sur* $K$ est le polynôme unitaire $f(X)$ de degré minimal qui s'annule en $a$, et il sera irréductible. Si $a$ est séparable sur $K$, alors toutes les racines de son polynôme minimal sur $K$ seront simples. Par contre, si $a$ n'est pas séparable sur $K$, alors toutes les racines de son polynôme minimal seront d'ordre une puissance de $p$ (plus précisément, si $m$ est le plus petit entier tel que $a^{p^m}$ soit séparable sur $K$, elles seront d'ordre $p^m$. Une extension de $K$ de la forme $K(a)$ où $a^{p^m} \in K$, $a \notin K$, est appelée une extension *purement inséparable* de $K$.

Une extension algébrique de $K$ est *séparable* si tous ses éléments sont séparables sur $K$ (elle est donc contenue dans $K^{sep}$). Elle est *normale* si pour tout $a \in L$, si $f(X)$ est le polynôme minimal de $a$ sur $K$, alors $L$ contient toutes les racines de $f(X)$. Notons que si $b$ est une autre racine de $f(X)$, alors les corps $K(a)$ et $K(b)$ sont $K$-isomorphes, et il existe donc un élément de $\mathcal{G}al(K^{alg}/K)$ qui envoie $a$ sur $b$.

L'extension $L$ est *Galoisienne*, ou *de Galois*, si elle est normale et séparable. Le groupe des automorphismes de $L$ qui fixe $K$ est alors dénoté par $\mathcal{G}al(L/K)$. (Nous utiliserons aussi cette notation si $L$ est seulement normale).

**Important** : Si $L$ est une extension finie séparable de $K$, alors il existe un élément $a \in L$ tel que $L = K(a)$. Si $[L : K] = n$, alors le polynôme minimal $f(X)$ de $a$ sur $K$ a exactement $n$ racines (qui sont distinctes), et si $L$ est Galois sur $K$, alors $|\mathcal{G}al(L/K)| = n$

Supposons que $L$ soit une extension de Galois de $K$ de degré fini, et soit $G = \mathcal{G}al(L/K)$. Si $M$ est un sous-corps de $L$ contenant $K$, nous définissons $G(M) = \{\sigma \in G \mid \forall a \in M,\ \sigma(a) = a\}$, et si $H$ est un sous-groupe de $G$, nous définissons $L^H = \{a \in L \mid \forall \sigma \in H,\ \sigma(a) = a\}$, le *sous-corps de L fixé par H*. Notons que $L^H = G$, et $L^{(1)} = L$.

**Théorème fondamental de la théorie de Galois**. Soit $L$ une extension de Galois finie de $K$, $G = \mathcal{G}al(L/K)$, $H$ un sous-groupe de $G$, et $M$ un sous-corps de $L$ contenant $K$. Alors

$$L^{G(M)} = M \qquad G(L^H) = H, \qquad H \text{ distingué} \leftrightarrow L^H \text{ normale sur } K.$$

De plus, si $H$ est un sous-groupe normal de $G$, alors $L^H$ est une extension de Galois de $K$, et $G/H$ est naturellement isomorphe à $\mathcal{G}al(L^H/K)$.

Pour plus de détails, voir n'importe quel livre d'algèbre. Si $L$ est une extension de Galois infinie de $K$, son groupe d'automorphisme sur $K$, $\mathcal{G}al(L/K)$, peut alors être décrit comme une limite projective du système de groupes finis $\mathcal{G}al(M/K)$, où $M$ parcourt l'ensembles des extensions de Galois finies de $K$ qui sont contenues dans $L$. Cela nous donne une topologie sur $\mathcal{G}al(L/K)$, ayant pour base d'ouverts les translatés des sous-groupes $\mathcal{G}al(L/M)$, $M$ une extensions finie de $K$ contenue dans $L$. Le groupe sera compact et Haussdorff pour cette

topologie. La dualité de Galois marche pas aussi, mais il faut faire attention à la topologie, et on a :

$$\text{sous-groupes } \textbf{fermés} \text{ de } \mathcal{G}al(L/K) \leftrightarrow \text{corps } M \text{ avec } K \subset M \subset L.$$

## 3.4 Extensions algébriques de corps valués

**3.5. Extensions de corps valués**. On a vu dans la preuve du cas 2 du Théorème 2.14 que si $K$ est un corps algébriquement clos, et si $a$ appartient à un corps valué étendant $K$, $a \notin K$, alors le corps valué pouvait être de trois types, chacun de ces types étant relativement facile à traiter. Ecrivons $L = K(a)$, et $k_K, k_L, \Gamma_K, \Gamma_L$ les corps résiduels et groupes de valeurs associés. Notons que l'on a toujours $k_K \subset k_L$ et $\Gamma_K \subset \Gamma_L$ (la deuxième assertion est évidente, la première vient du fait que $\mathcal{O}_K \subset \mathcal{O}_L$ et $\mathcal{M}_L \cap \mathcal{O}_K = \mathcal{M}_K$). Alors, l'extension $L/K$ était de l'un des types suivants :

(i) $k_L$ contient strictement $k_K$, et $\Gamma_K = \Gamma_L$.

(ii) $k_K = k_L$, et $\Gamma_L$ contient strictement $\Gamma_K$.

(iii) $k_K = k_L$ et $\Gamma_K = \Gamma_L$.

Dans le cas (i), on dit que l'extension $L/K$ est totalement résiduelle ou inertielle, dans le cas (ii) qu'elle est totalement ramifiée et dans le cas 3 qu'elle est immédiate. Le fait que $a$ était un singleton, et que $K$ était algébriquement clos était crucial : comme on le verra ci-dessous, si $K$ n'est pas algébriquement clos et $a$ est algébrique sur $K$, alors en général, si $v$ est une valuation sur $K(a)$ étendant celle de $L$, alors l'extension $K(a)/K$ peut s'écrire comme une extension immédiate d'une extension ramifiée d'une extension résiduelle. Les choses se compliquent donc grandement, et nous allons un peu voir ce qui se passe.

**3.6. Quelques définitions et un peu de notation**. Soit $(L, w)$ une extension finie du corps valué $(K, v)$. Si $[k_L : k_K] = [L : K]$ on dira que $L/K$ est (purement) *inertielle* ; si $[\Gamma_L : \Gamma_K] = [L : K]$ que $L/K$ est *totalement ramifiée* ; et si $\Gamma_L = \Gamma_K$ et $k_L = k_K$, que $L/K$ est *immédiate*. Si $\Gamma_L \neq \Gamma_K$, on dira que $L/K$ est *ramifiée*. Attention, ces notions dépendent de la valuation $w$ choisie : il se peut que $L$ soit inertielle pour $w$ et ramifiée pour une autre extension $w'$ de $v$. En cas d'ambiguité possible, il vaut mieux alors préciser la valuation $w$. Les notations utilisées seront :

- $e(L/K, w)$ pour $[w(L^\times) : \Gamma_K]$, appellé l'*indice de ramification de $v$ dans $(L, w)$*, ou bien encore *de $w$ sur $K$* (mais parfois je risque de dire "degré").
- $f(L/K, w)$ pour $[k_L : k_K]$, appellé le *degré d'inertie de $w$ sur $K$*.

**3.7. Lemme**. Soient $(K, v) \subset (L, w)$ deux corps valués. Soient $a_1, \dots a_r \in \mathcal{O}_w$ tels que $\operatorname{res} a_1, \dots, \operatorname{res} a_r$ soient $k_K$-linéairement indépendants (dans le $k_K$-espace vectoriel $k_L$), et soient $b_1, \dots, b_s \in L^\times$ tels que les cosets $w(b_i) + \Gamma_K$ sont deux à deux disjoints. Alors, les éléments $a_i b_j$, $1 \leq i \leq r$, $1 \leq j \leq s$, sont $K$-linéairement indépendants.

*Démonstration.* Soient $c_{ij} \in K$, non tous nuls, $1 \leq i \leq r$, $1 \leq j \leq s$. Nous allons montrer que

$$w(\sum_{i,j} c_{ij}a_ib_j) = \min_{i,j}\{w(b_j) + v(c_{ij})\}.$$

Cela entrainera que $\sum_{i,j} c_{ij}a_ib_j$ ne peut être nul, et donc le résultat.

Posons $\delta = \min_{i,j}\{v(c_{ij}) + w(b_j)\}$, et soit $I$ l'ensemble des paires $(i,j)$ telles que $v(c_{ij}) + w(b_j) = \delta$. Par 1.4, $w(\sum_{(i,j)\notin I} c_{ij}a_ib_j) > \delta$, et il suffit de montrer que $w(\sum_I c_{ij}a_ib_j) = \delta$. Notons d'abord que les indices $j$ qui apparaissent dans les paires de $I$ sont tous égaux : si $j \neq j'$, alors $w(b_j)$ et $w(b_{j'})$ sont dans des cosets disjoints de $\Gamma_K$ dans $\Gamma_L$, et leur différence ne peut être dans $\Gamma_K$. Soit $(i_0, j) \in I$ ; divisant par $c_{i_0j}b_j$ et posant $d_i = c_{i_0j}^{-1}c_{ij}$, il suffit donc de montrer que

$$w(\sum_{(i,j)\in I} d_ia_i) = 0, \text{ c'est-à-dire, que res}\,(\sum_{(i,j)\in I} d_ia_i) \neq 0.$$

La dernière inégalité provient du fait que les éléments $\operatorname{res} a_i$ sont $k_K$-linéairement indépendants, et que $d_{i_0} = 1$.

**3.8. Corollaires/Remarques**. Avec les mêmes notations, si l'on suppose de plus que $[L : K] = n$ :

(1) $r \leq f(L/K, w)$ et $s \leq e(L/K, w)$.

(2) Nous avons montré que $w(\sum_{ij} c_{ij}a_ib_j) = \min_{ij}\{w(c_{ij}a_ib_j)\}$, ce qui est bien pratique si $n = e(L/K, w)f(L/K, w)$ : nous pouvons trouver une base du $K$-espace vectoriel $L$ à partir de laquelle il est facile de calculer la valuation de $L$.

(3) $e(L/K, w)f(L/K, w) \leq n$.

**3.9. Extensions de Galois finies : groupes de décomposition et d'inertie.** Soient $(K, v) \subset (L, w)$ deux corps valués, avec $L$ une extension de Galois de $K$ de degré $n$. Nous posons $G = \mathcal{G}al(L/K)$. Nous savons déja que toutes les valuations sur $L$ qui étendent $v$ sont obtenues (à équivalence près) en composant avec un automorphisme de $L$ sur $K$, c.f. Théorème 2.7. De plus, si $\mathcal{O}$ dénote la clôture intégrale de $\mathcal{O}_v$ dans $L$, et si $\mathcal{M}_w$ dénote l'idéal maximal de l'anneau de valuation de la valuation $w$ (et $\mathcal{M}_{w'}$ celui de $w'$), alors on a $w = w'$ si et seulement si $\mathcal{O} \cap \mathcal{M}_w = \mathcal{O} \cap \mathcal{M}_{w'}$, puisque l'anneau de valuation de $w$ est obtenu en *localisant* $\mathcal{O}$ *en* $\mathcal{M}_w \cap \mathcal{O}$, c'est-à-dire, en ajoutant les inverses des éléments de $\mathcal{O} \setminus \mathcal{M}_w$, et de même pour l'anneau de valuation de $w'$. Notons aussi que si $w$ et $w'$ ne sont pas équivalentes, alors on aura que $1 \in \mathcal{M}_w \cap \mathcal{O} + \mathcal{M}_{w'} \cap \mathcal{O}$, car ces idéaux sont maximaux (voir Proposition 2.4). De plus, le morphisme $\mathcal{O}/\mathcal{M}_w \cap \mathcal{O} \to \mathcal{O}_w/\mathcal{M}_w$ est un isomorphisme (surjectif). On remarque aussi que, puisque $w' = w \circ \sigma$ pour un $\sigma \in \mathcal{G}al(L/K)$, on aura

$$e(L/K, w) = e(L/K, w'), \quad f(L/K, w) = f(L/K, w')$$

et nous pourrons donc omettre $w$ de la notation.

On définit le *groupe de décomposition de $w$ dans $L$* comme étant le sous-groupe

$$G_{\mathrm{dec},w} = G_{\mathrm{dec}} = \{\sigma \in G \mid \sigma(\mathcal{M}_w) = \mathcal{M}_w\}.$$

Ce sera donc le groupe d'automorphismes du corps valué $(L, w)$ sur $K$.

Notons que si $w' = w \circ \tau$, on a : $a \in \mathcal{M}_{w'} \iff w'(a) > 0 \iff w(\tau(a)) > 0 \iff \tau(a) \in \mathcal{M}_w \iff a \in \tau^{-1}(\mathcal{M}_w)$, c'est-à-dire $\mathcal{M}_{w'} = \tau^{-1}(\mathcal{M}_w)$. On vérifie facilement alors que $\sigma(\mathcal{M}_{w'}) = \mathcal{M}_{w'} \iff \tau\sigma\tau^{-1} \in G_{\mathrm{dec}}$, c'est-à-dire que le groupe de décomposition de $w'$ est $\tau^{-1}G_{\mathrm{dec},w}\tau$. Nous avons aussi, pour $\tau_1, \tau_2 \in G$ : $\tau_1^{-1}(\mathcal{M}_w) = \tau_2^{-1}(\mathcal{M}_w) \iff \tau_2\tau_1^{-1} \in G_{\mathrm{dec}} \iff G_{\mathrm{dec}}\tau_1 = G_{\mathrm{dec}}\tau_2$. Cela entraîne que $v$ a exactement $[G : G_{\mathrm{dec}}] = g$ extensions non-équivalentes à $L$, et que si $\tau_1, \cdots, \tau_g \in G$ sont tels que $G$ est la réunion disjointe des $G_{\mathrm{dec}}\tau_i$, alors les extensions de $w$ sont $w_1, \ldots, w_g$, où $w_i = w \circ \tau_i$. (Terminologie : chaque $G_{\mathrm{dec}}\tau_i$ est appelé un *coset à droite de $G_{\mathrm{dec}}$ dans $G$*, et l'ensemble $\{\tau_1, \ldots, \tau_g\}$ défini ci-dessus est un *système de représentants dans $G$ des cosets à droite de $G_{\mathrm{dec}}$ dans $G$*. De même, $\tau G_{\mathrm{dec}}$ est appelé un *coset à gauche de $G_{\mathrm{dec}}$ dans $G$*.)

Le sous-corps de $L$ fixé par les éléments de $G_{\mathrm{dec}}$ est appellé le *corps de décomposition de $w$ dans $L$*, et noté parfois $L^{\mathrm{dec}}$. Remarquons que $[L^{\mathrm{dec}} : K] = [G : G_{\mathrm{dec}}]$, et que $G_{\mathrm{dec}} = \mathcal{G}al(L/L^{\mathrm{dec}})$ (Ici nous utilisons l'hypothèse de séparabilité de $L$ sur $K$).

On pourrait aussi définir le groupe de décomposition de $w$ comme étant $\{\sigma \in G \mid \sigma(\mathcal{O}_w) = \mathcal{O}_w\}$, ou bien comme $\{\sigma \in G \mid \sigma(\mathcal{M}_w) \cap \mathcal{O} = \mathcal{M}_w \cap \mathcal{O}\}$. Le groupe $G_{\mathrm{dec}}$ est parfois noté $G_w$, $G_{\mathcal{M}_w}$, $G_{-1}$, etc. . Notons que si $\sigma \in G_{\mathrm{dec}}$, alors $\sigma$ induit un automorphisme $\bar{\sigma}$ de $k_L$ sur $k_K$ : on définit $\bar{\sigma}(\mathrm{res}\, a) = \mathrm{res}\,(\sigma(a))$, si $a \in \mathcal{O}_w$. Cette définition ne dépend pas du choix de $a$, puisque si $(a - b) \in \mathcal{M}_w$ alors $\sigma(a) - \sigma(b) \in \mathcal{M}_w$ par définition de $G_{\mathrm{dec}}$.

Le noyau de l'application $G_{\mathrm{dec}} \to \mathcal{G}al(k_L/k_K)$ est appellé le *groupe d'inertie de $w$ dans $L$* (ou *de $w$ sur $K$*). Il peut aussi être défini de la manière suivante : c'est l'ensemble des éléments $\sigma \in \mathcal{G}al(L/K)$ tels que pour tout $a \in \mathcal{O}$ on a $w(a - \sigma(a)) > 0$. On le note parfois $G_0$.

Parce que en fait, on peut définir d'autres sous-groupes de $G$ : si $\gamma \in \Gamma_L$ est positif, on peut définir $G_\gamma = \{\sigma \in G \mid \forall a \in \mathcal{O},\ w(a - \sigma(a)) > \gamma.\}$. Ces groupes, appelés *groupes de ramification supérieure*, sont utilisés quand la caractéristique résiduelle est positive. On peut trouver plus de détails dans le livre de Serre, *Corps locaux*. Nous ne les utiliserons pas.

**3.10. Proposition**. Hypothèses et notation comme ci-dessus.

(1) $L^{\mathrm{dec}}$ est le plus petit sous-corps $E$ de $L$ contenant $K$ et tel que $\mathcal{M}_w \cap \mathcal{O}$ soit l'unique idéal de $\mathcal{O}$ au-dessus de $\mathcal{M}_w \cap \mathcal{O} \cap E$.

(2) Le corps résiduel de $L^{\mathrm{dec}}$ (pour $w|_{L^{\mathrm{dec}}}$) est $k_K$, et son groupe de valeurs est $\Gamma_K$. $L^{\mathrm{dec}}$ est donc une extension immédiate de $K$.

(3) L'application $\sigma \mapsto \bar{\sigma}$ envoie $G_{\mathrm{dec}}$ sur $Aut(k_L/k_K)$.

*Démonstration.* (1) La condition "$\mathcal{M}_w \cap \mathcal{O}$ est l'unique idéal de $\mathcal{O}$ au-dessus de $\mathcal{M}_w \cap \mathcal{O} \cap E$" est équivalente à "$w$ est l'unique extension à $L$ de $w|_E$". Par définition de $G_{\mathrm{dec}}$, on sait que $w$

est l'unique valuation de $L$ qui étend $w|_{L^{\rm dec}}$. D'autre part, si $E$ est strictement contenu dans $L^{\rm dec}$, alors $\mathcal{G}al(L/E)$ contient un élément $\sigma \notin H$, et $\sigma(\mathcal{M}_w) \cap \mathcal{O}$ est aussi au-dessus de $\mathcal{M}_w \cap E$.

(2) Soit $B = \mathcal{O} \cap L^{\rm dec}$, c'est-à-dire la clôture intégrale de $\mathcal{O}_v$ dans $L^{\rm dec}$. Nous voulons montrer que $B/\mathcal{M}_w \cap B \simeq k_v$. Soit $a \in B$. Si $\sigma \notin G_{\rm dec}$, alors $\sigma(\mathcal{M}_w) \cap B \neq \mathcal{M}_w \cap B$ : cela provient de la première assertion. Donc, par le théorème du reste chinois, il existe $b \in B$ tel que $b - a \in \mathcal{M}_w$, et si $\sigma \notin G_{\rm dec}$, alors $b - 1 \in \sigma(\mathcal{M}_w)$. Soient $b = b_1, \ldots, b_r$ les racines du polynôme minimal $f(X)$ de $b$ sur $K$. Comme $b \in B$ et $G_{\rm dec}$ fixe $b$, nous savons que si $i \geq 2$, alors $b_i = \tau(b)$ pour un $\tau \notin G_{\rm dec}$ ; de $b - 1 \in \tau^{-1}\mathcal{M}_w$ nous déduisons $b_i - 1 \in \mathcal{M}_w$. Comme $\prod_i b_i \in K$, et $\prod_i \operatorname{res} b_i = \operatorname{res} a$, nous avons le résultat.

Je ne donne pas la preuve du fait que $L^{\rm dec}$ et $K$ ont même groupe de valeurs, je la donnerai peut-être plus tard. Celle du livre de Ribenboim nécessite trop de définitions supplémentaires. Voir aussi Théorème 3.24 pour un résultat du même genre.

(3) Le fait que $\sigma \mapsto \bar{\sigma}$ soit un morphisme de groupe est clair. Pour montrer qu'il est surjectif, nous pouvons, par (2), remplacer $K$ par $L^{\rm dec}$, et donc supposer que $\mathcal{M}_w \cap \mathcal{O}$ est l'unique idéal de $\mathcal{O}$ au-dessus de $\mathcal{O}_v$.

Soit $a \in B$ tel que $\operatorname{res} a$ soit séparable sur $k_K$ et non nul, et soit $f(X)$ le polynôme minimal unitaire de $a$ sur $K$. Alors $f(X) = \prod(X - a_i)$, où $a_1 = a$, et $a_2, \ldots, a_r$ sont les conjugués de $a$ sur $K$. Puisque $w$ est l'unique valuation de $L$ étendant $v$, tous les $a_i$ ont valuation 0, et $f(X) \in \mathcal{O}_v[X]$. Le groupe $G$ agit transitivement sur les racines de $f(X) = 0$, donc $\bar{G} = \{\bar{\sigma} \mid \sigma \in G\}$ agit transitivement sur l'ensemble de leurs images par res . Cela montre $G$ se projette sur $\mathrm{Aut}(k_w \cap k^{sep}/k_v)$. Comme tout automorphisme de $k_w \cap k_v^{sep}$ se prolonge uniquement à un automorphisme de $k_w$, on obtient que l'application $G \to \mathcal{G}al(k_w/k_v)$ est bien surjective. De plus, on obtient que $\operatorname{res}(f)(X)$ est une puissance du polynôme minimal de $\operatorname{res}(a)$ sur $k_K$.

## 3.5 Plus sur les corps Henséliens

**3.11.** Revenons aux corps Henséliens. Nous allons montrer ci-dessous un théorème très important et très utile.

**Théorème**. Soit $(K, v)$ un corps valué. Les propriétés suivantes sont équivalentes :

(1) $(K, v)$ est Hensélien.

(2) Si $L$ est une extension algébrique de $K$, alors $v$ a une unique extension à $L$.

(3) Si $f(T) \in \mathcal{O}_v[T]$ est un polynôme unitaire, et $g(T), h(T) \in k_v[T]$ sont tels que $g(T)$ et $h(T)$ sont relativement premiers, $f(T)$ et $\operatorname{res}(f)(T) = g(T)h(T)$, alors il existe $p(T), q(T) \in \mathcal{O}_v(T)$ tels que $f(T) = p(T)q(T)$ et $\operatorname{res}(p)(T) = g(T)$, $\operatorname{res}(q)(T) = h(T)$.

**3.12. Remarque**. Notons tout de suite une conséquence de la propriété (2). Soit $K$ un corps valué satisfaisant (2), et $w$ l'unique extension de $v$ à $K^{alg}$. Soit $a \in K^{alg}$, $f(T) \in K[T]$ son polynôme minimal sur $K$, de degré $n$. Puisque $w$ est l'unique extension de $v$ à $K^{alg}$, si $f(b) = 0$

on aura $w(a) = w(b)$. Nous allons montrer que

$$w(a) = \frac{v(f(0))}{n}.$$

Si $f(T)$ est séparable, alors ses racines $a = a_1, \ldots, a_n$ sont toutes distinctes, et on a $f(T) = \prod_{i=1}^{n}(T - a_i)$. On remarque que le coefficient de $T^{n-1}$ est égal à $-(a_1 + \cdots + a_n)$ (nous nous servirons de cette remarque dans la preuve) et que le coefficient de 1, $f(0)$, est égal à $(-1)^n \prod_{i=1}^{n} a_i$. Donc $v(f(0)) = \sum_{i=1}^{n} w(a_i) = nw(a)$.

Supposons maintenant que $f(T)$ ne soit pas séparable, et écrivons le $f(T) = h(T^{p^m})$, où $m \in \mathbb{N}$, $m \geq 1$, et $h(T)$ est séparable. Le polynôme $h(T)$ est donc le polynôme minimal de $a^{p^m}$ sur $K$. Par le cas précédent, nous avons $p^m w(a) = w(a^{p^m}) = w(h(0))/\deg(h)$. Comme $p^m \deg(h) = n$ cela donne le résultat.

Notez aussi que l'on a :

$$f(T) = \prod_{i=1}^{\deg(h)} (T - a_i)^{p^m}$$

si $\{a_1, \ldots, a_{\deg(h)}\}$ est l'ensemble des racines de $f(T)$. Chaque racine est de multiplicité $p^m$.

**3.13.** *Démonstration du Théorème 3.11.* (2) $\Rightarrow$ (1). Soient $f(T) \in \mathcal{O}_v[T]$ et $a \in \mathcal{O}_v$ tels que $v(f(a)) > 0$ et $v(f'(a)) = 0$. On peut supposer que $f(T)$ est irréductible sur $K$, disons de degré $n$. Nous allons montrer que $n = 1$, ce qui montrera que $f(T)$ a une racine dans $K$.

Soient $b_1, \ldots, b_n$ les racines de $f(T)$. Alors $f(T) = c\prod_{i=1}^{n}(T - b_i)$, pour un $c \in K$. Si $w$ est l'unique extension de $v$ à $K^{alg}$, on a alors $w(b_i) = w(b_j) := \gamma$ pour tout $i, j$.

Supposons d'abord que $v(c) = 0$. Multipliant par $c^{-1}$, on peut supposer que $c = 1$. Alors $\mathrm{res}\,(f)(T) = \prod_i (T - \mathrm{res}\,(b_i))$. Comme $f$ est irréductible et $w$ est l'unique extension de $v$ à $K^{alg}$, nous savons que $\mathrm{res}\,(f)(T)$ est une puissance du polynôme minimal sur $k_K$ d'une de ses racines, voir la fin de la démonstration de la Proposition 3.10 ; mais par hypothèse $\mathrm{res}\,(f(a)) = 0 \neq \mathrm{res}\,(f'(a))$, et $a \in K$, ce qui implique que $n = 1$, et prouve le résultat.

Regardons maintenant le cas général, et écrivons $f(T) = c(\sum_{i=0}^{n} a_i T^{n-i})$. Alors chaque $a_i$, étant (au signe près) une somme de produits de $i$ éléments parmi les $b_j$, est de valuation $\geq i\gamma$, avec égalité pour $i = 0, n$, car $a_0 = 1$ et $a_n = \prod_i b_j$.

Si $\gamma < 0$, puisque $f(T) \in \mathcal{O}_v[T]$ est d'image résiduelle non triviale, nous obtenons alors $0 \leq v(ca_n) < v(ca_i)$ pour $i < n$, d'où $\mathrm{res}\,(f)(T) = \mathrm{res}\,(ca_n)$ est constante, une contradiction. Si $\gamma > 0$, nous obtenons $\mathrm{res}\,(f)(T) = \mathrm{res}\,(c)T^n$, d'où $n = 1$, et $b_1 \in K$. Il ne reste donc que le cas où $\gamma = 0$, qui entraîne $v(c) = 0$ (car $\mathrm{res}\,(f)(T) \neq 0$), et nous ramène au cas traité précédemment.

(1) $\Rightarrow$ (2). Soit $L$ une extension normale finie de $K$ ayant plusieurs valuations étendant $v$. Nous pouvons supposer que $L$ est séparable sur $K$ (car toute valuation sur la clôture séparable $K^{sep}$ de $K$ s'étend uniquement à une valuation de $K^{alg}$), et donc Galois. Choisissons une valuation $w$ de $L$ étendant $v$, soit $G_{\mathrm{dec}}$ son groupe de décomposition, et $\mathcal{O}$ la clôture intégrale de $\mathcal{O}_v$ dans $L^{\mathrm{dec}}$. En raisonnant comme dans la preuve de 3.10(2), il existe $a \in \mathcal{O}$ tel que $a \notin \mathcal{M}_w$, et $a \in \sigma\mathcal{M}_w$ si $\sigma \notin G_{\mathrm{dec}}$. Regardons maintenant le polynôme minimal $f(T)$ de $a$

sur $K$, et écrivons-le $f(T) = \prod_{i=1}^{n}(T - a_i)$, où $a_1 = a$, et $a_2, \ldots, a_n$ sont les autres racines de $f(T)$ (elles sont toutes distinctes, car le polynôme $f(T)$ est séparable). Comme $a \in L^{\text{dec}}$, nous savons que les racines de $f(T)$ autres que $a$ sont de la forme $\sigma(a)$ pour des $\sigma \notin G_{\text{dec}}$. Donc $a$ est la seule racine de $f(T)$ de valuation 0, toutes les autres sont de valuation $> 0$ : si $\sigma \notin H$ alors $\sigma^{-1}(a) \in \mathcal{M}_w$. Si $f(T) = \sum b_i T^i$, avec $b_n = 1$, nous avons alors $b_{n-1} = -\sum_{i=1}^{n} a_i$, et donc $w(b_{n-1} + a) > 0$, et $w(b_i) > 0$ pour $i < n - 1$ (puisque si $i \geq 2$, alors $b_i$ est $\pm$ une somme de produits de $i$ éléments parmi les $a_j$). Donc $\operatorname{res}(f)(T) = T^{n-1}(T - \operatorname{res} a)$. Mais $\operatorname{res} a$ est une racine simple de ce polynôme, et puisque $K$ est Hensélien, $a \in K$, ce qui nous donne la contradiction désirée.

(3) $\Rightarrow$ (2) : Soit $f(T) \in \mathcal{O}_v[T]$ un polynôme unitaire, et $a \in \mathcal{O}_v$ tel que $\operatorname{res} a$ soit une racine simple de $\operatorname{res}(f)(T)$. Alors $\operatorname{res}(f)(T)$ s'écrit $(T - \operatorname{res} a)g(T)$ pour un polynôme $g(T) \in k_v[T]$ tel que $g(\operatorname{res} a) \neq 0$. Par (3), il existe $b \in \mathcal{O}_v$ et $q(T) \in \mathcal{O}_v[T]$ tels que $f(T) = (T - b)q(T)$ et $\operatorname{res} b = \operatorname{res} a$. Alors $f(b) = 0$, et $\operatorname{res} b = \operatorname{res} a$. Par la remarque ci-dessus, $K$ est Hensélien.

Pour (2) $\Rightarrow$ (3), soit $L$ l'extension normale de $K$ engendrée par les racines de $f(T)$, et écrivons $f(T) = \prod_{i=1}^{n}(T - a_i)$. Comme $f$ est unitaire, tous les $a_i$ sont entiers sur $\mathcal{O}_v$, et donc dans $\mathcal{O}_w$. En renumérotant les $a_i$, nous pouvons supposer que pour $i < r$, $\operatorname{res}(a_i)$ est une racine de $g(T)$, pour $i \geq r$, $\operatorname{res}(a_i)$ est une racine de $h(T)$. On peut aussi supposer que $g$ et $h$ sont unitaires (parce que $f(T)$ est unitaire). On sait que pour tout $i$, le polynôme minimal $f_i(T)$ de $a_i$ sur $K$ divise $f(T)$. Puisque l'extension de la valuation à $K(a_1, \ldots, a_n)$ est unique, cela entraîne que si $a_j$ est aussi une racine de $f_i(T)$, alors $\operatorname{res}(a_j)$ et $\operatorname{res}(a_i)$ seront conjugués au-dessus de $k_v$. En particulier on aura $i < r \leftrightarrow j < r$. En regardant la décomposition de $f(T)$ en facteurs premiers, on en déduit que $f(T)$ s'écrit $p(T)q(T)$, où $p(T)$ est un produit de puissances de $f_i(T)$, pour $i < r$, et $q(T)$ est un produit de puissances des $f_i(T)$, $r \leq i \leq n$. Il est alors clair que $\operatorname{res}(p)(T) = g(T)$, $\operatorname{res}(q)(T) = h(T)$.

**Remarque**. Une inspection de la preuve de (1) $\Rightarrow$ (2) montre que en fait nous avons montré : si pour tout polynôme unitaire $f(T) \in \mathcal{O}_v[T]$ et $a \in \mathcal{O}_v$ tel que $\operatorname{res} a$ soit une racine simple de $\operatorname{res}(f)(T)$, il existe $b$ tel que $f(b) = 0$ et $\operatorname{res} b = \operatorname{res} a$, alors le corps valué satisfait (2). L'équivalence de (1) et (2) entraîne donc que dans la définition de corps Hensélien, on peut se restreindre à des polynômes $f(T)$ qui sont unitaires.

**3.14. Corollaires et définitions**. Soit $(K, v)$ un corps valué, et $\mathcal{O}$ sa clôture intégrale dans $K^{sep}$. Fixons une extension $w$ de $v$ à $K^{sep}$, d'idéal maximal $\mathcal{M}_w$.

(1) Une extension algébrique d'un corps Hensélien est Hensélienne.

(2) Il existe un plus petit corps Hensélien contenant $K$ : c'est le sous-corps de $K^{sep}$ fixé par le groupe de décomposition $G_{\text{dec}} = \{\sigma \in \mathcal{G}al(K^{sep}/K) \mid \sigma(\mathcal{M}_w \cap \mathcal{O}) = \mathcal{M}_w \cap \mathcal{O}\}$. Ce corps sera appelé la *Hensélianisée de* $K$ (ou *le Hensélianisé*, ou *la Hensélianisation*). Il est unique à $K$-isomorphisme près et je le noterai $K^h$.

(3) $K^h$ est une extension immédiate de $K$.

*Démonstration.* (1) est clair.

Pour (2), soit $w$ une extension de $v$ à $K^{sep}$ (la clôture séparable de $K$), et soit $K^h$ le corps de décomposition de $w$. Nous savons que $K^{sep}$ est la réunion de toutes les extensions de Galois finies de $K$.

Montrons d'abord que $w|_{K^h}$ a une seule extension à $K^{sep}$. Pour cela il suffit de montrer que si $L$ est une extension de Galois finie de $K$, alors $w|_{K^h\cap L}$ a une seule extension à $L$ : c'est exactement ce que dit 3.10, puisque l'image de $G_w$ dans $\mathcal{G}al(L/K)$ est précisément le groupe de décomposition de $w|_L$ sur $K$, c'est-à-dire que $L\cap K^h = L^{\rm dec}$ (en utilisant la notation de 3.9). De même, si $E$ est un sous-corps de $M$ contenant $K$ et différent de $K^h$, alors il existe une extension de Galois finie $L$ de $K$ telle que $E\cap L \neq K^h\cap L = L^{\rm dec}$, et de nouveau nous pouvons appliquer 3.10. Par 3.11 nous obtenons donc que $K^h$ est Hensélien, et que tout sous-corps propre de $K^h$ contenant $K$ ne l'est pas.

(3) provient de 3.10, puisque pour toute extension finie $L$ de $K$, nous avons que $K^h\cap L = L^{\rm dec}$ est une extension immédiate de $K$. Nous utilisons aussi 3.6.

**3.15. Exercice**. Soit $(K, v)$ un corps valué. Vérifiez que les conditions suivantes sont équivalentes:

(1) $K$ est Hensélien.

(2) Soit $f(T) \in \mathcal{O}_v[T]$ tel que $v(f(0)) > 2v(f'(0))$. Alors il existe $b \in \mathcal{O}_v$ tel que $v(b) = v(f(0)) - v(f'(0))$ et $f(b) = 0$.

L' implication (2) $\Rightarrow$ (1) est facile. Pour (1) $\Rightarrow$ (2), on pose $c = -f(0)/f'(0)$, et on considère le polynôme $g(T) = f(cT)/f(0)$ ; on montre que $g(T) \in \mathcal{O}_v[T]$, que $g(1) \in \mathcal{M}_v$ et $g'(1) + 1 \in \mathcal{M}_v$.

## 3.6 Sous-groupes convexes et valuations qui leur sont associées

**3.16. Etude des sous-groupes convexes d'un groupe ordonné abélien**. Soit $\Gamma$ un groupe abélien ordonné. Rappelons qu'un sous-ensemble $I$ de $\Gamma$ est *convexe*, si pour tout $a < b < c \in \Gamma$, si $a$ et $c$ sont dans $I$, alors $b$ aussi. Si $\Delta$ est un sous-groupe convexe de $\Gamma$, alors l'ordre de $\Gamma$ induit un ordre sur le groupe quotient $\Gamma/\Delta$, en posant $a+\Delta < b+\Delta \iff a < b$ et $a - b \notin \Delta$. L'*enveloppe convexe* d'un sous-groupe $H$ de $\Gamma$ sera donc l'ensemble $\{a \in \Gamma \mid \exists b \in H,\ -b < a < b\}$. On vérifie facilement que c'est un sous-groupe.

A $c \in \Gamma^{>0}$ on peut associer deux sous-groupes convexes de la façon suivante (par $|x|$ je note la "valeur absolue" de $x$, c'est-à-dire, $\sup\{x, -x\}$) :

$$H(c) = \{a \in \Gamma \mid \exists n \in \mathbb{N}\ |b| < nc\}, \quad H^-(c) = \{a \in \Gamma \mid \forall n \in \mathbb{N}\ n|b| < c\}.$$

Alors $H(c)$ est l'enveloppe convexe du sous-groupe engendré par $c$, et $H^-(c)$ est le plus gros sous-groupe convexe de $\Gamma$ ne contenant pas $c$. Alors $H(c)/H^-(c)$ est un groupe archimédien : la suite $nc$, $n \in \mathbb{N}$, est cofinale dans $H(c)$, et tout élément positif de $H(c)$ qui n'est pas dans $H^-(c)$ est plus grand que $c/n$ pour un $n \in \mathbb{N}$.

Les sous-groupes convexes de $\Gamma$ forment une suite, totalement ordonnée par l'inclusion (et qui en général n'est pas bien ordonnée).

**3.17. Exemples**. Soient $\Gamma_1$ et $\Gamma_2$ deux groupes ordonnés. L'*ordre lexicographique* sur $\Gamma_1 \times \Gamma_2$ est défini par :

$$(a_1, a_2) < (b_1, b_2) \iff (a_1 < a_2) \vee (a_1 = a_2 \wedge b_1 = b_2).$$

Les éléments de $\Gamma_2$ sont donc moins importants que ceux de $\Gamma_1$. On vérifie sans peine que $0 \times \Gamma_2$ est un sous-groupe connexe de $\Gamma_1 \times \Gamma_2$.

Plus généralement, soit $I$ un ensemble totalement ordonné, et pour chaque $i \in I$, soit $\Gamma_i$ un groupe ordonné. Si $(a_i) \in \prod_{i\in I} \Gamma_i$, on définit $Supp((a_i)_i) = \{i \in I \mid a_i \neq 0\}$. On considère l'ensemble $\Gamma$ des éléments de $\prod_{i\in I} \Gamma_i$ dont le support est bien ordonné. On définit un ordre sur $\Gamma$ en posant

$$(a_i)_i < (b_i)_i \iff \text{ si } j = \inf Supp((a_i - b_i)_i), \text{ alors } a_j < b_j.$$

Là par contre, on voit que si $I$ n'est pas bien ordonné, l'ensemble des sous-groupes convexes de $\Gamma$ contiendra une sous-suite de type d'ordre celui de $I$.

**3.18. Connections avec les valuations**. Soit $(K, v)$ un corps valué, de groupe de valeurs $\Gamma$, d'anneau de valuation $\mathcal{O}_v$ et d'idéal maximal $\mathcal{M}_v$. Nous savons déja que les idéaux de $I$ correspondent aux segments finaux de $\Gamma^{>0}$, par l'application $I \mapsto C(I) = v(I \setminus 0)$. On vérifie facilement que si $P$ est un idéal premier de $\mathcal{O}$, alors $\Delta^+(P) = \Gamma^{>0} \setminus C(P)$ est clos par addition. Cela entraîne que le sous-groupe $\Delta(P)$ de $\Gamma$ engendré par $\Delta^+(P)$, qui égale $-\Delta^+(P) \cup \{0\} \cup \Delta^+(P)$, est un sous-groupe convexe de $\Gamma$. Réciproquement, si $\Delta$ est un sous-groupe convexe de $\Gamma$, alors $P = \{a \in \mathcal{O}_v \mid |a| > \Delta\}$ est un idéal premier de $\mathcal{O}_v$.

Nous avons donc une correspondance entre les idéaux premiers de $\mathcal{O}_v$ et les sous-groupes convexes de $\Gamma$. Nous avons $\Delta((0)) = \Gamma$, $\Delta(\mathcal{M}_v) = (0)$.

**3.19. Comment définir de nouvelles valuations sur $K$.** Notations comme ci-dessus.

Soit $\Delta$ un sous-groupe convexe de $\Gamma$, que nous supposerons propre (c'est-à-dire, $\neq 0, \Gamma$), et soit $\pi : \Gamma \to \Gamma/\Delta = \Lambda$ l'application naturelle.

Alors $\pi \circ v$ définit une application $v_\Lambda : K^\times \to \Lambda$, qui est une valuation si on définit $v_\Lambda(0) = \infty$. L'anneau de valuation de $v_\Lambda$ est alors $\mathcal{O}_{v_\Lambda} = \{a \in K \mid \exists \delta \in \Delta,\ \delta < v(a)\}$, et son idéal maximal est $\mathcal{M}_{v_\Lambda} = \{a \in K \mid v(a) > \Delta\}$ (qui est l'idéal premier correspondant à $\Delta$). L'anneau $\mathcal{O}_{v_\Lambda}$ est donc obtenu à partir de $\mathcal{O}_v$ en ajoutant les inverses des éléments ayant valuation dans $\Delta$. On a donc $\mathcal{O}_v \subset \mathcal{O}_{v_\Lambda}$ et $\mathcal{M}_{v_\Lambda} \subset \mathcal{M}_v$.

Le corps résiduel $k_{v_\Lambda}$ peut lui aussi être muni d'une valuation $v_\Delta$ avec groupe de valeurs $\Delta$ : si $a \in \mathcal{O}_{v_\Lambda}^\times$, alors $v(a) \in \Delta$, et si $b$ est tel que $(a - b) \in \mathcal{M}_{v_\Lambda}$, alors $v(a) = v(b)$.

Nous avons donc, à partir de $\Gamma$ et de $\Delta$, fabriqué deux valuations : l'une, $v_\Lambda$, qui est plus grossière que $v$, et l'autre, $v_\Delta$, qui est définie sur le corps résiduel de $v_\Lambda$.

**3.20.** Réciproquement, supposons que nous ayions une valuation $v_\Delta$ sur le corps résiduel $k_w$ de $(K, w)$, de groupe de valeurs $\Delta$. Nous pouvons alors définir une nouvelle valuation, plus fine, de $K$, de la façon suivante :

Posons

$$\begin{aligned} \mathcal{O} &= \{a \in \mathcal{O}_w \mid v_\Delta(\mathrm{res}_w(a)) \geq 0\}, \\ \mathcal{M} &= \{a \in \mathcal{O}_w \mid v_\Delta(\mathrm{res}_w(a)) > 0\}. \end{aligned}$$

On vérifie que $\mathcal{O}$ est un anneau de valuation (c'est-à-dire, si $a \in K \setminus \mathcal{O}$ alors $a^{-1} \in \mathcal{O}$), d'idéal maximal $\mathcal{M}$, et nous appellerons $v$ la valuation associée. Son groupe de valeurs sera isomorphe à $\Gamma \times \Delta$ (muni de l'ordre lexicographique) **en tant qu'ensemble ordonné**, mais pas nécessairement en tant que groupe. Pour chaque $\gamma \in \Gamma$, on choisis $s(\gamma) \in K^\times$ satisfaisant $v(s(\gamma)) = \gamma$ ; par définition de $v$, étant donnés $a, b \in K^\times$, on a $v(a) > v(b)$ si et seulement si $w(a) > w(b)$, ou $w(a) = w(b)$ et $v_\Delta(a) > v_\Delta(b)$. L'application $\varphi : K^\times \to \Gamma \times \Delta$ qui a $a$ associe $(w(a), v_\Delta(\mathrm{res}\,(as(-w(a)))))$ satisfait alors : $\varphi(a) < \varphi(b) \iff v(a) < v(b)$, ce qui montre notre assertion. Notons cependant que en général $\varphi$ n'est pas une valuation, car elle ne satisfait pas $\varphi(ab) = \varphi(a) + \varphi(b)$. Elle ne sera une valuation que si on arrive à choisir $s$ de sorte que $s$ satisfasse $s(\alpha + \beta) = s(\alpha)s(\beta)$, ce qui n'est pas toujours possible.

**3.21. Remarques**. Plusieurs propriétés peuvent être montrées par induction, et en se servant des valuations subordonnées. Soit $(K, v)$ un corps valué, de groupe valeurs $\Gamma$, soit $\Delta$ un sous-groupe convexe de $\Gamma$, et $v_\Delta$, $v_\Lambda$ les deux valuations associées. Alors

(1) $(K, v)$ est Hensélien si et seulement si $(K, v_\Lambda)$ et $(k_{v_\Lambda}, v_\Delta)$ sont Henséliens.

(2) Soit $L$ une extension algébrique de $K$, $w$ une extension de $v$ à $L$, et supposons qu'elle soit non ramifiée (c'est-à-dire, $v(K^\times) = w(L^\times)$). Alors à $w$ sont associées les deux valuations $w_\Lambda$ sur $L$ et $w_\Delta$ sur $k_{w_\Lambda}$ (qui est une extension algébrique de $k_{v_\Lambda}$), et on a : $[k_w : k_v] = [k_{w_\Lambda} : k_{v_\Lambda}][k_{w_\Delta} : k_{v_\Delta}]$.

(3) Soient $L$ une extension algébrique de $K$, et $w$ une extension de $v$ à $L$. Si $L$ est une extension immédiate de $K$ pour la valuation $w$, alors elle est aussi une extension immédiate de $K$ pour la valuation $w_\Lambda$, et son corps résiduel $k_{w_\Lambda}$ est une extension immédiate de $k_{v_\Lambda}$ pour la valuation $v_\Delta$.

(4) Supposons que $K$ soit de caractéristique 0, et supposons que $v(p) > 0$. Soit $\Delta$ l'enveloppe convexe du sous-groupe de $\Gamma$ engendré par $v(p)$. Alors $k_{v_\Lambda}$ est de caractéristique 0.

**3.22. Exercice** Montrez que l'anneau $\mathcal{O}$ défini en 3.20 est bien un anneau de valuation, et que $\mathcal{M}$ est son idéal maximal.

**3.23. Exercice** Montrez l'assertion (1) de la Remarque 3.21.

## 3.7 Plus sur les extensions de corps valués

**3.24.** Les deux résultats suivants sont classiques, importants, et la preuve du deuxième est longue. Je les cite sans démonstration.

**Théorème**. Soient $(K, v)$ un corps valué, $L$ une extension séparable de $K$ de degré $n$, et $w_1, \ldots, w_g$ les extension de $v$ à $L$. Alors

$$n \geq \sum_{i=1}^{g} e(L/K, w_i) f(L/K, w_i).$$

*Esquisse de preuve.* Ecrivons $L = K(a)$, et choisissons une Hensélisation $M$ de $K$ (nous savons qu'elles sont uniques à $K$-isomorphisme près, et que $M$ est une extension immédiate de $K$). Soit $f(T)$ le polynôme minimal de $a$ sur $K$, et soit $f(T) = f_1(T) \cdots f_r(T)$ sa décomposition en facteurs irréductibles sur $M[T]$. On considère maintenant $(K^{alg}, w^*)$, où $w^*$ est l'unique valuation de $K^{alg}$ étendant $w$. Pour chaque $K$-plongement $\varphi$ du corps $L$ dans le corps $K^{alg}$, on obtient une valuation $v_\varphi$ qui prolonge $v$ (tout simplement $w^* \circ \varphi$). Alors on montre : $v_\varphi$ et $v_\psi$ sont équivalentes si et seulement si $\varphi(a)$ et $\psi(a)$ sont racines du même polynôme $f_i(T)$. Si $v$ a $g$ extensions distinctes à $L$, on aura donc $g \leq r$. Par 3.7, si $\varphi(a)$ satisfait $f_i(T) = 0$, alors $e(\varphi(L)M/M, w^*) f(\varphi(L)M/M, w^*) \leq \deg(f_i)$. [Ici, $\varphi(L)M$ dénote le sous-corps de $K^{alg}$ engendré par $\varphi(L)$ et par $M$.] Comme $M$ est une extension immédiate de $K$, $e(\varphi(L)M/M, w^*) = e(L/K, v_\varphi)$ et $f(\varphi(L)M/M, w^*) = f(L/K, v_\varphi)$, ce qui montre le résultat.

Pour plus de détails, voir par exemple le livre de Ribenboim, chapitre G, Corollaire 1.

**3.25. Théorème** (Ostrowski). Soit $(K, v)$ un corps valué Hensélien, et $L$ une extension algébrique de degré $n$, et $w$ l'unique extension de $v$ à $L$. Alors

$$n = e(L/K) f(L/K) \chi^d,$$

pour un entier $d \geq 0$, où $\chi$ dénote la caractéristique de $k_v$ si elle est positive, et 1 sinon.

**Commentaires**. L'entier $d$ est appelé le *défaut* de l'extension.

En fait, si $L$ est Galois sur $K$ et la valuation est archimédienne, on peut combiner les deux résultats pour obtenir que $[L : K] = gef\chi^d$, où $e = e(L/K)$, $f = f(L/K)$ et $g = [L^{\text{dec}} : K]$ est le nombre d'extensions de $v$ à $L$.

La preuve de ce résultat utilise les suites pseudo-convergentes et leurs propriétés. Elles ont été introduites par Ostrowski, sont très utiles. Une très bonne exposition en est faite dans l'article de I. Kaplansky, Maximal fields with valuations, Duke Journal, vol 9 (1942), 303 – 321. C'est un article concis, on apprend beaucoup en le lisant. Je les ferai probablement à un moment ou à un autre, mais pas maintenant, nous avons fait assez de résultats techniques pour le moment.

**3.26. Théorème**. Soit $(K, v)$ un corps valué Hensélien, de caractéristique résiduelle nulle. Alors $K$ n'a pas d'extension algébrique immédiate (propre).

*Démonstration.* Le théorème d'Ostrowski nous donne que si $L$ est une extension algébrique immédiate de $K$, alors son degré est 1 (car $\chi = 1$).

**3.27. Théorème**. Soit $(K, v)$ un corps valué Hensélien de caractéristique nulle, de caractéristique résiduelle $p > 0$, et supposons que $\Gamma_v$ a un plus petit élément 1, et que $v(p) = e1$ ($e1$ sera noté $e$) pour un entier $e > 0$. Alors $K$ n'a pas d'extension algébrique immédiate (propre).

*Démonstration.* On suppose d'abord que $\Gamma_v$ est archimédien. Comme $\Gamma_v$ a un plus petit élément positif, cela entraîne que $\Gamma_v$ est isomorphe à $\mathbb{Z}$. Soit $a \in K^{alg}$, et supposons que $L = K(a)$ est une extension immédiate de $K$. Comme dans le sous-cas 2c de Théorème 2.14, nous pouvons trouver une suite infinie $a_n \in K$, telle que $v(a-a_{n+1}) > v(a-a_n)$ pour tout $n$. Comme $\Gamma_K \simeq \mathbb{Z}$, la suite $v(a - a_n)$ est donc cofinale dans $\Gamma_K$. Soit $f(T) \in K[T]$ le polynôme minimal de $a$ sur $K$. Comme $f(a) = 0$, et $f(a_n) = \sum_{i\geq 1} D_i(f)(a)(a_n - a)^i$, nous obtenons que $v(f(a_n))$ est aussi cofinale dans $\Gamma_K$. En effet, les $D_i(f)(a)$ ont valuation fixée. D'un autre côté, comme $K$ est de caractéristique nulle, nous savons que $f'(a) \neq 0$. En raisonnant de la même façon, nous obtenons que pour un $n$ suffisamment grand, nous avons $v(f'(a_n)) = v(f'(a)) < 2v(f(a_n))$. Nous appliquons alors les résultats de l'exercice 3.15 pour conclure.

*Esquisse de preuve dans le cas général.* Soit $\Delta$ l'enveloppe convexe du sous-groupe de $\Gamma$ engendré par $v(p)$. Notre hypothèse entraîne que $\Delta$ est archimédien. Alors, avec les notations de 3.19, $k_{v_\Lambda}$ est de caractéristique 0, et les deux corps valués $(K, v_\Lambda)$ et $(k_{v_\Lambda}, v_\Delta)$ sont Henséliens. Par 3.26 et par le cas archimédien, ils n'ont aucune extension algébrique immédiate propre. Nous obtenons le résultat par la Remarque 3.19.

**3.28. Lemme**. Soient $(E, v) \subset (F, w)$ des corps valués de caractéristique 0, ayant même corps résiduel, et avec $F$ Hensélien. Si la caractéristique du corps résiduel de $E$ est $p > 0$, nous supposerons que $\Gamma_E$ a un plus petit élément, noté 1, et que c'est aussi le plus petit élément de $\Gamma_F$. Nous supposerons aussi dans ce cas qu'il existe $e \in \mathbb{N}$ tel que $v(p) = e$.

(1) Si $u \in F$ est tel que $w(u) > 2w(n)$, alors $1 + u$ a une racine $n$-ième $b \in F$ telle que $w(b - 1) = w(u) - w(n)$.

(2) Soit $\gamma \in \Gamma_F$, et supposons que $n\gamma \in \Gamma_E$ pour un $n \in \mathbb{N}^{>0}$, avec $n$ minimal pour cette propriété. Alors il existe $b \in F$ tel que $b^n \in E$ et $w(b) = \gamma$.

*Démonstration.* (1) Nous considérons le polynôme $f(T) = T^n - (1 + u)$. Alors $w(f(1)) = w(u) > 2w(n) = w(f'(1))$. Par l'exercice 3.15, il existe $b \in F$ tel que $b^n = 1 + u$, et $w(b - 1) = w(u) - w(n)$.

(2) Soient $a \in F$ et $c \in E$ tels que $w(a) = \gamma$ et $v(c) = n\gamma$. Puisque $k_E = k_F$, nous pouvons choisir ce $c$ tel que $\mathrm{res}\,(a^n c^{-1}) = 1$, et donc $a^n = c(1 + u)$, où $w(u) > 0$. Si la caractéristique de $k_E$ est nulle ou ne divise pas $n$, nous pouvons appliquer (1), puisque $w(n) = 0$, et trouver $d$ tel que $d^n = (1 + u)$, ce qui entraîne que $c$ a une racine $n$-ième dans $F$.

Supposons maintenant que la caractéristique résiduelle soit $p > 0$ et divise $n$, soit $\pi \in E$ tel que $v(\pi)$ est le plus petit élément de $\Gamma_E$ (et donc aussi de $\Gamma_F$). Alors, puisque $k_E = k_F$, pour tout $s \in \mathbb{N}$, nous pouvons trouver des éléments $u_1, \ldots, u_s \in E$ tels que $w(u - \sum_{i=1}^s u_i\pi^i) > sw(\pi)$. Choisissons un tel $s$ qui soit $> 2w(n)$. Nous obtenons alors $a^n = c(1 + \sum_{i=1}^s u_i\pi^i)(1 + u')$, avec $w(u') > s$. Par (1), $(1 + u')$ a une racine $n$-ième $d$ dans $F$, et donc $c(1 + \sum_{i=1}^s u_i\pi^i)$ aussi.

**3.29. Remarques**. (1) Quand le plus petit élément de $\Gamma_E$ n'est pas le plus petit élément de $\Gamma_F$, c'est un peu plus compliqué, et on n'obtient pas nécéssairement que l'extension est radicielle. Supposons par exemple que $F = E(\pi)$, avec $nw(\pi)$ le plus petit élément de $\Gamma_E$, et soit $e$ tel que $w(p) = ew(\pi)$. Alors on montre qu'il existe un polynôme $g(T) \in \mathcal{O}_E[T]$ de degré $< e$, tel que $w(g(0)) = 0$, et tel que $w(\pi^e - pg(\pi)) > 2w(e\pi^{e-1} - pg'(\pi))$. Puisque $F$ est Hensélien, il existera un élément $\alpha$ avec $\alpha^e = pg(\alpha)$ ; nécessairement on aura $w(\alpha) \geq w(p)/e$, et les conditions sur $g(T)$ entrainent que $w(\alpha) = w(p)/e$ et donc $F = E(\alpha)$ puisque $nv(p) = e$. On peut trouver la démonstration dans le livre d'A. Prestel et P. Roquette, *Formally p-adic fields*, Lemme 3.5.

(2) L'hypothèse $\Gamma_F = \langle \Gamma_E, w(a) \rangle$ est vérifiée si $n$ est un nombre premier. Dans le cas général, elle n'est pas toujours vérifiée, car il se peut très bien que $\Gamma_F/\Gamma_E$ ne soit pas cyclique. Dans ce cas nous obtiendrons que $F = E(a_1, \ldots, a_r)$, où pour chaque $i$, une puissance de $a_i$ est dans $E$.

**3.30. Lemme**. Soit $(E, v)$ un corps valué contenu dans un corps valué $(E(a), v)$, et tel que $E(a)$ soit une extension immédiate de $E$.

(1) L'ensemble $I = \{v(a-b) \mid b \in E\}$ n'a pas de plus grand élément, et est un segment initial de $\Gamma_v$.

(2) S'il existe un polynôme (non nul) $p(T) \in E[T]$ et $b \in E$ tel que pour tout $c, d \in E$, $v(d-b) > v(c-b)$ implique $v(p(d)) > v(p(c))$, alors il existe un élément $\alpha$ algébrique sur $E$, tel que $v(\alpha - c) > v(a - c)$ pour tout $c \in E$, et $E(\alpha)$ est une extension immédiate de $E$. Le type d'isomorphisme du corps valué $E(\alpha)$ est complètement déterminé par le polynôme minimal de $\alpha$ sur $E$ et la fonction $E \to \Gamma_E$, $b \mapsto v(\alpha - b)$.

(3) Si le cas (2) n'est pas vrai, alors $a$ est transcendant sur $E$. De plus, si $(F, w)$ est un autre corps valué contenant $E$ et contenant un élément $a'$ tel que pour tout $b \in A$, $v(a-b) = w(a'-b)$, alors l'isomorphisme $E(a) \to E(a')$ qui fixe $E$ et envoie $a$ sur $a'$ est un isomorphisme de corps valués. En particulier, $E(a')$ est une extension immédiate de $E$.

*Démonstration.* (1) est prouvé de la même façon que le cas 2c du théorème 2.14. Notons qu'il n'existe pas d'élément $c \in E$ satisfaisant $v(c-b) = v(a-b)$ pour tout $b \in E$ : si $b \in E$ est tel que $v(a-b) > v(a-c)$ alors $v(c-b) = v(a-c) < v(a-b)$.

(2) Soit $p(T)$ un polynôme non nul et de degré minimal en $T$ satisfaisant notre hypothèse. Alors $p(T)$ est irréductible, et nous pouvons supposer qu'il est unitaire. Notre hypothèse dit la chose suivante : si $\gamma = v(a-b)$, alors sur la boule ouverte $B(a;\gamma) \cap E$, la fonction $v(p(x))$ croît avec $v(x-a)$ et son image n'a pas de plus grand élément. Nous allons en fait nous intéresser seulement aux éléments de $B(a;\gamma) \cap E$, ceux qui donnent une (assez) bonne approximation de $a$.

Nous allons montrer, par induction sur le degré d'un polynôme $q(T) \in E[T]$ de degré $\leq \deg(p)$, qu'il existe $\delta_0 \in I$ tel que la fonction $v(q(x) - q(a))$ croît avec $v(x-a)$ sur la boule $B(a;\delta_0) \cap E$, et que son image n'a pas de plus grand élément. Si le degré de $q(T)$ est inférieur à celui de $p(T)$ alors il existera aussi $\delta_1 \in I$ tel que pour tout $c \in B(a;\delta_1) \cap E$, $v(q(c)) = v(q(a))$.

Si le degré de $q(T)$ est 1, alors c'est tout simplement l'hypothèse sur $I$ : $q(T)$ s'écrit $T-c$, et si $d \in B(a; v(a-c))$ alors $v(q(a)-q(d)) = v(a-d) > v(a-c)$. Supposons le résultat montré pour les polynômes de degré inférieur à celui de $q(T)$, nous allons le montrer pour $q(T)$. Ecrivons

$$q(c) - q(a) = \sum_{i=1}^{\deg(q)} D_i(q)(a)(c-a)^i.$$

Comme les valuations des $D_i(q)(a)$ sont fixes, et que $I$ n'a pas de plus grand élément, il existe $j$, $1 \leq j \leq \deg(q)$, et $\delta_0 \in I$ tel que si $\delta > \delta_0$ et $1 \leq i \leq \deg(q)$, $i \neq j$, alors

$$v(D_i(q)(a)) + i\delta > v(D_j(q)(a)) + j\delta.$$

Nous avons donc, pour tout $d \in B(a;\delta_0) \cap E$,

$$v(q(d) - q(a)) = v(D_j(q)(a)) + jv(d-a). \tag{1}$$

Cela entraîne bien que $\{v(q(x)-q(a)) \mid x \in B(a;\delta_0) \cap E\}$ n'a pas de plus grand élément. Deux cas sont alors possibles :

**Cas 1**. Il existe $\delta_1 \in I$ tel que $v(q(a)) < v(D_j(q)(a)) + j\delta_1$.

Alors nous aurons, en remplaçant $\delta_1$ par $\delta_0$ si $\delta_0 > \delta_1$, et en utilisant l'équation (1) :

$$\text{Pour tout } d \in B(a;\delta_1)\ v(q(d)) = v(q(a)).$$

**Cas 2**. Il n'existe pas de tel $\delta_1$.

L'équation (1) entraîne alors que l'ensemble $\{v(q(d)) \mid d \in B(a;\delta_0) \cap E\}$ n'a pas de plus grand élément. En effet, l'equation (1) nous donne que $v(q(d)) = v(D_j(q)(a)) + jv(d-a)$. On s'aperçoit alors que $q(T)$ satisfait exactement les hypothèses satisfaites par $p(T)$, et donc doit avoir même degré que $p(T)$. Ce cas n'est donc pas possible quand $\deg(q) < \deg(p)$.

[Une parenthèse. Notons que pour $q(T)$ un polynôme de degré $\leq \deg(p)$, l'équation (1) implique, en remplaçant $a$ par n'importe quel élément $c$ de $B(a;\delta)$ pour $\delta \in I$ suffisamment grand, que

$$\text{Pour tout } d \in B(c;\delta)\ v(q(d)-q(c)) = v(D_j(q)(c)) + jv(d-c). \tag{1'}$$

En effet, puisque les $D_i(q)(T)$ sont de degré inférieur à $\deg(p)$, on sait par ce que nous avons déja montré que pour $\delta$ suffisamment grand, on aura $v(D_i(q)(c)) = v(D_i(q)(a))$ pour tout $c \in B(a;\delta) \cap E$. Comme pour un tel $c$ on a $B(a;\delta) = B(c;\delta)$, on obtient le résultat. ]

Nous considérons maintenant l'extension algébrique $E(\alpha)$ de $E$, où $\alpha$ est une racine de $p(T) = 0$. Nous allons étendre la valuation $v$ à $E(\alpha)$, en définissant $v(q(\alpha))$ pour tous les polynômes de degré $< \deg(p)$. Comme nous savons que ces polynômes tombent dans le cas 1 ci-dessus, nous prenons pour $v(q(\alpha))$ la valeur constante de $v(q(x))$ sur une boule $B(a;\delta) \cap E$ avec $\delta \in I$ suffisamment grand. Cela définit bien une valuation.

Nous allons maintenant montrer que le fait que pour tout $b \in E$ on ait $v(\alpha - b) = v(a-b)$ entraîne que la valuation sur $E(\alpha)$ est nécessairement celle que nous avons définie ci-dessus.

En effet, soit $q(T)$ un polynôme de degré $< \deg(p)$, et soit $\delta \in I$ tel que pour tout $i \leq \deg(q)$ et $d \in B(a;\delta) \cap E$ on ait $v(D_i(q)(d)) = v(D_i(q)(a))$. On a alors

$$q(\alpha) = q(d) + \sum_{i=1}^{\deg(q)} D_i(q)(d)(\alpha - d)^i,$$

ce qui entraîne que $v(q(\alpha)) = v(q(d))$.

(3) La preuve est similaire. On raisonne comme dans le (2), pour montrer que pour tout polynôme $p(T) \in E[T]$ il existe $\delta$ tel que si $b \in B(a;\delta)$ alors $v(p(a)) = v(p(b))$. Si d'autre part $\alpha$ est tel que $v(a-b) = v(\alpha-b)$ pour tout $b \in E$, alors le même raisonnement que dans (2) nous donne que pour tout $p(T) \in E[T]$, pour $\delta \in I$ suffisamment grand, on aura $v(p(\alpha)) = v(p(a))$, c'est-à-dire que les corps valués $E(a)$ et $E(\alpha)$ sont isomorphes.

**3.31. Remarque**. En fait je vous ai fait des séries pseudo-convergentes sans le dire (Voir la sous-section qui suit pour plus de détails sur ces suites). Il est important de remarquer que dans le (2), l'élément $a$ n'est pas nécessairement une racine de $p(T)$. Les contre-exemples sont faciles à visualiser dans les corps de séries généralisées.

On prend $\Gamma = \mathbb{Z} \times \mathbb{Z}$ avec l'ordre lexicographique, et on regarde $\mathbb{Q}(\Gamma) \subset \mathbb{Q}((\Gamma))$ ($\mathbb{Q}(\Gamma)$ est le sous-corps de $\mathbb{Q}((\Gamma))$ engendré par les $t^\gamma$, $\gamma \in \Gamma$). On voit alors que pour tout $n > 1$ et pour tout $u$ de valuation positive, l'élément $1+u$ aura une racine $n$-ième, car il a une racine résiduelle simple (1), et parce que $\mathbb{Q}((\Gamma))$ est Hensélien. Si par exemple $u = t^{(0,1)}$, alors le support de la racine $n$-ième $\alpha$ de $1+u$ sera $0 \times \mathbb{N}$. Et si $u = t^{(1,0)}$ le support de la racine $n$-ième $\beta$ de $1+u$ sera $\mathbb{N} \times 0$. Donc les approximations dans $\mathbb{Q}(\Gamma)$ de $\alpha+\beta-1$ et de $\alpha$ seront les mêmes. Pourtant le polynôme minimal de $\alpha+\beta-1$ est certainement de plus grand degré que celui de $\alpha$.

Notons que même dans le cas où $\Gamma$ est archimédien il y a des contre-exemples. En effet, prenons maintenant $\Gamma = \mathbb{Q}$, et considérons $\mathbb{F}_p((\mathbb{Q}))$, et son sous-corps $E = \bigcup_n \mathbb{F}_p((t^{1/n}))$. Alors $E$ est Hensélien puisque c'est une extension algébrique du corps Hensélien $\mathbb{F}_p((t))$. Nous savons que les racines de l'équation $X^p - X = t^{-1}$ sont de la forme $j + \sum_{i=1}^{\infty} t^{-1/p^i}$, où $j \in \mathbb{F}_p$, et donc de support bien ordonné mais qui n'est pas contenu dans un sous-groupe discret de $\Gamma$, donc ces racines ne sont pas dans $E$. Pareillement pour l'équation $X^p - X = t^{-2}$. Si $\alpha$ est une racine de $X^p - X = t^{-1}$, et $\beta$ une racine de $X^p - X = t^{-2}$, alors le polynôme irréductible de l'élément $a = \alpha + p\beta$ est de degré $p^2$ sur $E$. Cependant, comme les ensembles $\{v(b-a) \mid b \in E\}$ et $\{v(b-\alpha) \mid b \in E\}$ coïncident (ils sont tous deux égaux à $\mathbb{Q}^{<0}$), le polynôme $p(T)$ de degré minimal sera dans ce cas le polynôme $X^p - X - t^{-1}$. I.e., les éléments de $E$ ne peuvent pas distinguer entre $\alpha$ et $\alpha + p\beta$.

**3.32. Une autre remarque**. Revenons à la preuve du (2) de 3.30. Nous montrons quelque part que si $\deg(q) \leq \deg(p)$, alors il existe $j$ et $\delta_0 \in I$ tel que pour tout $\delta > \delta_0$, $v(D_j(q)(a)) + j\delta$ soit plus petit que tous les autres $v(D_i(q)(a)) + i\delta$. En fait, un ingrédient important de la preuve du théorème d'Ostrowski 3.25 est de montrer que cet indice $j$ est une puissance de la caractéristique résiduelle. Si celle-ci est 0, il est donc nécessairement égal à 1. Cela permet ensuite, en utilisant des variantes de la propriété de Hensel, de montrer que si le corps $E$ est Hensélien, alors le polynôme $p(T)$ est de degré 1, et nous donne une contradiction.

## 3.8 Suites pseudo-convergentes et pseudo-limites

**3.33. Définition**. Soit $(K, v)$ un corps valué. Une suite *pseudo-convergente* dans $K$ est une suite $(a_\alpha)_{\alpha<\kappa}$ d'éléments de $K$, indexée par des ordinaux, et telle que si $\alpha < \beta < \gamma$ alors $v(a_\alpha - a_\beta) < v(a_\beta - a_\gamma)$.

On remarque tout de suite que l'inégalité 1.2(ii) nous donne que si $\alpha < \beta$, alors $v(a_\alpha - a_\beta) = v(a_\alpha - a_{\alpha+1})$ ne dépend que de $\alpha$, et nous le notons $\gamma_\alpha$. La suite $(\gamma_\alpha)$ est donc strictement croissante.

**Définition** Soit $(a_\alpha)_{\alpha<\kappa}$ une suite pseudo-convergente, dans un corps valué $(K, v)$. Un élément $a$ (de $K$, ou bien d'une extension de $K$) est une *pseudo-limite de* $(a_\alpha)$, noté $(a_\alpha) \Rightarrow a$, si pour tout $\alpha < \kappa$ on a $v(a - a_\alpha) = \gamma_\alpha$.

**3.34. Extensions immédiates et suites pseudo-convergentes**.

Soit $(L, v)$ une extension immédiate de $(K, v)$, et soit $a \in L \setminus K$. Nous pouvons alors associer à $a$ une suite pseudo-convergente ayant $a$ pour pseudo-limite : nous considérons $I = \{v(c - a) \mid c \in K\}$ ; nous savons que c'est un segment initial de $\Gamma$ sans plus grand élément ; nous choisissons une suite strictement croissante $(\gamma_\alpha)$ d'éléments de $I$ qui soit cofinale dans $I$, puis des éléments $a_\alpha \in K$ tels que $v(a - a_\alpha) = \gamma_\alpha$.

Réciproquement, soit $(a_\alpha)_{\alpha<\kappa}$ une suite pseudo-convergente d'éléments de $K$, et supposons qu'elle n'ait pas de pseudo-limite dans $K$. S'il existe $p(T) \in K[T]$ non nul et tel que $(p(a_\alpha))_\alpha \Rightarrow 0$, on dira que la suite est de type *algébrique*, et sinon qu'elle est de type *transcendant*. Dans les deux cas, comme dans la preuve du Lemme 3.30, on montre qu'il existe une extension immédiate de $K$ engendrée au-dessus de $K$ par une pseudo-limite $a$ de la suite, et que le type d'isomorphisme du corps $K(a)$ est uniquement déterminé si la suite est de type transcendant, et aussi si elle est de type algébrique et on impose que $p(T)$ est le polynôme minimal de $a$ sur $K$ et est de degré minimal tel que $(p(a_\alpha))$ pseudo-converge.

Comme nous l'avons déjà observé dans 3.31, si la suite $(\gamma_\alpha)$ associée à la suite pseudo-convergente $(a_\alpha)$ n'est pas cofinale dans le groupe de valeurs $\Gamma$ de $K$, alors la suite $(a_\alpha)_\alpha$ a plusieurs pseudo-limites dans $K(a)$ : en efffet, si $b \in K$ est tel que $v(b) > \gamma_\alpha$ pour tout $\alpha$, alors $(a_\alpha) \Rightarrow a + b$.

Le seul groupe de valeurs pour lequel toute suite pseudo-convergente a une unique pseudo-limite est donc $\mathbb{Z}$ (ou bien 0, si on admet la valuation triviale).

# 4 Elimination des quantificateurs dans le langage de Pas

**4.1.** Rappellons que le langage de Pas, $\mathcal{L}_{\text{Pas}}$, est le langage à 3 sortes : la sorte du corps, celle du groupe de valeurs, et celle du corps résiduel, auxquels on rajoute les symboles suivants :

— Pour les éléments du corps valué, le langage des anneaux $\mathcal{L}_{\text{c.val}} = \{+, -, \cdot, 0, 1\}$.

— Pour les éléments du groupe de valeurs, le langage des groupes ordonnés augmenté par une constante $\infty$ : $\mathcal{L}_{\text{gp}} = \{+, -, <, 0, \infty\}$.

— Pour les éléments du corps résiduel, le langage des anneaux $\mathcal{L}_{\text{c.rés}} = \{+, -, \cdot, 0, 1\}$.

Nous avons aussi une application $v$ allant du corps valué dans le groupe de valeurs (union $\infty$), et une application coefficient angulaire $\overline{\text{ac}}$ allant du corps valué sur le corps résiduel.

**Théorème** (Pas). Soient $(K, v)$ un corps valué Hensélien de caractéristique résiduelle **nulle** et muni d'une application coefficient angulaire, et $(K, \Gamma, k)$ la $\mathcal{L}_{\text{Pas}}$-structure qui lui est associée.

Alors

(1) On considère la théorie $T_0$ obtenue en prenant tout d'abord la théorie à trois sortes dont les modèles sont les $\mathcal{L}_{\text{Pas}}$-structures à 3 sortes associées à des corps valués Henséliens $(K, v)$ qui satisfont les conditions ci-dessus : on dit que $K$ est un corps, que l'application $v$ est une application de $K$ dans $\Gamma \cup \{\infty\}$, qui définit une valuation sur $K$, de groupe de valeurs $\Gamma$, et que $K$ est Hensélien pour cette valuation. De plus l'application $\overline{\text{ac}} : K \to k$ satisfait les conditions suivantes : $\overline{\text{ac}}(0) = 0$ ; sa restriction à $K^\times$ définit un morphisme de groupe (multiplicatif) à valeurs dans $k^\times$ ; si on définit res : $\mathcal{O}_v \to k$ en posant

$$\operatorname{res} x = \begin{cases} \overline{\text{ac}}(x) & \text{si } v(x) = 0, \\ 0 & \text{si } v(x) > 0, \end{cases}$$

alore l'application res est un morphisme d'anneau qui est surjectif et a pour noyau l'idéal $\mathcal{M}_v$ ; le corps $k$ est de caractéristique 0.

A cette théorie $T_0$ nous ajoutons $\text{Th}(k)$ (dans $\mathcal{L}_{\text{c.rés}}$) et $\text{Th}(\Gamma)$ (dans $\mathcal{L}_{\text{gp}}$) pour obtenir une théorie $T$.

Alors $T$ est complète.

(2) La théorie $T$ élimine les quantificateurs du corps valué, c'est-à-dire, étant donné une formule $\Phi(x, \xi, \bar{u})$ ($x, \xi, \bar{u}$ des uplets de variables), il existe une formule $\Psi(x, \xi, \bar{u})$ dans laquelle les seules variables quantifiées sont des variables du groupe ou du corps résiduel, et telle que

$$T \vdash \forall x, \xi, \bar{u}\ (\Phi(x, \xi, \bar{u}) \iff \Psi(x, \xi, \bar{u})).$$

Pour montrer ce résultat, nous aurons tout d'abord besoin d'un lemme de théorie des modèles :

**4.2. Lemme**. Soient $\mathcal{L}$ un langage (contenant au moins un symbole de constante), $\kappa$ un cardinal infini $> |\mathcal{L}|$, $\Delta$ un ensemble de formules clos par combinaisons Booléennes, et $T$ une théorie.

Supposons que si $M$ et $N$ sont deux modèles $\kappa$-saturés de $T$, et si $f : A \to B$ est un isomorphisme entre des sous-structures $A$ de $M$ et $B$ de $N$ avec $|A| < \kappa$, qui préserve les formules de $\Delta$ (c'est-à-dire, pour toute formule $\varphi(x) \in \Delta$ et uplet $a$ dans $A$, on a $M \models \varphi(a) \Rightarrow N \models \varphi(f(a))$), alors pour tout $a \in M$ il existe un isomorphisme $g$ entre des sous-structures de $M$ et $N$ respectivement, qui prolonge $f$ et a $a$ dans son domaine, et préserve les formules de $\Delta$.

Alors, si $\varphi(x)$ est une formule, il existe $\psi(x) \in \Delta$ telle que $T \models \forall x\ (\varphi(x) \leftrightarrow \psi(x))$.

Si de plus on a que étant donnés deux modèles quelconques $M$ et $N$ de $T$, alors $M$ et $N$ satisfont les mêmes énoncés de $\Delta$, alors la théorie $T$ est complète.

*Démonstration.* Soit $\mathcal{L}'$ le langage obtenu en ajoutant à $\mathcal{L}$ un symbole de relation $R_\varphi$ pour chaque formule $\varphi(x) \in \Delta$, $R_\varphi$ étant de même arité que $\varphi(x)$, et soit $T'$ l'extension par définitions de $T$ obtenu en ajoutant à $T$ les axiomes $\forall x(R_\varphi(x) \leftrightarrow \varphi(x))$. Tout modèle $M$ de $T$ s'enrichit alors uniquement en une $\mathcal{L}'$-structure $M'$ modèle de $T'$, et nos hypothèses impliquent alors que $T'$ élimine les quantificateurs dans le langage $\mathcal{L}'$, cf. Lemme 2.10 (Bien que notre hypothèse ne nous donne formellement que le *va*, le *vient* suit car nous avons supposé que $\Delta$ était clos par négation).

Toute $\mathcal{L}$-formule $\varphi(x)$ est donc équivalente, modulo $T'$, à une $\mathcal{L}'$-formule sans quantificateurs ; c'est-à-dire, comme $\Delta$ est clos par combinaison Booléennes, à une formule $R_\psi(x)$ pour une formule $\psi \in \Delta$ ; ou encore, à une formule $\psi(x)$ de $\Delta$. En utilisant les lemmes d'interpolation, l'équivalence $\varphi(x) \leftrightarrow \psi(x)$ est démontrable dans $T$, ce qui nous donne le résultat.

Le deuxième assertion suit de la première, puisque tout énoncé est équivalent à un énoncé dans $\Delta$.

**4.3.** *Plan de démonstration du Théorème 4.1.*

Soient $(K, \Gamma_K, k_K)$ et $(L, \Gamma_L, k_L)$ des modèles $\aleph_1$-saturés de $T$. Soit $\Delta$ l'ensemble des formules dans lesquelles les seules variables quantifiées sont celles du groupe de valeurs et du corps résiduel. Remarquons tout d'abord que la sous-structure de $(K, \Gamma_K, k_K)$ engendrée par les constantes et la sous-structure de $(L, \Gamma_L, k_L)$ engendrée par les constantes sont isomorphes :

En effet, ces deux sous-structures seront égales à $(\mathbb{Z}, (0), \mathbb{Z})$, avec valuation triviale.

Soient $(A, \Gamma_A, k_A)$ et $(B, \Gamma_B, k_B)$ des sous-structures dénombrables de $(K, \Gamma_K, k_K)$ et $(L, \Gamma_L, k_L)$ respectivement, isomorphes par un isomorphisme $f$ qui préserve les formules de $\Delta$. Nous voulons montrer que étant donné un élement $a \in K \cup \Gamma_K \cup k_K$ nous pouvons prolonger $f$ à un isomorphisme partiel $g$ ayant $a$ dans son domaine et qui préserve les formules de $\Delta$.

Soit $(C, \Gamma_C, k_C)$ une sous-structure élémentaire de $(K, \Gamma_K, k_K)$ qui contient $(A, \Gamma_A, k_A)$ et $a$, et est dénombrable. Nous allons prolonger $f$ à cette sous-structure. Notons d'abord que nous avons $v(A \setminus 0) \subset \Gamma_A$ et $\overline{\mathrm{ac}}(A) \subset k_A$, ces inclusions pouvant être strictes. Par contre, les applications $v : C^\times \to \Gamma_C$ et $\mathrm{res} : \mathcal{O}_C = \mathcal{O}_K \cap C \to k_C$ sont surjectives.

La démonstration se fera en plusieurs étapes, chacune agrandissant la structure $(A, \Gamma_A, k_A)$. Certaines étapes seront répétées plusieurs fois. L'ingrédient principal qui fait marcher la démonstration, est le fait que si $A$ est un sous-corps valué de $K$, alors sa Hensélianisée n'a pas d'extension algébrique immédiate, et qu'elle est unique à $A$-isomorphisme près. Cela nous permettra de conclure que si nous avons un isomorphisme entre $A \subset K$ et $B \subset L$, alors cet isomorphisme s'étend en un isomorphisme entre les Hensélianisées de $A$ et de $B$. Cet ingrédient est malheureusement faux la plupart du temps quand la caractéristique résiduelle n'est pas nulle.

Les étapes de la preuve sont les suivantes :

Etape 0 : remplacer $A$ et $k_A$ par leur corps des fractions (facile).

Etape 1 : agrandir $k_A$ pour obtenir $(A, \Gamma_A, k_C)$ et étendre $f$ (facile).

Etape 2 : agrandir $\Gamma_A$ pour obtenir $(A, \Gamma_C, k_C)$, et étendre $f$ (facile).

Etape 3 : remplacer $A$ par $A^h$ et étendre $f$ (facile).

Etape 4 : agrandir $A$ pour l'application res soit surjective sur $k_C$, et étendre $f$ (pas difficile).

Etape 5 : agrandir $A$ pour que $v$ soit surjective sur $\Gamma_C$, et étendre $f$. Cette partie sera faite en plusieurs étapes, et utilisera le lemme 3.28. C'est le seul endroit où nous devrons faire attention à $\overline{\text{ac}}$.

Etape 6 : Etendre $f$ à tout $C$, en plusieurs étapes, et en utilisant le fait que $C$ est une extension immédiate de $A$.

**4.4. Remarques**. La preuve de ce théorème nous donnera (assez) facilement d'autres résultats :

— Si on agrandit les langages du groupe de valeurs et du corps résiduel de façon à ce qu'ils éliminent les quantificateurs, on obtient alors une élimination de quantificateurs dans ce nouveau langage. En particulier, dans le cas des séries formelles, on connait un langage dans lequel la théorie du groupe ordonné $\mathbb{Z}$ élimine les quantificateurs : on rajoute pour chaque $n > 1$ un symbole de relation $\equiv_n$, interprété par "congru modulo $n$". Nous pourrons alors en déduire le résultat d'élimination des quantificateurs pour la théorie des corps de séries formelles sur un corps algébriquement clos de caractéristique 0 (ou sur un corps réel clos, si on ajoute l'ordre au langage du corps résiduel).

— Ce résultat nous donnera immédiatement le principe d'AKE (Ax-Kochen-Ershov) pour ces corps.

— La preuve s'adaptera au cas des corps $p$-adiques, et de ses extensions finies, grâce aux lemmes algébriques. Nous en déduirons l'élimination des quantificateurs dans le langage $\mathcal{L}_{\text{Mac}}$ de Macintyre.

## 4.1 Preuve du Théorème 4.1

**4.5. Les formules de $\Delta$**. Avant de commencer, nous allons un peu regarder à quoi ressemblent les formules de $\Delta$. Soit $\Phi(x, \xi, \bar{u})$ une telle formule, avec $x$ un uplet de variables de $\mathcal{L}_{\text{c.val}}$, $\xi$ un uplet de variables de $\mathcal{L}_{\text{gp}}$ et $\bar{u}$ un uplet de variables de $\mathcal{L}_{\text{c.rés}}$. Alors, $\Phi$ est une formule de la forme

$$\bar{Q}(\xi_1, \bar{u}_1)\ \Psi(x, \xi, \xi_1, \bar{u}, \bar{u}_1),$$

où $\Psi$ est une formule sans quantificateurs, $(\xi_1, \bar{u}_1)$ est un uplet de variables de $\mathcal{L}_{\text{gp}} \cup \mathcal{L}_{\text{c.rés}}$, et $\bar{Q}$ un uplet de quantificateurs. De plus, la formule $\Psi$ sera une disjonction de formules de la forme

$$\varphi_0(x) \wedge \psi_1(v(t_1(x)), \xi, \xi_1) \wedge \psi_2(\overline{\text{ac}}(t_2(x)), \bar{u}, \bar{u}_1),$$

où $\varphi_0(x)$ est une $\mathcal{L}_{\text{c.val}}$-formule sans quantificateurs, $\psi_1(\lambda, \xi, \xi_1)$ est une $\mathcal{L}_{\text{gp}}$-formule sans quantificateurs, $\psi_2(\bar{v}, \bar{u}, \bar{u}_1)$ est une $\mathcal{L}_{\text{c.rés}}$-formule sans quantificateurs, $t_1(x)$ et $t_2(x)$ sont des uplets de termes obtenus en utilisant les opérations de $\mathcal{L}_{\text{c.val}}$. Les variables de $\xi_1$ n'apparaissent que dans les formules de type $\psi_1$, et celles de $\bar{u}_1$ que dans les formules de type $\psi_2$. Cela entraîne que $\Phi(x, \xi, \bar{u})$ est logiquement équivalente à une disjonction de formules de la forme

$$\varphi_0(x) \wedge \varphi_1(v(t_1(x)), \xi) \wedge \varphi_2(\overline{\text{ac}}(t_2(x)), \bar{u}), \tag{1}$$

où $\varphi_0(x)$ est une $\mathcal{L}_{\text{c.val}}$-formule sans quantificateurs, $\varphi_1(\lambda, \xi)$ est une $\mathcal{L}_{\text{gp}}$-formule, $\varphi_2(\bar{v}, \bar{u})$ est une $\mathcal{L}_{\text{c.rés}}$-formule, $t_1(x)$ et $t_2(x)$ sont des uplets de termes obtenus en utilisant les opérations de $\mathcal{L}_{\text{c.val}}$. Ici j'utilise tout simplement que si le uplet de variables $y$ n'apparaît pas dans la formule $\varphi(x)$ alors $\exists y\ (\varphi(x) \wedge \psi(x,y))$ [resp. $\exists y\ (\varphi(x) \vee \psi(x,y))$] est logiquement équivalente à $\varphi(x) \wedge \exists y\ \psi(x,y)$ [resp. à $\varphi(x) \vee \exists y\ \psi(x,y)$]. Ces équivalences sont valides en logique classique du premier ordre, donc aussi pour les logiques à plusieurs sortes. Pour vérifier qu'un $\mathcal{L}_{\text{Pas}}$-isomorphisme préserve les formules de $\Delta$, il suffit donc de vérifier qu'il préserve celles comme dans (1).

**4.6. Remarque sur les coefficients angulaires** On montre facilement que si $a, b \in K$ ont la même valuation, alors

$$\overline{\text{ac}}(a) = \overline{\text{ac}}(b) \iff v(a-b) > v(a).$$

En effet, si $v(a) = v(b)$ alors $v(\frac{a}{b}) = 0$. $\overline{\text{ac}}(a) = \overline{\text{ac}}(b)$ est équivalent à $\overline{\text{ac}}(\frac{a}{b}) = 1$, ce qui est équivalent à $v(\frac{a}{b} - 1) > 0$, et donc à $v(a-b) = v(b) + v(\frac{a}{b} - 1) > v(b) = v(a)$. Cette remarque nous sera utile pour les extensions immédiates.

**4.7. Etape 0**.

Comme la langage des groupes contient $-$, nous savons que $\Gamma_A$ est un sous-groupe de $\Gamma_K$. Celui des anneaux ne contient pas $^{-1}$, et donc $A$ et $k_A$ ne seront a priori que des anneaux. Il est cependant clair que les isomorphismes $f|_A$ et $f|_{k_A}$ s'étendent uniquement à des isomorphismes définis sur les corps de fractions correspondant. De plus, l'extension de $f|_A$ au corps de fractions est un isomorphisme de corps valués, qui commute avec $\overline{\text{ac}}$ : si $a, b \neq 0 \in A$, alors $v(a/b) = v(a) - v(b)$ et $\overline{\text{ac}}(ab^{-1}) = \overline{\text{ac}}(a)\overline{\text{ac}}(b)^{-1}$.

*Nous pourrons donc toujours supposer que les structures $A$ et $k_A$ sont des corps.*

**Etape 1**. Nous prolongeons $f$ à $k_C$.

Soit $a_i$, $i \in \mathbb{N}$, une énumération de $k_C$. Par hypothèse, l'isomorphisme induit par $f$ sur les anneaux $k_A$ et $k_B$ préserve toutes les formules, c'est-à-dire, est élémentaire au sens de la théorie du corps résiduel. Nous travaillons maintenant dans le langage $\mathcal{L}_{\text{c.rés}}$ du corps résiduel, auquel nous ajoutons des constantes pour les éléments de $k_A$. L'isomorphisme $f : k_A \to k_B$ est donc un isomorphisme de $\mathcal{L}_{\text{c.rés}}(k_A)$-structures.

Considérons l'ensemble $\Sigma(u)$ de $\mathcal{L}_{\text{c.rés}}(k_A)$-formules satisfaites par $a_0$. Cet ensemble est finiment satisfaisable dans $k_K$, et comme $f|_{k_A}$ est un isomorphisme élémentaire (c'est-à-dire, qui préserve les $\mathcal{L}_{\text{c.rés}}$-formules), il est aussi finiment satisfaisable dans $k_L$. Comme $L$ est $\aleph_1$-saturé, il existe $b_0 \in k_L$ qui satisfait les mêmes $\mathcal{L}_{\text{c.rés}}(k_A)$-formules que $a_0$, et nous prolongeons $f$ au sous-corps de $k_C$ engendré par $a_0$ au-dessus de $k_A$ en un isomorphisme $f_1$ qui envoie $a_1$ sur $b_0$. Alors $f_1$ est un $\mathcal{L}_{\text{Pas}}$-isomorphisme, dont la restriction au sous-corps de $k_C$ engendré par $k_A$ et $a_0$ est élémentaire (au sens de $\text{Th}(k_K)$). Comme $A$ n'a pas grandi, et que son image par $v$ est contenue dans $\Gamma_A \cup \{\infty\}$, son image par $\overline{\text{ac}}$ est contenue dans $k_A$, et par les commentaires faits au début de la preuve, nous avons que $f_1$ préserve bien les formules de $\Delta$. On répète cette procédure jusqu'à ce qu'on ait étendu la fonction $f$ à $(A, \Gamma_A, k_C)$ en préservant les formules de $\Delta$.

*Nous pouvons donc supposer que $f$ est définie sur la structure $(A, \Gamma_A, k_C)$.*

**Etape 2**. Nous prolongeons $f$ à $\Gamma_C$.

Soit $\gamma_i$, $i \in \mathbb{N}$, une énumération de $\Gamma_C$. On raisonne comme dans l'étape 1, pour prolonger $f$ à la sous-structure $(A, \Gamma_C, k_C)$ en préservant les formules de $\Delta$.

*Nous pouvons donc supposer que $f$ est définie sur la structure $(A, \Gamma_C, k_C)$. Il reste à étendre $f$ sur la sorte "corps valué", c'est-à-dire, l'étendre à tout $C$.*

**4.8. Remarque utile**. Supposons que nous ayions réussi à prolonger $f$ en un $\mathcal{L}_{\text{Pas}}$-isomorphisme $f_1$ d'une sous-structure $(A_1, \Gamma_C, k_C)$ de $(C, \Gamma_C, k_C)$. Comme $v(A_1) \subset \Gamma_C \cup \{\infty\}$, $\overline{\text{ac}}(A_1) \subset k_C$, nous aurons que nécessairement $f_1$ préserve les formules de $\Delta$. En effet, il suffit de regarder celles de la forme $\varphi_0(x) \wedge \varphi_1(v(t_1(x)), \xi) \wedge \varphi_2(\overline{\text{ac}}(t_2(x)), \bar{u})$ donnée dans (1) : $f_1$ étant un $\mathcal{L}_{\text{Pas}}$-isomorphisme, il préservera les formules de type $\varphi_0$ (puisqu'elles sont sans quantificateurs, et ne font que dire des choses sur le corps valué). D'autre part, si $a$ est un uplet de $a_1$, alors $v(t_1(a)) \in v(A) = \Gamma_C \cup \{\infty\}$, et $\overline{\text{ac}}(t_2(a)) \in k_A = k_C$. Comme $f_1$ est un $\mathcal{L}_{\text{Pas}}$-isomorphisme, il préservera donc les formules de type $\varphi_1$ et $\varphi_2$. Dans toutes les étapes qui suivent, il nous suffira donc de montrer que $f$ s'étend à un $\mathcal{L}_{\text{Pas}}$-isomorphisme.

**4.9. Etape 3**. Etendre $f$ à l'Hensélianisée de $A$.

Nous savons que l'Hensélianisée $A^h$ de $A$ est unique (à $A$-isomorphisme près), et donc le corps Hensélien $C$ en contient une copie (que nous noterons aussi $A^h$). Par le Théorème 3.26, nous savons que en fait $A^h = C \cap A^{alg}$. Le même raisonnement donne que $L \cap B^{alg}$ est la Hensélianisée de $B$, et comme $f$ est un isomorphisme de corps valués, et $L$ est un corps Hensélien contenant $B$, $f|_A$ s'étend à un isomorphisme $f_1$ de corps valués $A^h \to B^h$. Puisque $A^h$ est une extension immédiate de $A$, si $a \in A^h \setminus A$, alors il existe $a' \in A$ tel que $v(a - a') > v(a) = v(a')$. C'est à dire, $a = a'(1 + u)$ où $v(u) > 0$, et $\overline{\text{ac}}(a) = \overline{\text{ac}}(a')$. On aura aussi $w(f(a) - f(a')) > w(f(a))$ et $\overline{\text{ac}}(f(a)) = \overline{\text{ac}}(f(a')) = f(\overline{\text{ac}}(a))$, ce qui montre que $f_1 \cup f|_{\Gamma_C} \cup f|_{k_C}$ est un $\mathcal{L}_{\text{Pas}}$-isomorphisme, qui préserve les formules de $\Delta$.

**4.10. Etape 4**. Etendre $f$ à un sous-corps $D$ de $C$ tel que $\text{res}(\mathcal{O}_D) = k_D$ ($\mathcal{O}_D$ dénotant $\mathcal{O}_C \cap D = \mathcal{O}_K \cap D$).

Tout d'abord, nous pouvons supposer que $A$ est un sous-corps de $K$, dont le corps résiduel sera noté $k'_A$, et l'anneau de valuation $\mathcal{O}_A$. Le corps résiduel du corps $f(A) = B$ sera noté $k'_B$, et son anneau de valuation $\mathcal{O}_B$. Puisque $f(A) = B$, $f$ définit un isomorphisme entre $k'_A$ et $k'_B$. Soit $\bar{a} \in k_C$, $\bar{a} \notin k'_A$, et supposons le algébrique sur $k'_A$. Soit $\bar{F}(T)$ son polynôme minimal unitaire sur $k'_A$, et soit $F(T) \in \mathcal{O}_A[T]$ un polynôme unitaire de même degré que $\bar{F}(T)$ tel que $\text{res}(F)(T) = \bar{F}(T)$. Alors $F(T)$ est aussi irréductible. Comme $k_K$ est de caractéristique nulle, nous savons que $\bar{F}'(\bar{a}) \neq 0$. Puisque $C$ est Hensélien, il existe $a \in \mathcal{O}_C$ tel que $\text{res}(a) = \bar{a}$ et $F(a) = 0$. Nous regardons maintenant ce qui se passe de l'autre côté. Nous savons que $f(\bar{F})(T)$ est irréductible sur $k'_B$, séparable, a $f(\bar{a})$ pour racine simple, et il existe donc $b \in L$ tel que $\text{res}(b) = f(\bar{a})$, $f(F)(b) = 0$. On étend $f$ à $A(a)$ en posant $f_1(a) = b$. Si $n$ est le degré de $F$ (et de $\bar{F}$), on sait que les éléments $1, \text{res}(a), \ldots, \text{res}(a^{n-1})$ sont $k'_A$-linéairement indépendants, et donc que si $c_0, \ldots, c_{n-1} \in A$, alors $v(\sum_{i=0}^{n-1} c_i a^i) = \min_i\{v(c_i)\}$ (cf la preuve de 3.7). De même, les éléments $1, \text{res}(b), \ldots, \text{res}(b^{n-1})$ sont $k'_B$-linéairement indépendants, et cela entraîne que $f_1$ définit bien un isomorphisme entre les corps valués $A(a)$ et $B(b)$. On remarque

maintenant que tout élément (non nul) de $A(a)$ s'écrit comme le produit d'un élément de valuation 0 et d'un élément de $A$ (puisque les groupes de valeurs de $A$ et de $A(a)$ sont les mêmes). Par construction, $f_1$ commute avec l'application res, qui coïncide avec $\overline{\text{ac}}$ sur les éléments de valuation 0. L'isomorphisme $f_1$ est donc bien un isomorphisme de $\mathcal{L}_{\text{Pas}}$-structures.

Si $\bar{a}$ n'est pas algébrique sur $k'_A$, alors nous prenons pour $a$ un élément de $C$ tel que $\text{res}\,(a) = \bar{a}$, pour $b$ un élément de $L$ tel que $\text{res}\,(b) = f(\bar{a})$, et étendons $f$ en posant $f(a) = b$. Les éléments $a$ et $b$ sont alors transcendants sur $A$ et sur $B$ respectivement, et comme dans le cas précédent, si $c_0, \ldots, c_n \in A$ alors $v(\sum_i c_i a^i) = \min_i\{v(c_i)\}$ et $w(\sum_i f(c_i)b^i) = \min_i\{w(f(c_i))\} = f(\min_i\{v(c_i)\}) = f(v(\sum_i c_i a^i))$, ce qui montre que l'isomorphisme de corps $A(a) \to B(b)$ qui prolonge $f$ et envoie $a$ sur $b$ est un isomorphisme de corps valués. Comme dans le cas précédent, c'est un isomorphisme de $\mathcal{L}_{\text{Pas}}$-structures, qui préserve donc les formules de $\Delta$.

Nous répétons cette procédure jusqu'à ce que nous ayions épuisé $k_C$.

*Nous sommes donc dans la situation où $A$ a corps résiduel $k_C$, et où $\Gamma_A = \Gamma_C$.*

**4.11. Etape 5**. Etendre $f$ à un sous-corps $E$ de $C$ tel que $v(E^\times) = \Gamma_C$.

Soit $\Gamma'_A$ le groupe de valeurs de $A$, et soit $\alpha \in \Gamma_A$, $\alpha \notin \Gamma'_A$, et $\alpha > 0$. Supposons d'abord que pour tout entier positif $n$, $n\alpha \notin \Gamma'_A$. Alors, si $a \in C$ est tel que $v(a) = \alpha$, $a$ sera transcendant sur $A$, et si $b \in L$ est tel que $w(b) = f(\alpha)$, $b$ sera transcendant sur $B$. Choisissons de tels $a$ et $b$ avec $\overline{\text{ac}}(a) = 1$, $\overline{\text{ac}}(b) = 1$, et prenons un prolongement $f_1$ de $f|_A$ à $A(a)$ en envoyant $a$ sur $b$. Alors, par 3.7, $f_1$ est un isomorphisme de corps valués, et donc $f_1 \cup f|_{\Gamma_A \cup k_A}$ est un $\mathcal{L}_{\text{Pas}}$-isomorphisme.

Supposons maintenant qu'il existe un entier $n > 0$ tel que $n\alpha \in \Gamma'_A$, et prenons un tel $n$ minimal. Le lemme 3.28 nous donne qu'il existe $a \in C$ tel que $v(a) = \alpha$, et $a^n \in A$. Il nous faut donc montrer que $f(a^n)$ a une racine $n$-ième dans $L$, et qu'on peut la prendre ayant pour coefficient angulaire $f(\overline{\text{ac}}(a))$.

Par le lemme 3.28 nous savons qu'il existe $c \in L$ tel que $c^n \in B$ et $w(c) = f(\alpha)$. Comme $c$ est algébrique sur $B$ et le corps résiduel de $B$ est $f(k_C) \prec k_L$, il existe $d \in \mathcal{O}_B$ tel que $\text{res}\,(d) = f(\overline{\text{ac}}(\bar{a}))\overline{\text{ac}}(c^{-1})$ ; multipliant $c$ par $d$, nous pouvons supposer que $\overline{\text{ac}}(c) = f(\overline{\text{ac}}(a))$. Alors $f(a^n) = c^n(1+u)$, où $w(u) > 0$. Comme $w(n) = 0$, grâce à 3.28(1), il existe $d \in L$ tel que $d^n = (1+u)$ et $\text{res}\,(d) = 1$, et nous posons alors $b = cd$. Nous avons $w(cd) = f(\alpha)$, $\overline{\text{ac}}(cd) = f(\overline{\text{ac}}(a))$, et par 3.7, l'isomorphisme $A(a) \to B(b)$ qui prolonge $f$ et envoie $a$ sur $b$ est un $\mathcal{L}_{\text{Pas}}$-isomorphisme.

Nous itérons la procédure jusqu'à ce que nous ayions épuisé $\Gamma_C$.

Nous nous trouvons maintenant dans la situation suivante : nous avons un $\mathcal{L}_{\text{Pas}}$-isomorphisme $f : (A, \Gamma_C, k_C) \to (B, f(\Gamma_C), f(k_C))$ qui respecte les formules de $\Delta$, où $A$ et $B$ sont des sous-corps de $C$ et $L$ respectivement, et $C$ est une extension immédiate de $A$. En appliquant l'étape 3, nous supposerons que $A$ est Hensélien.

**Etape 6**.

Soit $a \in C$, $a \notin A$, et considérons $I = \{v(c-a) \mid c \in A\}$. Par 3.26, nous savons $A$ n'a pas d'extension algébrique immédiate propre, et cela entraîne que $a$ est transcendant sur $A$, et que si $p(T) \in A[T]$, alors pour un $\delta \in I$, nous avons que $v(p(x))$ est constant sur $B(a;\delta) \cap A$.

Supposons que nous ayions trouvé $b \in L$ tel que $w(b - f(c)) = f(v(a - c))$ pour tout $c \in A$. Alors $v(f(p)(x))$ sera constant sur $B(f(a'); f(\delta)) \cap A$, où $a'$ est n'importe quel élément de $B(a; \delta) \cap A$. Cela entraîne que $b$ est transcendant sur $B$, et que l'isomorphisme $f_1 : A(a) \to B(b)$ qui prolonge $f|_A$ et envoie $a$ sur $b$, est un isomorphisme de corps valués. Comme dans l'étape 3, on vérifie que $f_1 \cup f$ commute avec $\overline{\text{ac}}$ et définite donc un $\mathcal{L}_{\text{Pas}}$-isomorphisme étendant $f$.

Considérons l'ensemble de formules $\Sigma(x) = \{w(x - f(c)) = f(v(a - c)) \mid c \in A\}$. Cet ensemble est finiment consistant dans $B$ : si $c_1, \ldots, c_n \in A$ alors il existe $c \in A$ tel que $v(a - c) > v(a - c_i)$ pour $i = 1, \ldots, n$, et donc $v(c - c_i) = v(a - c_i)$ pour $i = 1, \ldots, n$. Cela entraîne que $f(c)$ satisfait $w(x - f(c_i)) = f(v(a - c_i))$ pour $i = 1, \ldots, n$.

En utilisant la $\aleph_1$-saturation de $L$ ($f(A)$ est dénombrable), il existe donc $b \in L$ tel que pour tout $c \in A$,

$$w(b - f(c)) = f(v(a - c)).$$

Le type d'isomorphisme du corps valué $B(b)$ est lui aussi uniquement déterminé par la fonction $B \to f(I)$, $d \mapsto w(b - d)$, et nous avons donc que l'isomorphisme $f_1 : A(a) \to B(b)$ qui prolonge $f$ et envoie $a$ sur $b$ est bien un isomorphisme de corps valués. Comme $A(a)$ est une extension immédiate de $A$, c'est aussi un $\mathcal{L}_{\text{Pas}}$-isomorphisme.

Maintenant nous appliquons les résultats de l'étape 3 pour prolonger $f_1$ à la clôture Hensélienne de $A(a)$, c'est-à-dire, à $A(a)^{alg} \cap C$. Nous itérons cette procédure jusqu'à ce que nous ayions épuisé $C$. Fin de la preuve !!

**4.12. Une conséquence facile de 4.1**. Soit $\mathcal{L}'_{\text{Pas}}$ un langage à 3-sortes obtenu à partir du langage $\mathcal{L}_{\text{Pas}}$ en agrandissant les langages $\mathcal{L}_{\text{gp}}$ et $\mathcal{L}_{\text{c.rés}}$. On a donc

$$\mathcal{L}'_{\text{Pas}} = \mathcal{L}_{\text{c.val}} \cup \mathcal{L}'_{\text{gp}} \cup \mathcal{L}'_{\text{c.rés}} \cup \{v, \overline{\text{ac}}\}.$$

Par exemple on peut leur rajouter des symboles de constantes, mais on peut aussi rajouter de la structure plus compliquée. Si on examine la preuve de 4.1, on observe que le seul endroit où on travaille vraiment avec les structures de groupes valués et de corps résiduels, est pendant les étapes 1 et 2. Après cela, on travaille uniquement sur l'univers du corps valué. Nous avons donc en fait montré un résultat bien plus fort :

**Théorème**. Soient $(K, v)$ un corps valué Hensélien de caractéristique résiduelle **nulle**, et $(K, \Gamma, k)$ la $\mathcal{L}_{\text{Pas}}$-structure qui lui est associée. Soient $\mathcal{L}'_{\text{gp}}$ et $\mathcal{L}'_{\text{c.rés}}$ des langages contenant $\mathcal{L}_{\text{gp}}$ et $\mathcal{L}_{\text{c.rés}}$ respectivement, et supposons que $\Gamma$ est muni d'une $\mathcal{L}'_{\text{gp}}$-structure, et $k$ d'une $\mathcal{L}'_{\text{c.rés}}$-structure.

(1) A la théorie $T_0$ définie dans 4.1 nous ajoutons $\text{Th}_{\mathcal{L}'_{\text{c.rés}}}(k)$ et $\text{Th}_{\mathcal{L}'_{\text{gp}}}(\Gamma)$ pour obtenir une théorie $T'$ de $\mathcal{L}'_{\text{Pas}}$.

Alors $T'$ est complète.

(2) La théorie $T'$ élimine les quantificateurs du corps valué, c'est-à-dire, étant donné une formule $\Phi(x, \xi, \bar{u})$, il existe une formule $\Psi(x, \xi, \bar{u})$ dans laquelle les seules variables quantifiées sont des variables du groupe ou du corps résiduel, et telle que

$$T \vdash \forall x, \xi, \bar{u}\ (\Phi(x, \xi, \bar{u}) \iff \Psi(x, \xi, \bar{u})).$$

**4.13. Corollaire**. Notations et hypothèses comme dans 4.12. Si de plus $\mathrm{Th}_{\mathcal{L}'_{\mathrm{c.rés}}}(k)$ et $\mathrm{Th}_{\mathcal{L}'_{\mathrm{gp}}}(\Gamma)$ éliminent les quantificateurs, alors $T'$ aussi.

*Démonstration.* Par la remarque faite au début de la preuve de 4.1, on sait que toute $\mathcal{L}'_{\mathrm{Pas}}$-formule $\Phi(x, \xi, \bar{u})$ est équivalente, modulo $T'$, à une disjonction de formules de la forme

$$\varphi_0(x) \wedge \varphi_1(v(t_1(x), \xi) \wedge \varphi_2(t_2(x), \bar{u})$$

où $t_1(x)$, $t_2(x)$ sont des $\mathcal{L}_{\mathrm{c.val}}$-termes (c'est-à-dire, des polynômes sur $\mathbb{Z}$), $\varphi_0$ est une $\mathcal{L}_{\mathrm{c.val}}$-formule sans quantificateurs, $\varphi_1(\lambda, \xi)$ est un $\mathcal{L}'_{\mathrm{gp}}$-formule, et $\varphi_2(\bar{v}, \bar{u})$ est une $\mathcal{L}'_{\mathrm{c.rés}}$-formule. Nos hypothèses entrainent que nous pouvons supposer que $\varphi_2$ et $\varphi_3$ sont aussi sans quantificateurs, ce qui donne le résultat.

**4.14. D'autres langages dans lesquels nous aurons l'élimination des quantificateurs**

Quand on regarde de près la preuve du Théorème 4.1, on s'aperçoit que l'application $\overline{\mathrm{ac}}$ est très peu utilisée, et qu'on pourrait très bien la remplacer par l'application résiduelle res . Cela est presque vrai : seule l'étape 0 pose probleème. En effet, alors que dans le langage de Pas, nous savons que le corps résiduel du corps des fractions de $A$ est nécéssairement contenu dans le corps des fractions de $k_A$, nous ne savons pas que c'est le cas dans le langage à 3 sortes classique. Une solution est alors d'ajouter $^{-1}$ au langage $\mathcal{L}_{\mathrm{c.val}}$, et tout s'arrange.

Un examen de la preuve montre aussi que l'on peut ajouter à $\mathcal{L}_{\mathrm{c.val}}$ des constantes pour obtenir un langage $\mathcal{L}'_{\mathrm{c.val}}$ à condition d'en ajouter suffisamment aussi aux langages $\mathcal{L}_{\mathrm{gp}}$ et $\mathcal{L}_{\mathrm{c.rés}}$ : il faut en effet que si $t(x)$ est un $\mathcal{L}'_{\mathrm{c.val}}$-terme, alors $v(t(x))$ est un $\mathcal{L}'_{\mathrm{gp}}$-terme et $\overline{\mathrm{ac}}(t(x))$ est un $\mathcal{L}'_{\mathrm{c.rés}}$-terme. Si ces contraintes sont satisfaites, le théorème 4.1 se généralise.

**4.15. Corollaire** (Principe d'Ax-Kochen-Ershov). Soient $(K, v)$ et $(L, w)$ des corps valués Henséliens de caractéristique résiduelle 0.

(1)
$$(K, v) \equiv (L, w) \iff [k_K \equiv k_L \text{ and } \Gamma_K \equiv \Gamma_L].$$

(2) Supposons que $(K, v) \subset (L, w)$. Alors
$$(K, v) \prec (L, w) \iff [k_K \prec k_L \text{ and } \Gamma_K \prec \Gamma_L].$$

*Démonstration.* Les deux assertions sont claires si l'on savait que les corps valués sont munis d'applications $\overline{\mathrm{ac}}$. Nous avons vu précédemment que tout corps valué muni d'une section peut être enrichi avec une application $\overline{\mathrm{ac}}$. Le résultat ci-dessous, Lemme 4.17, nous donne l'existence d'une section quand le corps valué est $\aleph_1$-saturé.

Pour le (1): Si $K \not\equiv L$, il en serait de même d'extensions élémentaires de $K$ et $L$. Soient $K^*$ et $L^*$ des extensions élémentaires de $K$ et $L$ respectivement, et qui sont $\aleph_1$-saturées. Leurs structures à 3 sortes associées peuvent donc être enrichies à des modèles de $T_0$. Le résultat suit maintenant par Théorème 4.1.

Pour le (2) le raisonnement est similaire. Soit $\mathcal{L}'_{\mathrm{Pas}}$ le langage obtenu en prenant $\mathcal{L}'_{\mathrm{c.val}} = \mathcal{L}_{\mathrm{c.val}}(K)$, $\mathcal{L}'_{\mathrm{gp}} = \mathcal{L}_{\mathrm{gp}}(\Gamma_K)$ et $\mathcal{L}'_{\mathrm{c.rés}} = \mathcal{L}_{\mathrm{c.rés}}(k_K)$. Ce langage satisfait les conditions énoncées

dans 4.14. De plus, $K \prec L$ (dans n'importe quel langage) si et seulement $L$ est modèle de la théorie de $K$ dans le langage auquel on a ajouté des constantes pour les éléments de $K$. En se plaçant dans ce langage étendu, nous obtenons donc le résultat.

**4.16. Corollaire** (Le fameux théorème d'Ax et Kochen, et Ershov). Soit $Q$ l'ensemble des nombres premiers, et $\mathcal{U}$ un ultrafiltre non-principal sur $Q$. Alors

$$\prod_{p\in Q} \mathbb{Q}_p/\mathcal{U} \equiv \prod_{p\in Q} \mathbb{F}_p((t))/\mathcal{U}.$$

*Démonstration.* Tous deux sont des corps valués Henséliens, de corps résiduel $\prod_{p\in Q} \mathbb{F}_p/\mathcal{U}$ (qui est de caractéristique nulle), et de groupe de valeurs $\mathbb{Z}^Q/\mathcal{U}$.

**4.17. Remarques**. La démonstration originale du théorème 4.15 utilise les sections, et montre un résultat analogue à celui que nous avons montré, mais dans le langage à 3 sortes auquel nous avons ajouté une fonction $s$ du groupe de valeurs dans le corps valué. Il n'est pas vrai que tous les corps valués aient une section, cependant on peut montrer que tous les corps valués $\aleph_1$-saturés en ont une. Cela provient en fait d'un résultat d'algèbre assez simple, qui ne parle que de groupes.

**Lemme**. Soit $G$ un groupe abélien, $H$ un sous-groupe de $G$, et supposons que la structure $(G, H)$ est $\aleph_1$-saturée (le groupe $G$, avec un prédicat unaire interprété par $H$), et que $G/H$ est sans torsion. Alors il existe un homomorphisme de groupes $s : G/H \to G$ tel que, si $\pi : G \to G/H$ dénote la projection canonique, alors $\pi \circ s = id$.

*Démonstration.* Voici une esquisse de la démonstration, qui est laissée en exercice. On prend une énumération $(a_\alpha)_{\alpha<\kappa}$ de $A = G/H$. Pour chaque $\alpha < \kappa$ on considère *l'enveloppe pure* $A_\alpha$ du sous-groupe $\langle a_\beta \mid \beta < \alpha\rangle$ de $G/H$ engendré par les $a_\beta$, pour $\beta < \alpha$ : c'est le plus petit sous-groupe de $A$ contenant $\langle a_\beta \mid \beta < \alpha\rangle$, et tel que si $b \in A$ et $n \in \mathbb{N}^{>0}$ sont tels que $nb \in \langle a_\beta \mid \beta < \alpha\rangle$, alors $b \in A_\alpha$. On a alors que $A/A_\alpha$ est sans torsion.

On construit le morphisme $s$ par induction sur les $A_\alpha$. Si $\alpha = 0$, alors $A_0 = (0)$, et nous n'avons rien à faire. Supposons que $s$ soit défini sur $A_\alpha$, nous allons l'étendre à $A_{\alpha+1}$. Si $a_\alpha \in A_\alpha$, nous n'avons rien à faire. Sinon, nous savons que $\langle A_\alpha, a_\alpha\rangle = A_\alpha \oplus \langle a_\alpha\rangle$, car aucun multiple non-nul de $a_\alpha$ n'est dans $A_\alpha$. Soit $S$ l'ensemble des entiers positifs $n$ tels que $A/\langle A_\alpha, a_\alpha\rangle$ contienne un élément d'ordre $n$. Si $n \in S$, il existera alors $b_n \in A$, $c_n \in A_\alpha$ et $j_n \in \mathbb{Z}$ tels que $nb_n = c_n + j_n a_\alpha$, et comme $A/A_\alpha$ n'a pas de torsion, $j_n$ sera premier à $n$. Changeant $b_n$ et $c_n$, on peut donc supposer que $j_n = 1$. De plus, si $m, n \in S$ alors leur ppcm sera aussi dans $S$.

On montre alors que $A_{\alpha+1} = \langle A_\alpha, b_n \mid n \in S\rangle$ (exercice).

Remarquons que si $n = dm$, alors $nb_n = c_n + (mb_m - c_m)$, ce qui entraîne que $c_n - c_m$ est divisible par $m$ dans $A$, et donc dans $A_\alpha$ (puisque $A/A_\alpha$ est sans torsion). Cela entraîne qu'il existe $c_{m,n} \in A_\alpha$ tel que $db_n = c_{m,n} + b_m$ $(*)$.

Nous avons déja construit $s$ sur $A_\alpha$, et nous voulons la définir sur $A_{\alpha+1}$. C'est-à-dire, nous voulons trouver des éléments $d_n \in G$, $n \in S$, tels que $\pi(d_n) = b_n$, et $nd_n = s(c_n) + j_n d_1$. Prenons des $e_n$, $n \in S$, dans $G$ tels que $\pi(e_n) = b_n$ pour tout $n \in S$. Pour trouver les $d_n$, il suffit donc de trouver des éléments $h_n \in H$, $n \in S$, tels que $n(e_n + h_n) = s(c_n) + (e_1 + h_1)$. Nous

avons donc un ensemble dénombrable de formules, ayant comme paramètres les $s(c_n)$ et $e_n$, et comme "variables" les $h_n$. Par $\aleph_1$-saturation de $(G, H)$, il suffit de montrer que cet ensemble de formules est finiment satisfaisable dans $H$. Soit $S_0$ un sous-ensemble finie de $S$. Puisque $S_0$ est fini, nous pouvons supposer qu'il contient un élément $n$ qui est divisible par tous les autres.

Prenons $h_n = 0$. Il nous faut trouver $h_m$ pour $m$ divisant $n$. Par l'équation $(*)$, si $n = md$, alors $db_n = c_{m,n} + b_m$. Donc, l'élément $h_m = de_n - e_m - s(c_{m,n})$ est dans $H$, et satisfait l'équation désirée.

**4.18. Les $\mathbb{Z}$-groupes ordonnés.** Avant de passer à l'étude de $\mathbb{Q}_p$, nous allons étudier les groupes ordonnés élémentairement équivalents à $\mathbb{Z}$. Ils sont appellés des $\mathbb{Z}$-groupes ordonnés, et satisfont les axiomes suivants :

Pres 1 $G$ est un groupe abélien sans torsion.

Pres 2 Si $n$ est un entier $> 1$, alors $[G : nG] = n$.

Pres 3 $G$ est un groupe ordonné, et a un plus petit élément positif, en général noté 1.

Les axiomes Pres 1 et Pres 2 axiomatisent la théorie du groupe $\mathbb{Z}$. Pressbürger a aussi montré que la théorie du groupe $\mathbb{Z}$ admet l'élimination des quantificateurs dans le langage $\{+, -, 0, \equiv_n |\ n \in \mathbb{N}^{>1}\}$, où $a \equiv_n b$ si et seulement s'il existe $c$ tel que $nc = (a - b)$. Ce résultat d'élimination des quantificateurs s'étend à la théorie du groupe ordonné $\mathbb{Z}$, en rajoutant au langage ci-dessus les symboles $<$ (la relation d'ordre) et 1 (le plus petit élément). Ce langage sera noté $\mathcal{L}_{\text{oPres}}$. La théorie de $\mathbb{Z}$ dans ce langage est obtenue en ajoutant aux axiomes de base les axiomes définissant les relations $\equiv_n$, et le fait que 1 est le plus petit élément positif. Notons que le fait que $[G : nG] = n$ s'exprime aussi de la façon suivante : $\forall x \bigvee_{i=0}^{n-1}(x \equiv_n i)$.

**4.19. Applications**. Quelles sont les théories de corps pour lesquels on a une élimination des quantificateurs dans un langage pas trop compliqué ? Evidemment la théorie des corps algébriquement clos dans le langage des anneaux. Mais aussi la théorie des corps réels clos dans le langage des anneaux ordonnés (un corps *réel clos* est un corps ordonné tel que tout élément positif a une racine carrée, et tout polynôme de degré impair a une racine).

On sait que la théorie des groupes ordonnés divisibles élimine les quantificateurs (cf Exercice 2.18). Cela nous donne donc : la $\mathcal{L}_{\text{Pas}}$-théorie des corps algébriquement clos de caractéristique résiduelle nulle élimine les quantificateurs. La discussion ci-dessus nous donne une autre théorie de groupe ordonné qui élimine les quantificateurs.

En mettant tout ensemble nous avons donc :

**Corollaire**. Soit $\mathcal{L}'_{\text{Pas}} = \mathcal{L}_{\text{c.val}} \cup \mathcal{L}'_{\text{gp}} \cup \mathcal{L}'_{\text{c.rés}} \cup \{v, \overline{\text{ac}}\}$. Les corps valués apparaissant dans la liste ci-dessous, ont une $\mathcal{L}'_{\text{Pas}}$-théorie qui élimine les quantificateurs dans $\mathcal{L}'_{\text{Pas}}$ :

(1) Le corps de séries généralisées $\mathbb{C}((\Gamma))$, $\Gamma$ un groupe ordonné divisible, $\mathcal{L}'_{\text{Pas}} = \mathcal{L}_{\text{Pas}}$ (cf. 1.29).

(2) Le corps de séries généralisées $\mathbb{R}((\Gamma))$, $\Gamma$ un groupe ordonné divisible, $\mathcal{L}'_{\text{gp}} = \mathcal{L}_{\text{gp}}$, $\mathcal{L}'_{\text{c.rés}} = \mathcal{L}_{\text{c.rés}} \cup \{<\}$.

(3) Le corps de séries $\mathbb{C}((t))$, $\mathcal{L}'_{\text{gp}} = \mathcal{L}_{\text{oPres}}$, $\mathcal{L}'_{\text{c.rés}} = \mathcal{L}_{\text{c.rés}}$.

(4) Le corps de séries formelles $\mathbb{R}((t))$, $\mathcal{L}'_{\text{gp}} = \mathcal{L}_{\text{oPres}}$, $\mathcal{L}'_{\text{c.rés}} = \mathcal{L}_{\text{c.rés}} \cup \{<\}$.

**4.20. Exercice**. Nous allons montrer que les corps de séries généralisées sont Henséliens, en montrant ... qu'ils n'ont pas d'extension immédiate propre du tout, et a fortiori, pas d'extension immédiate algébrique, ce qui nous permettra de conclure en utilisant 3.11. Soit $k$ un corps, $\Gamma$ un groupe abélien ordonné. Rappelons que le corps $K = k((\Gamma))$ est l'ensemble des sommes formelles de la forme

$$f = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma,$$

où les $a_\gamma \in k$, et le support de $f$, $\text{Supp}(f) = \{\gamma \in \Gamma \mid a_\gamma \neq 0\}$ est bien ordonné. Voir 1.29 pour plus de détails.

Pour chaque $\gamma \in \Gamma$ et $f$ comme ci-dessus, on définit *la troncation de $f$ à $\gamma$* par :

$$f|_\gamma = \sum_{\delta \leq \gamma} a_\delta t^\delta.$$

Supposons que $L = K(a)$ soit une extension immédiate de $K$, et soit $I = \{v(a-b) \mid b \in K\}$ le segment initial de $\Gamma \cup \{\infty\}$ qui lui est associé. Si $a \notin L$, nous savons que $I$ n'a pas de plus grand élément.

(1) Soit $\gamma \in I$, $b \in K$ tel que $v(a-b) > \gamma$. Vérifiez que $B(a;\gamma) = \{c \in K \mid c|_\gamma = b|_\gamma\}$. Déduisez-en qu'il existe un (unique) élément dans $B(a;\gamma)$ dont le support est contenu dans $(-\infty, \gamma]$.

(2) Montrez qu'il existe une suite $\gamma_\alpha$ indexée par des ordinaux $< \kappa$ pour un certain ordinal $\kappa$, qui est strictement croissante et cofinale dans $I \cap \Gamma$.

(3) A chaque $\alpha < \kappa$, nous associons un élément $f_\alpha$ dans la boule $B(a;\gamma_\alpha)$ tel que $\text{Supp}(f_\alpha) \subset (-\infty, \gamma_\alpha]$. Montrez que l'élément $f = \cup_{\alpha<\kappa} f_\alpha$ est bien un élément de $K$ (c'est-à-dire, il faut montrer que $\bigcup_{\alpha<\kappa} \text{Supp}(f_\alpha)$ est bien ordonné.)

(4) Déduisez-en que $\infty \in I$, et donc que $a \in K$.

# 5 Les corps $p$-adiques

Nous allons montrer dans cette section le résultat d'élimination des quantificateurs de Macintyre pour les corps $p$-adiques, dans le langage $\mathcal{L}_{\text{Mac}} = \{+, -, \cdot, 0, 1, \text{div}, P_n \mid n \in \mathbb{N}^{>1}\}$, où $P_n$ est un prédicat unaire, interprété par $P_n(x) \leftrightarrow \exists y\ y^n = x$. La preuve suivra les étapes de celle du théorème 4.1, avec quelques modifications.

Nous allons d'abord discuter des difficultés qui nous empêchent d'obtenir l'analogue de 4.1 quand la caractéristique résiduelle est $p > 0$. Nous avons donc un corps valué $K$, de corps résiduel $k$ de caractéristique $p > 0$, et de groupe de valeurs $\Gamma$ qui est un $\mathbb{Z}$-groupe ordonné, avec $v(p)$ un multiple entier de $1 = v(\pi)$. Nous nous plaçons dans le langage $\mathcal{L}_{\text{Pas}}$, et essayons de reproduire la preuve de 4.1. On voit, grâce aux résultats 3.27 et 3.30, que les étapes 1, 2, 3 et 6 ne posent pas de problèmes. Restent les étapes 4 et 5.

Pour l'étape 4 (augmenter le corps résiduel) : pas de problème si l'élément $\bar{a}$ qu'on veut rajouter est séparable sur le corps résiduel $k'_A$ de $A$ : on applique tout simplement la propriété de Hensel. Mais si $\bar{a}$ est purement inséparable sur $k'_A$ que fait-on? Par exemple, nous avons $\bar{a}^p = \text{res}\, b$, et nous voulons trouver un représentant de $\bar{a}$. Il est clair que parmi les éléments qui ont pour image résiduelle $\text{res}\, b$, certains n'auront pas de racine $p$-ième : si $a_1 = a_2 + \pi u$, où $v(u) \geq 0$, alors $a_1^p = (a_2 + \pi u)^p$, et en développant on obtient que $v(a_1^p - a_2^p) \geq v(p) + 1$. Il faut donc distinguer entre ceux qui ont une racine $p$-ième, et les autres.

Ce problème provient du fait que, bien que l'on ait

$$\exists y\ y^p = x \rightarrow (\exists y \in k_K\ y^p = \overline{\text{ac}}(x) \wedge \exists \xi\ p\xi = v(x)),$$

la réciproque est fausse. C'est à dire : les prédicats $P_n$, bien que définissables, ne sont pas définissables sans quantificateurs dans un langage de type $\mathcal{L}'_{\text{Pas}}$. Pour pallier à ce problème, on peut par exemple rajouter à $\mathcal{L}_{\text{Pas}}$ une suite $(\overline{\text{ac}}_n)_{n\geq 1}$ de fonctions, avec $\overline{\text{ac}}_1 = \overline{\text{ac}}$, et $\overline{\text{ac}}_n : K \rightarrow \mathcal{O}/\pi^n\mathcal{O}$ une fonction qui vaut 0 en 0, est multiplicative sur $K^\times$, et coïncide avec la projection naturelle $\mathcal{O} \rightarrow \mathcal{O}/\pi^n\mathcal{O}$ sur les éléments de valuation 0.

Les problèmes pour l'étape 5 sont similaires, mais en fait cette adjonction des $\overline{\text{ac}}_n$ suffit à résoudre le problème dans ce cas aussi. Voir L. Bélair, *Types dans les corps valués munis d'applications coefficients*, Illinois J. of Math. 43 (1999), Nr 2, 410 – 425.

Ou alors, tout simplement, rajouter les prédicats $P_n$ de Macintyre. On s'aperçoit alors, dans le cas des $p$-adiques, que ces prédicats nous disent aussi si $v(x)$ est divisible par $n$ dans le groupe de valeurs. Donc, dans le cas de $\mathbb{Q}_p$, en passant au langage $\mathcal{L}_{\text{div}}$ agrandi par les $P_n$, on a, sur le groupe de valeurs, tout ce qu'il faut pour l'élimination des quantificateurs.

**5.1. Théorème**. Soit $T$ la théorie de $\mathcal{L}_{\text{Mac}}$ dont les modèles sont des corps valués Henséliens de caractéristique 0, ayant corps résiduel isomorphe à $\mathbb{F}_p$, et avec $v(p)$ le plus petit élément positif du groupe de valeurs. De plus, les éléments satisfaisant $P_n$ sont exactement les éléments non nuls ayant une racine $n$-ième, et le groupe de valeurs est un $\mathbb{Z}$-groupe ordonné.

Alors $T$ est complète et élimine les quantificateurs.

*Démonstration.* Tout d'abord il est clair que ces propriétés sont exprimables dans le langage $\mathcal{L}_{\text{Mac}}$ : nous avons vu dans le chapitre 1 que dans la $\mathcal{L}_{\text{div}}$-structure associée à un corps valué,

on pouvait réinterpréter la structure à 3 sortes associée à ce corps valué. Nous avions aussi vu qu'un $\mathcal{L}_{\mathrm{div}}$-isomorphisme entre des anneaux produisait un isomorphisme de corps valués en passant au corps des fractions.

Observons que $v(p)$ est le plus petit élément positif du groupe de valeurs, se dit : $1 \operatorname{div} p$, $\neg(p \operatorname{div} 1)$, et $\forall x\ [1 \operatorname{div} x \wedge \neg(x \operatorname{div} 1) \to p \operatorname{div} x]$.

Nous prenons donc deux modèles $\aleph_1$-saturés de $T$, $K$ et $L$. Nous allons montrer que si $f : A \to B$ est un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme entre des sous-anneaux dénombrables $A$ et $B$ de $K$ et $L$ respectivement, et si $C$ est une sous-structure élémentaire dénombrable de $K$ contenant $A$, alors il existe $g$ qui prolonge $f$, et définit un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme de $C$ dans une sous-structure de $L$.

Soient $f : A \to B$ et $C$ comme ci-dessus. Nous allons étendre $f$ à $C$, en s'inspirant de la preuve de 4.3.

**Etape 0**.

Nous avons déjà vu que $f$ se prolonge uniquement à un $\mathcal{L}_{\mathrm{div}}$-isomorphisme entre les corps de fractions de $A$ et de $B$. Comme nous avons

$$P_n(ab^{-1}) \iff P_n(ab^{n-1}),$$

ce prolongement unique est un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme.

Nous pourrons donc toujours supposer que $A$ et $B$ sont des corps.

**Etapes 1, 2 et 4**. Rien à faire, car les corps résiduels de $A$ et $B$ sont $\mathbb{F}_p$.

**Etape 3**. Prolongement de $f$ à $A^h$.

Comme dans la preuve de 4.3, nous savons que $f$ se prolonge à un $\mathcal{L}_{\mathrm{div}}$-isomorphisme $f_1$ entre les hensélianisées $A^h \to B^h$. Il faut cependant vérifier que $f_1$ respecte les prédicats $P_n$. Cela découle du Lemme suivant, qui nous servira aussi pour l'étape 6 :

**5.2. Lemme**. Soit $F$ un corps valué Hensélien, de caractéristique résiduelle $p > 0$, et satisfaisant que $v(p)$ est un multiple entier du plus petit élément positif du groupe de valeurs $\Gamma$. Soit $E$ un sous-corps de $F$, et supposons que $a \in F$ soit tel que $E(a)$ est une extension immédiate de $E$. Si $\gamma = v(a) + 2v(n)$, alors

$$F \models \exists y\ y^n = a \iff \text{pour tout } b \in B(a;\gamma) \cap E(a),\ F \models \exists y\ y^n = b.$$

*Démonstration.* Alors $b \in B(a;\gamma) \cap E(a)$ si et seulement si $v(ab^{-1} - 1) > 2v(n)$. Par 3.28(1), nous savons que $v(u') > 2v(n)$ implique $1 + u'$ a une racine $n$-ième dans $F$. C'est-à-dire : si $b \in B(a;\gamma)$ alors $ab^{-1}$ a une racine $n$-ième dans $F$. Cela donne le résultat. □

Nous allons maintenant nous occuper du groupe de valeurs. Le fait d'être obligé de préserver les $P_n$ complique un peu les choses, et nous serons obligés de prolonger $f$ à des sous-corps de $C$ qui ne sont pas finiment engendrés au-dessus de $A$. Nous remarquons que le fait que $f$ est un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme entraîne que l'isomorphisme induit sur les groupes de valeurs préserve les prédicats $\equiv_n$ : en effet, $P_n(a)$ entraine que $v(a) \equiv_n 0$. Comme dans l'étape 2 de 4.1, nous pouvons donc prolonger $f : \Gamma_A \to \Gamma_B$ à un plongement $\tilde{f} : \Gamma_C \to \Gamma_L$, qui respecte les prédicats

$\equiv_n$, $n \in \mathbb{N}^{>1}$. Nous fixons un tel $\tilde{f}$. Nous allons prolonger $f$ de telle façon que l'isomorphisme induit sur les groupes de valeurs coïncide avec $\tilde{f}$. Notons que $\tilde{f}$ est uniquement déterminée sur le groupe de valeurs de $A^{alg} \cap C$, car chaque élément de ce groupe a un multiple non nul dans $\Gamma_A$.

Nous pouvons écrire $C$ comme l'union d'une chaîne croissante de sous-corps $(C_n)_{n\in\mathbb{N}}$, et satisfaisant : $C_n^{alg} \cap C = C_n$ ; $tr.deg(C_{n+1}/C_n) = 1$ ; $C_0 = A^{alg} \cap C$. Il suffit donc de prolonger $f$ à chacun des $C_n$.

Pour cela, nous allons nous servir d'une propriété des modèles $\aleph_1$-saturés, qui nous permet de nous ramener au cas d'extensions de type fini :

**Fait**. Soit $E$ un sous-corps de $C$ contenant $A$. Si pour tout $n$ et $a_1, \ldots, a_n \in E$, il existe un plongement du corps valué $A(a_1, \ldots, a_n)$ dans $L$ qui prolonge $f$, alors il existe un plongement du corps valué $E$ dans $L$ qui prolonge $f$.

La preuve de ce fait est esquissée dans 5.4 ci-dessous.

**Assertion**. Si $E \subset C$ satisfait $E^{alg} \cap C = E$, alors tout isomorphisme $g$ du corps valué $E$ dans un sous-corps de $L$ qui induit $\tilde{f}$ sur $\Gamma_E$, respecte les prédicats $P_n$.

*Démonstration.* Si $a \in E$ satisfait $P_n$, alors la racine $n$-ième de $a$ est dans $E$, et donc $L \models P_n(g(a))$. Supposons maintenant que $g(a)$ satisfasse $P_n$ dans $L$. Notons que $\Gamma_K/\Gamma_E$ est sans torsion (comme $C \prec K$, nous avons aussi $E^{alg} \cap K = E$). Comme l'application induite par $g$ sur les groupes de valeurs respecte les $\equiv_n$ (puisqu'elle coïncide avec $\tilde{f}$), nous aurons aussi que $\Gamma_L/\Gamma_{g(E)}$ est sans torsion. On sait que $g(E)$ est Hensélien. D'après 3.27, il n'a pas d'extension immédiate algébrique propre, et comme son corps résiduel est le même que celui de $L$, cela entraîne que toute extension algébrique propre finie de $g(E)$ est totalement ramifiée. Si la racine $n$-ième de $g(a)$ n'est pas dans $g(E)$, elle engendre donc une extension totalement ramifiée de $g(E)$. C'est a dire, il existe un entier $e$ tel que $e$ divise $v(g(a))$ dans $\Gamma_L$ mais pas dans $\Gamma_{g(E)}$. Cela contredit le fait que $\Gamma_L/\Gamma_{g(E)}$ est sans torsion.

*Prolongement de $f$ à $C_0$.*

Soit $E \subset C_0$ un sous-corps qui est finiment engendré sur $A$. Alors, par 3.27, nous savons que $E/A$ est totalement ramifiée, c'est-à-dire, $[\Gamma_E : \Gamma_A] = [E : A]$. D'autre part le groupe $\Gamma_E/\Gamma_A$ est un groupe abélien fini, donc une somme directe de groupes cycliques. Choisissons $\gamma_1, \ldots, \gamma_m \in \Gamma_E$ tels que $\Gamma_E/\Gamma_A = \langle \gamma_1 + \Gamma_A \rangle \oplus \cdots \oplus \langle \gamma_m + \Gamma_A \rangle$, et pour chaque $i$ soit $n_i$ l'ordre de $\gamma_i + \Gamma_A$ dans $\Gamma_E/\Gamma_A$. Par 3.28, pour chaque $i$, il existe $a_i \in E$ tel que $v(a_i) = \gamma_i$, et $a_i^{n_i} \in A$. De plus, $E = A(a_1, \ldots, a_m)$. Comme $f$ préserve les $P_n$, on a que $L \models P_{n_i}(f(a^{n_i}))$ pour tout $i$, et donc il existe $b_1, \ldots, b_m \in L$ tels que $b_i^{n_i} = f(a^{n_i})$ pour $i = 1, \ldots, m$. L'isomorphisme $f_1$ qui prolonge $f$ et envoie $a_i$ sur $b_i$, est alors un isomorphisme de corps valués $E \to B(b_1, \ldots, b_m)$, car ces deux extensions sont des extensions totalement ramifiées, et l'isomorphisme de corps respectera la valuation (cf. Remarque 3.7).

En utilisant le fait et l'assertion, nous avons donc montré que $f$ se prolonge à $C_0$, en un $\mathcal{L}_{\text{Mac}}$-isomorphisme. Supposons que nous ayions étendu $f$ à $C_n$. Deux cas sont possibles : ou bien $\Gamma_{C_{n+1}} = \Gamma_{C_n}$, ce qui entrainera que $C_{n+1}$ est une extension immédiate de $C_n$ ; ou bien $\Gamma_{C_{n+1}} \neq \Gamma_{C_n}$. Nous allons d'abord traiter le deuxième cas.

*Prolongement de $f$ à $C_{n+1}$ quand $\Gamma_{C_{n+1}} \neq \Gamma_{C_n}$.*

Si $E$ est un sous-corps de $C_{n+1}$ qui est finiment engendré au-dessus de $C_n$, alors $\Gamma_E/\Gamma_{C_n}$ est finiment engendré, et sans torsion. De plus, comme $tr.deg(E/C_n) = 1$, cela entraine que $\Gamma_E/\Gamma_{C_n} \simeq \mathbb{Z}$. Nous pouvons donc trouver $\gamma \in E$ tel que $\Gamma_E = \Gamma_{C_n} \oplus \langle\gamma\rangle$. Soit $a \in E$ tel que $v(a) = \gamma$ et soit $b \in L$ tel que $w(b) = \tilde{f}(\gamma)$. Alors, si $g : C_n(a) \to f(C_n)(b)$ est l'isomorphisme qui prolonge $f$ et envoie $a$ sur $b$, c'est un isomorphisme de corps valués : on sait que si $c_0, \ldots, c_m \in C_n$, alors $v(\sum_i c_i a^i) = \min_i\{v(c_i) + i\gamma\}$, et si ce minimum est atteint pour $j$, alors on aura $w(\sum_i f(c_i)b^i) = w(f(c_j)) + j\tilde{f}(\gamma)$.

Nous avons donc montré que $f$ se prolonge à $C_n(a)$. Comme $E$ est une extension immédiate (algébrique) de $C_n(a)$, et que $L$ est Hensélien, nous pouvons prolonger à tout $E$.

L'assertion nous dit que $f$ se prolonge à $C_{n+1}$.

*Prolongement de $f$ à $C_{n+1}$ quand $C_{n+1}$ est une extension immédiate de $C_n$.*

Soit $a \in C_{n+1}$, $a \notin C_n$. Nous reproduisons le raisonnement de l'étape 6 de 4.1 pour trouver $b \in L$ tel que, pour tout $c \in C_n$,

$$w(b - f(c)) = f(v(a - c)).$$

Prolongeant $f$ à $C_n(a)$ en posant $f_1(a) = b$, nous donne donc un isomorphisme de corps valués. Nous savons que $C_{n+1}$ est une extension immédiate algébrique de $C_n$, qui est Hensélienne car relativement algébriquement close dans le corps Hensélien $C$. D'après le Théorème 3.27, $C_{n+1}$ est donc la Hensélianisée de $C_n(a)$ ; comme $L$ est Hensélien, cet isomorphisme $f_1$ se prolonge alors à un isomorphisme de domaine $C_{n+1}$ et d'image contenue dans $L$.

## 5.1 Un résultat sur les modèles saturés

**5.3. Rappels sur les types**. Soient $T$ une théorie dans un langage $\mathcal{L}$, $M$ un modèle de $T$, et $A$ un sous-ensemble de $M$. Un *$m$-type partiel sur $A$* est un ensemble $\Sigma(\bar{x})$ de $\mathcal{L}(A)$-formules en $\bar{x}$, $\bar{x}$ étant un $m$-uplet de variables, qui est finiment satisfaisable dans $M$. Si $\Sigma(\bar{x})$ a la propriété que pour toute $\mathcal{L}(A)$-formule $\varphi(\bar{x})$ il existe une conjonction finie $\psi(\bar{x})$ de formules de $\Sigma(\bar{x})$ telle que $T \vdash \forall\bar{x}\ \psi(\bar{x}) \to \varphi(\bar{x})$ ou bien $T \vdash \forall\bar{x}\ \psi(\bar{x}) \to \neg\varphi(\bar{x})$, alors $\Sigma(\bar{x})$ est *un type complet*. Un type complet qui est clos par déductions sera donc un type maximal consistent : si $\psi(\bar{x}) \in \Sigma(\bar{x})$ alors ou bien $\psi(\bar{x}) \in \Sigma(\bar{x})$, ou bien $\neg\psi(\bar{x}) \in \Sigma(\bar{x})$. On montre facilement que tout type est contenu dans un type complet [On associe au type $\Sigma(\bar{x})$ une théorie $T(A, \bar{c})$ dans le langage $\mathcal{L}(A)_\cup\{\bar{c}\}$, $\bar{c}$ un $m$-uplet de nouvelles constantes, on prend une complétion de cette théorie, puis on regarde le type complet correspondant.]

**Exemples de types**. Soient $M$ un modèle de $T$, $A \subset M$ et $a$ un $m$-uplet d'éléments de $M$, $\bar{x}$ un $m$-uplet de variables. Alors $tp(a/A) =_{\text{def}} \{\varphi(\bar{x}) \mid \varphi(\bar{x}) \in \mathcal{L}(A),\ M \models \varphi(a)\}$ est un type complet, appellé le *type de $a$ sur $A$*.

La définition de la saturation peut être exprimée de la façon suivante : $M$ est $\kappa$-saturé si pour tout sous-ensemble $A$ de $M$ de cardinalité $< \kappa$, tout 1-type sur $A$ est réalisé dans $M$. L'exercice suivant montre que l'on peut remplacer 1-type par $n$-type, ou même par $\lambda$-type, pour $\lambda < \kappa$.

**5.4. Exercice**. Soit $\kappa$ un cardinal infini, et $M$ un modèle $\kappa$-saturé d'une $\mathcal{L}$-théorie complète $T$.

(1) Montrez que si $A$ est un sous-ensemble de $M$ de cardinalité $< \kappa$, et $m \in \mathbb{N}$, alors tout $m$-type sur $A$ est réalisé dans $M$. [Il suffit de le montrer pour les types complets. On remarque que si $\bar{x} = (x_1, \ldots, x_m)$ et $\psi(\bar{x}) \in \Sigma(\bar{x})$, alors $\exists x_2, \ldots, x_m\ \psi(\bar{x}) \in \Sigma(\bar{x})$ et a pour seule variable libre $x_1$.]

(2) Soient $\bar{x}$ un uplet de variables de longueur $\lambda < \kappa$, $A$ un sous-ensemble de $M$ de cardinalité $< \kappa$ et $\Sigma(\bar{x})$ un ensemble de $\mathcal{L}(A)$-formules en $\bar{x}$ qui est finiment satisfaisable dans $M$. Montrez que $\Sigma(\bar{x})$ est réalisé dans $M$.

## 5.2 Etude des extensions finies de $\mathbb{Q}_p$

**5.5.** Nous allons maintenant nous intéresser aux extensions algébriques finies de $\mathbb{Q}_p$. Soit $E$ une telle extension, de degré $n$ sur $\mathbb{Q}_p$. Alors nous savons que $n = ef$, où $e = v(p)$ (1 dénotant le plus petit élément positif de $\Gamma_E$), et $k_E = \mathbb{F}_q$ avec $q = p^f$. En effet, comme $E$ est Hensélien, on trouve un sous-corps $E'$ de $E$ de degré $ef$ sur $\mathbb{Q}_p$, ayant même groupe de valeurs et corps résiduel que $E$. Alors $E$ est une extension immédiate du corps Hensélien $E'$, et par le théorème 3.27, $E' = E$. Plus précisément, soit $\alpha \in \mathbb{F}_p^{alg}$ tel que $\mathbb{F}_p(\alpha) = \mathbb{F}_q$, et soit $\bar{Q}(T) \in \mathbb{F}_p(T)$ son polynôme minimal (unitaire), et $Q(T) \in \mathbb{Z}[T]$ un polynôme unitaire de même degré tel que $\mathrm{res}\,(Q)(T) = \bar{Q}(T)$. Puisque $E$ est Hensélien, il existe $\zeta \in \mathcal{O}_E$ tel que $\mathrm{res}\,(\zeta) = \alpha$ et $Q(\zeta) = 0$. Maintenant, par le Lemme 3.28, il existe $\pi \in E$ tel que $\pi^e \in \mathbb{Q}_p(\zeta)$ et $ev(\pi) = v(p)$. Alors $v(\pi)$ est le plus petit élément de $\Gamma_E$, et par 3.27, $E = \mathbb{Q}_p(\zeta, \pi)$. Soit $P(X, Y) \in \mathbb{Z}[X, Y]$ un polynôme irréductible qui s'annule sur $(\zeta, \pi)$. Alors $P$ est de degré $e$ en $Y$.

Nous considérons maintenant la théorie $T$ dans le langage $\mathcal{L}_{\mathrm{Mac}} \cup \{c_1, c_2\}$ dont les modèles sont les corps valués $(K, \mathrm{div}\,)$ satisfaisant :
$K$ est Hensélien de caractéristique 0 ; son corps résiduel a $q$ éléments, et $c_1$ satisfait $Q(T) = 0$; $v(c_2)$ est le plus petit élément du groupe de valeurs de $K$, et ce groupe de valeurs est un $\mathbb{Z}$-groupe (ordonné) ; nous avons $v(p) = ev(c_2)$ et $P(c_1, c_2) = 0$ ; les $P_n$ définissent les puissances $n$-ièmes.

**Théorème**. La théorie $T$ décrite ci-dessus est complète et élimine les quantificateurs.

*Démonstration.* La démonstration de l'élimination des quantificateurs est identique à celle du théorème 5.1. Pour montrer que $T$ est complète, il faut montrer que si $K$ et $L$ sont des modèles de $T$, alors leurs sous-structures engendrées par les constantes sont isomorphes.

Nous dénoterons les interprétations des constantes $c_1$ et $c_2$ dans $K$ par $\zeta_K$ et $\pi_K$, et dans $L$ par $\zeta_L$ et $\pi_L$. Nos hypothèses sur la théorie $T$ entrainent que $\zeta_K, \pi_K$ et $\zeta_L, \pi_L$ engendrent des sous-corps valués $A$ et $B$ de $K$ et $L$ respectivement, qui sont isomorphes. En effet, les extensions $\mathbb{Q}(\zeta_K)$ et $\mathbb{Q}(\zeta_L)$ sont purement inertielles, et les extension $A/\mathbb{Q}(\zeta_K)$ et $B/\mathbb{Q}(\zeta_L)$ sont totalement ramifiées. Nous appelons $f$ l'isomorphisme de $A$ dans $B$ qui envoie $\zeta_K$ sur $\zeta_L$ et $\pi_K$ sur $\pi_L$.

Nous pouvons étendre $f$ à un isomorphisme $A^h \to B^h$. Nous savons que $k_K = \mathbb{F}_q = k_A$ et que $\Gamma_A$ est *pur* dans $\Gamma_K$, c'est-à-dire que $\Gamma_K/\Gamma_A$ est sans torsion. Cela implique, par 3.27,

que $A^h = K \cap A^{alg}$ ; le même raisonnement donne que $B^h = L \cap B^{alg}$. Cela entraine alors que l'isomorphisme $f$ respecte les $P_n$: en effet, on a

$$K \models P_n(a) \iff A^h \text{ contient une racine } n\text{-ième de } a,$$

et pareillement pour $L$ et $f(a)$.

**5.6. Remarque**. Malheureusement, on ne peut se passer des constantes, même quand $v(p) = 1$ est le plus petit élément positif du groupe de valeurs. Voici un contre-exemple dans le cas $v(p) = 1$, $q = p^2$, et $n = q - 1$. On suppose notre corps $K$ muni d'une section $s$ du groupe de valeurs, on prend $\alpha \in \Gamma_K$ divisible par $n$ (dans $\Gamma_K$), $\alpha \notin \mathbb{Z}$ et $a = s(\alpha)c$, où $c \in K$ est tel que $v(c) = 0$, $\operatorname{res} c \notin \mathbb{F}_p$, et on considère $A = \mathbb{Q}(a)$. Dans $K$ nous avons $P_n(s(\alpha))$, mais comme 1 est le seul élément de $\mathbb{F}_q$ qui soit une puissance $n$-ième, tous les éléments de $K$ de valuation $\alpha$ qui sont dans $P_n$ satisfont $v(x - s(\alpha)) > \alpha$. En particulier, $\mathbb{Q}(a)$ ne contient aucun élément de $P_n$ de valuation $\alpha$. C'est à dire, la $\mathcal{L}_{\text{Mac}}$-structure $\mathbb{Q}(a)$ ne nous dit pas que $\alpha$ est divisible par $n$.

**5.7.** Ces théorèmes ont des conséquences nombreuses. Par exemple, on voit tout de suite que si $T$ est la théorie décrite ci-dessus, si $K$ est un modèle de $T$, et si $E^{alg} \cap K = E$, alors $E$ est un modèle de $T$, et de plus est une sous-structure élémentaire de $K$. En effet, $E$ est un corps Hensélien modèle de $T$.

En fait on peut montrer des résultats plus forts. Soit $K$ comme ci-dessus. On sait que pour tout entier $n$, $K$ a un nombre fini d'extensions de degré $n$. Cela entraîne que $K^{alg} = K\mathbb{Q}^{alg}$. En effet, nous savons que $\mathbb{Q}^{alg} \cap K$ est une sous-structure élémentaire de $K$, et que pour tout $n$, $\mathbb{Q}^{alg} \cap K$ et $K$ ont le même nombre d'extensions algébriques de degré $n$. Cela entraine que les extension algébriques de $K$ sont contenues dans $K\mathbb{Q}^{alg}$.

Soient $\zeta$ et $\pi \in K$ définis par : $\zeta$ est une racine primitive $(p^f - 1)$-ième de l'unité, et $P(\zeta, \pi) = 0$. Nous savons que $v(\pi)$ est le plus petit élément positif de $\Gamma_K$. De plus ons s'aperçoit que $\mathcal{O}_K$ est définissable dans le langage des corps : si $p > 2$, on a $x \in \mathcal{O}_K$ si et seulement si $1 + \pi x^2$ a une racine carrée ; si $p = 2$, $x \in \mathcal{O}_K$ si et seulement si $1 + \pi x^3$ a une racine cubique. Nous avons donc montré que la théorie de $K$ dans le langages des anneaux est *modèle-complète*, c'est-à-dire, si $E \subset F$ sont des modèles de cette théorie, alors $E \prec F$. En effet, par ce que nous avons vu ci-dessus, la valuation est définissable. Comme d'autre part, $E \cap \mathbb{Q}^{alg} = F \cap \mathbb{Q}^{alg}$, et $E\mathbb{Q}^{alg} = E^{alg}$, $F\mathbb{Q}^{alg} = F^{alg}$, nous avons que $E^{alg} \cap F = E$.

Vous connaissez sans doute le résultat d'Artin qui dit que si $K$ est un corps tel que $\mathcal{G}al(K^{alg}/K) \simeq \mathbb{Z}/2\mathbb{Z}$, alors $K$ est un corps réel clos. Un résultat analogue a été montré par J. Koenisgmann : soit $K$ un corps, et supposons que $\mathcal{G}al(K^{alg}/K) \simeq \mathcal{G}al(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$. Alors $K \equiv \mathbb{Q}_p$. En particulier, $K$ est de caractéristique 0.

## 5.3 Ajout d'un prédicat pour des représentants de Teichmüller

L'extension maximale algébrique non ramifiée de $\mathbb{Q}_p$ est obtenue en ajoutant à $\mathbb{Q}_p$ toutes les racines primitives de l'unité d'ordre premier à $p$. Cette extension est importante pour les théoriciens des nombres. Notons $K$ cette extension. Si $S$ est un sous-groupe multiplicatif de $K$ qui est tel que l'application res définisse un homomorphisme de groupe $S \to \mathbb{F}_p^{alg\,\times}$, alors $S$ est appelé un système de *représentants de Teichmüller*. En fait $S$ est unique, comme nous verrons ci-dessous. Van den Dries a étudié la théorie des modèles de ce corps muni d'un prédicat pour les représentants de Teichmüller. Les références pour cette sous-section sont

[vdD] L. van den Dries, On the elementary theory of rings of Witt vectors with a multiplicative set of representatives for the residue field, Manuscripta Math. 98, 133-137 (1999).

[S] J. P. Serre, *Corps locaux*, Paris, Hermann, 1962.

**5.8. Proposition**. Soit $A$ un anneau complet pour la topologie $I$-adique, où $I$ est un idéal radical de $A$, tel que $\bigcap_n I^n = (0)$. On suppose que $k = A/I$ est un anneau parfait de caractéristique $p > 0$ (*parfait* voulant dire, comme pour les corps, que tout élément est une puissance $p$-ième). Soit $\pi : A \to k$ l'application naturelle.

(1) Il existe une unique section $f : k \to A$ qui satisfasse $f(x^p) = f(x)^p$ pour tout $x \in k$.

(2) Un élément de $A$ est dans l'image de $f$ si et seulement s'il est une puissance $p^n$-ième pour tout $n > 0$.

(3) $f$ est multiplicative.

(4) Si la caractéristique de $A$ est $p$, alors $f$ est aussi additive.

*Démonstration.* Soit $\alpha \in k$. On considère $U_n = \pi^{-1}(\alpha) \cap A^{p^n}$, où $A^{p^n}$ dénote $\{a^{p^n} \mid a \in A\}$. Comme $k$ est parfait, chaque $U_n$ est non vide : en effet, si $\pi(a) = \alpha^{1/p^n}$ alors $a^{p^n} \in U_n$. Les $U_n$ forment une suite décroissante. Nous allons montrer que leur intersection est réduite à un point. Pour cela, on montre d'abord que si $a - b \in I^n$, alors $a^p - b^p \in I^{n+1}$ : soit $c = a - b$, alors $b^p - a^p = pca^{p-1} + \sum_{i=2}^{p} \binom{p}{i} c^i a^{p-i}$ ; si $c \in I^n$, alors le deuxième terme est dans $I^{2n} \supset I^{n+1}$, et le premier dans $I^{n+1}$ car $p \in I$. Cela entraine, par induction sur $n$, que si $a - b \in I$, alors $a^{p^n} - b^{p^n} \in I^{n+1}$.

Supposons que $a, b \in U_n$, et écrivons-les $a = x^{p^n}$ et $b = y^{p^n}$. Comme $k$ n'a pas d'éléments nilpotents (puisque $I$ est radical), l'égalité $0 = \pi(a - b) = \pi(x - y)^{p^n}$ entraîne que $x - y \in I$, d'où $a - b \in I^{n+1}$.

Ceci montre que $\bigcap_n U_n$ contient au plus un point ; comme $A$ est complet pour la topologie $I$-adique, il en contient un. Nous définissons $f(\alpha)$ comme cet unique élément. On vérifie alors facilement que $f(\alpha^p) = f(\alpha)^p$.

Remarquons maintenant que comme $f$ commute avec l'application $x \mapsto x^p$, et que $k$ est parfait, et donc clos par l'application $x \mapsto x^{1/p}$, nécéssairement un élément de $f(k)$ sera dans $\bigcap_n A^{p^n}$. Cela montre 2, et 1. Pour 3, il suffit d'utiliser 2, et de remarquer que si $a$ et $b$ sont

des puissances $p^n$-ièmes pour tout $n$, alors aussi $ab$ ; de plus, si $A$ est de caractéristique $p$, alors $a+b$ sera aussi une puissance $p^n$-ième pour tout $n$, ce qui montre 4.

**5.9.** Soit $A$ un anneau comme ci-dessus, avec $I = pA$, et soit $f : k \to A$. Alors tout élément de $A$ peut s'écrire (uniquement) de la forme $\sum_{i=0}^{\infty} f(\alpha_i)p^i$. Le résultat suivant, prouvé dans le livre de Serre, nous dit comment calculer les sommes et produits :

**5.10. Théorème** Il existe des polynômes $P_i(X_0, \ldots, X_i, Y_0, \ldots, Y_i), Q_i(X_0, \ldots, X_i, Y_0, \ldots, Y_i) \in \mathbb{F}_p[X_0, \ldots, X_i, Y_0, \ldots, Y_i]$ tels que, si $A$ est un anneau comme ci-dessus, avec $I = pA$, et si $(\alpha_i), (\beta_i) \in k$, alors

$$\begin{aligned} \sum_{i=0}^{\infty} f(\alpha_i)p^i + \sum_{i=0}^{\infty} f(\beta_i)p^i &= \sum_{i=0}^{\infty} \gamma_i p^i, \\ \sum_{i=0}^{\infty} f(\alpha_i)p^i \times \sum_{i=0}^{\infty} f(\beta_i)p^i &= \sum_{i=0}^{\infty} \delta_i p^i, \end{aligned}$$

où $\gamma_i = P_i(\alpha_0^{p^i}, \ldots, \alpha_i^{p^i}, \beta_0^{p^i}, \ldots, \beta_i^{p^i})$ et $\delta_i = Q_i(\alpha_0^{p^i}, \ldots, \alpha_i^{p^i}, \beta_0^{p^i}, \ldots, \beta_i^{p^i})$.

**5.11. Corollaire**. Soient $n$ un entier positif et $\ell \in \mathbb{Z}^n$. Il existe des polynômes $R_0(X), \ldots, R_N(X) \in \mathbb{F}_p[X]$, $X = (X_1, \ldots, X_n)$ tels que, si $A$ est comme ci-dessus, alors pour tout $\alpha \in k^n$,

$$\ell \cdot f(\alpha) = 0 \iff R_0(\alpha) = \cdots = R_N(\alpha) = 0.$$

[Ici, $\ell \cdot f(\alpha)$ dénote le produit vectoriel du $n$-uplet $\ell$ avec le $n$-uplet $f(\alpha)$.]

*Démonstration.* Une application du résultat précédent nous donne des polynômes $R_i(X) \in \mathbb{F}_p[X]$ tels que, pour tout $A$ et $\alpha \in k^n$, nous ayions

$$\ell \cdot f(\alpha) = \sum_{i=0}^{\infty} R_i(\alpha^{p^i})p^i.$$

Alors $\ell \cdot f(\alpha) = 0 \iff R_i(\alpha^{p^i}) = 0$ pour tout $i$ ; comme $R_i$ a ses coefficients dans $\mathbb{F}_p$, $R_i(\alpha^{p^i}) = 0 \iff R_i(\alpha) = 0$ ; comme $\mathbb{F}_p[X]$ est Noethérien, l'idéal engendré par tous les $R_i$ est finiment engendré, c'est-à-dire, il existe $N$ tel que pour tout $x$, $R_0(x) = \cdots = R_N(x) = 0$ implique $R_i(x) = 0$ pour tout $i$.

**5.12. Lemme**. Soient $U$ et $V$ des sous-groupes multiplicatifs des corps de caractéristique 0 $E$ et $F$, et $f : U \to V$ un isomorphisme. Supposons que pour tout $n$ et $n$-uplet $\ell \in \mathbb{Z}^n$, $n$-uplet $x \in U^n$, nous ayions

$$\ell \cdot x = 0 \iff \ell \cdot f(x) = 0.$$

Alors $f$ se prolonge à un isomorphisme de corps $\mathbb{Q}(U) \to \mathbb{Q}(V)$.

**5.13. Lemme**. Soit $(K, v)$ un corps valué Hensélien de catactéristique résiduelle nulle, et soit $K_0$ un sous-corps de $\mathcal{O}_v$, maximal pour la propriété $K_0 \cap \mathcal{M}_v = (0)$. Alors $\mathrm{res}\,(K_0) = k_v$.

*Démonstration.* Soit $k_0 = \mathrm{res}\,(K_0)$, et supposons que $\alpha \in k_v \setminus k_0$. Si $\alpha$ est algébrique sur $k_0$, alors en utilisant le fait que $K$ est Hensélien, on trouve $a \in K$ tel que $\mathrm{res}\,(a) = \alpha$ et $[K_0(a) : K_0] = [k_0(\alpha) : k_0]$ ; comme $K_0(a)/K_0$ est purement résiduelle, elle est contenue dans $\mathcal{O}_v \setminus \mathcal{M}_v \cup \{0\}$, ce qui contredit la maximalité de $K_0$. On raisonne de la même façon si $\alpha$ est transcendant sur $k_0$.

**5.14. L'axiomatisation**. Nous allons considérer la théorie $T$ dans le langage à 3 sortes (avec les fonctions $v$, res et $f$) qui est axiomatisée de la façon suivante : les modèles de $T$ sont les structures $(K, \Gamma, k)$ satisfaisant :

(i) $(K, \Gamma, k)$ est la structure associée à un corps valué Hensélien de caractéristique 0.

(ii) $v(p)$ est le plus petit élément positif de $\Gamma$.

(iii) $\mathrm{Th}(\Gamma)$, $\mathrm{Th}(k)$.

(iv) $f : k \to K$ prend ses valeurs dans $\mathcal{O}_v$ et est multiplicative.

(v) Pour chaque $n$ et $\ell \in \mathbb{Z}^\ell$, soient $R_0, \ldots, R_n$ les polynômes donnés par 5.11. Alors on ajoute un axiome disant:

$$\forall x \ \ell \cdot f(x) = 0 \iff R_0(x) = \cdots = R_N(x) = 0.$$

**5.15. Théorème** La théorie $T$ décrite ci-dessus est complète.

*Démonstration.* Soit $(K, \Gamma_K, k_K)$ un modèle $\aleph_1$-saturé de $T$, avec valuation $v$. Nous allons voir comment simplifier le problème.

Comme $v(p)$ est le plus petit élément de $\Gamma_K$, le sous-groupe engendré par $v(p)$ est convexe et isomorphe à $\mathbb{Z}$. Soit $\tilde{v}$ la valuation obtenue en composant $v$ avec la projection $\Gamma \to \Gamma/\mathbb{Z}$ (voir la sous-section 3.6). Alors son anneau de valuation $\mathcal{O}_{\tilde{v}}$ égale $\mathcal{O}_v[1/p]$. De plus, $v$ induit une valuation $v^*$ sur le corps résiduel $k_{\tilde{v}}$ de $\tilde{v}$, et on a $\Gamma_{v^*} = \mathbb{Z}$, et $k_{v^*} = k_K = k_v$. Notons que $k_{\tilde{v}}$ est de caractéristique 0, et qu'il est complet pour la valuation $v^*$ (par $\aleph_1$-saturation de $K$).

Soit maintenant $(L, \Gamma_L, k_L)$ un autre modèle de $T$, qui est $\aleph_1$-saturé, et dont nous noterons la valuation par $w$. On définit de la même façon une valuation $\tilde{w}$, et une valuation $w^*$ sur $k_{\tilde{w}}$. On peut supposer, passant à des extensions élémentaires de $K$ et de $L$ si nécessaire, que les corps résiduels $k_K$ et $k_L$ sont isomorphes, et les groupes de valeurs $\Gamma_K$ et $\Gamma_L$ aussi. Les corps valués (discrets complets) $(k_{\tilde{v}}, v^*)$ et $(k_{\tilde{w}}, w^*)$ seront alors isomorphes, par un isomorphisme $\varphi$. Que se passe-t-il pour les représentants de Teichmüller ? Nous savons que $f(k_K)$ est contenue dans $\mathcal{O}_v^\times = \{a \in K \mid v(a) = 0\}$, et composant avec l'application $\mathcal{O}_v \subset \mathcal{O}_{\tilde{v}} \to k_{\tilde{v}}$, nous obtenons une application $\tilde{f} : k_K \to \mathcal{O}_{v^*}^\times$ qui est multiplicative ; de même, l'application $f$ sur $L$ nous donne une application $\tilde{f} : k_L \to \mathcal{O}_{w^*}^\times$, et $\varphi$ commute avec $\tilde{f}$ (par 5.8).

Par le Lemme 5.13, il existe des sous-corps $K_0 \subset \mathcal{O}_{\tilde{v}}$ et $L_0 \subset \mathcal{O}_{\tilde{w}}$ tels que l'application résiduelle associée à $\tilde{v}$ soit une bijection entre $K_0$ et le corps résiduel $k_{\tilde{v}}$, et pareillement

pour $L_0$. De plus, ces corps peuvent être choisis contenant $f(k_K)$ et $f(k_L)$ respectivement. L'isomorphisme $\varphi$ induit alors un isomorphisme $\psi : K_0 \to L_0$, et cet isomorphisme commute avec $f$ et est un isomorphisme de corps valués.

Maintenant, en appliquant la version forte du Théorème de Pas aux corps valués $(K, \tilde{v})$ et $(L, \tilde{w})$, nous déduisons qu'il existe un système de va-et-vients qui contient $\psi$. C'est-à-dire, les $\mathcal{L}'_{\text{Pas}}$-structures $K$ et $L$ sont élémentairement équivalentes, où $\mathcal{L}'_{\text{Pas}}$ est obtenu en prenant pour $\mathcal{L}'_{\text{c.rés}}$ un langage suffisamment fort pour décrire le corps valué $(k_{\tilde{v}}, v^*)$ muni de l'application $\tilde{f}$.

## 5.4 Clôtures algébriques et définissables

**5.16. Espaces de types**. Soient $T$ une théorie, $M$ un modèle de $T$, et $A \subset M$, $n$ un entier. Un *$n$-type* est un ensemble de $\mathcal{L}(A)$-formules en $x = (x_1, \ldots, x_n)$ qui est finiment satisfaisable dans $M$ ; un $n$-type maximal sera appelé *complet*, et sinon il sera *partiel*. [Finiment satisfaisable dans $M$ : si $\varphi_1(x), \ldots, \varphi_m(x)$ appartiennent au type alors il existe $a \in M^n$ tel que $M \models \bigwedge_i \varphi_i(a)$.] De façon équivalente, un type $p(x)$ est complet si pour toute $\mathcal{L}(A)$-formule $\varphi(x)$, ou bien $\varphi(x) \in p(x)$, ou bien $\neg\varphi(x) \in p(x)$. Notez que tout type complet contient $T(A)$, la $\mathcal{L}(A)$-théorie de $M$.

L'espace des $n$-types (complets) est noté $S_n(A)$ ; on le munit d'une topologie, dont les ouverts de base sont

$$\langle\varphi(x)\rangle := \{p(x) \in S_n(A) \mid \varphi(x) \in p(x)\}.$$

Remarquez que le complémentaire de $\langle\varphi(x)\rangle$ est $\langle\neg\varphi(x)\rangle$, et que donc $\langle\varphi(x)\rangle$ est un ouvert-fermé. Le théorème de compacité nous donne que $S_n(A)$ est compact ; l'espace $S_n(A)$ est donc un espace Booléen. Les points isolés de $S_n(A)$ sont appelés des *types isolés*. Si $\varphi(x)$ est une $\mathcal{L}(A)$-formule isolant un point $p(x)$, alors on dira que la formule $\varphi(x)$ est *complète*, et que $p(x)$ est *isolé* par $\varphi(x)$.

**5.17.** Soit $M$ un modèle d'une $\mathcal{L}$-théorie complète $T$, et soient $A \subset M$, $a \in M$. On dit que $a$ est *définissable sur $A$*, s'il existe une $\mathcal{L}(A)$-formule $\varphi(x)$ qui est satisfaite par $a$ dans $M$, et par aucun autre élément de $M$. On dit que $a$ est *algébrique sur $A$*, s'il existe une $\mathcal{L}(A)$-formule satisfaite par $a$ dans $M$, et qui n'est satisfaite que par un nombre fini d'éléments de $M$. L'ensemble des éléments de $M$ qui sont définissables sur $A$ est noté $dcl(A)$, celui des éléments qui sont algébriques sur $A$ est noté $acl(A)$. On vérifie facilement les propriétés suivantes :

$$A \subset B \text{ implique } dcl(A) \subset dcl(B) \text{ et } acl(A) \subset acl(B)$$
$$dcl(dcl(A)) = dcl(A) \subset acl(A) = acl(acl(A)).$$

On montre facilement que si $a \in acl(A)$ (un $n$-uplet), et $T(A)$ dénote la $\mathcal{L}(A)$-théorie de $M$, alors il existe une $\mathcal{L}(A)$-formule $\varphi(x)$ satisfaite par $a$, et telle que

$$T(A) \cup \{\varphi(x)\} \vdash tp(a/A),$$

c'est-à-dire que tous les éléments qui satisfont $\varphi(x)$ dans $M$ satisfont les mêmes $\mathcal{L}(A)$-formules. En effet, on prend pour $\varphi(x)$ une $\mathcal{L}(A)$-formule $\varphi(x)$ satisfaite par $a$ et ayant un nombre

minimal de réalisations dans $M$. Si $\psi(x)$ est une autre $\mathcal{L}(A)$-formule satisfaite par $a$, alors $|\varphi(M^n) \wedge \psi(M^n)| \geq |\varphi(M^n)|$ [les uplets satisfaisant $\varphi \wedge \psi$ et $\varphi$ respectivement], ce qui entraine que les uplets de $M$ satisfaisant $\varphi(x)$ satisfont aussi $\psi(x)$ et donc $T(A) \vdash \varphi(x) \to \psi(x)$.

On dénote par $\mathrm{Aut}(M/A)$ l'ensemble des automorphismes de $M$ qui sont l'identité sur $A$. Si $B \subset M$, on dénote par $\mathrm{Aut}(B/A)$ toutes les permutations $\sigma$ de $B$ qui fixent $A$ et sont élémentaires au sens de $M$, i.e., pour tout uplet $b$ dans $B$ et $\mathcal{L}(A)$-formule $\varphi$, on a $M \models \varphi(a)$ si et seulement si $M \models \varphi(\sigma(a))$.

Remarquons que si $A \subset M \prec N$, alors $acl(A)$ au sens de $M$ et de $N$ sont les mêmes. Voici une caractérisation des clôtures algébriques et définissables en termes de groupes d'automorphismes :

(1) $a \in dcl(A)$ si et seulement si pour toute extension élémentaire $N$ de $M$ et $\sigma \in \mathrm{Aut}(N/A)$, $\sigma(a) = a$.

(2) $a \in dcl(A)$ si et seulement si pour toute extension élémentaire $N$ de $M$, l'orbite de $a$ par $\mathrm{Aut}(N/A)$ est finie.

Ces propriétés suivent facilement de la

**5.18. Remarque importante/Exercice**. Si $A \subset M$ et $a$, $b$ sont deux uplets de $M$ qui ont le même type sur $A$ (c'est-à-dire, $tp(a/A) = tp(b/A)$), alors il existe une extension élémentaire $N$ de $M$ et un automorphisme $\sigma$ de $N$ qui fixe $A$ et envoie $a$ sur $b$. [Ce résultat est en fait un résultat classique, et est immédiat si on sait que tout modèle se plonge élémentairement dans un modèle homogène. Il existe cependant des preuves plus simples, voici des indications pour une telle preuve. Montrez d'abord qu'il suffit de le montrer pour $M$ dénombrable. Puis, étant donnés $M$ et un isomorphisme partiel élémentaire $f : B \to C$ où $B, C \subset M$, montrez que $M$ a une extension élémentaire $N$ de même cardinalité, dans laquelle $f$ s'étend à un isomorphisme partiel élémentaire de domaine contenant $M$.]

**5.19. Définitions**. Soit $A \subset M$. On dénote par $\mathrm{Aut}(acl(A)/A)$ l'ensemble des automorphismes de la $\mathcal{L}$-structure $acl(A)$ qui sont élémentaires (au sens de $M$). C'est un groupe profini.

Si $\mathrm{Aut}(acl(A)/A)$ est réduit à 1 élément, alors on dit que $acl(A)$ est *rigide sur* $A$. Dans ce cas on aura que $acl(A) = dcl(A)$. Plus généralement, si $A \subset B \subset M$, on dit que $B$ est *rigide* sur $A$ si tout automorphisme de $B$ qui est élémentaire au sens de $M$ et fixe les éléments de $A$ est l'identité.

## 5.5 Fonctions de Skolem

**5.20. Définition**. Soit $T$ une théorie dans un langage $\mathcal{L}$. On dit que $T$ a *des fonctions de Skolem définissables* si pour toute $\mathcal{L}$-formule $\varphi(x, y)$, $y$ une seule variable, il existe une formule $\psi(x, y)$ telle que :

(i) $T \vdash \forall x, y\ \psi(x, y) \to \varphi(x, y)$

(ii) $T \vdash \forall x \exists^{\leq 1} y\ \psi(x, y)$

(iii) $T \vdash \forall x\ (\exists y\ \varphi(x,y) \to \exists y\ \psi(x,y))$.

Notons que la condition (ii) dit que dans tout modèle $M$ de $T$, $\psi(x,y)$ définit le graphe d'une fonction $f_\varphi$. Les conditions (iii) et (i) nous disent alors que cette fonction choisit, pour chaque uplet $a$ tel que $\varphi(a,M)$ $(= \{b \in M \mid M \models \varphi(a,b)\})$ est non-vide, un élément de $\varphi(a,M)$.

On peut toujours étendre le langage et fabriquer une théorie étendant notre théorie $T$ et qui ait des fonctions de Skolem définissables dans ce nouveau langage : pour chaque $\mathcal{L}$-formule $\varphi(x,y)$, on ajoute à $\mathcal{L}$ un symbole de fonction $f_\varphi$, et puis on ajoute à $T$ l'axiome disant que $f_\varphi$ est une fonction de Skolem pour $\varphi$. La théorie ainsi obtenue est appelée la *Skolémisée* de $T$.

**5.21. Théorème**. Soit $T$ une $\mathcal{L}$-théorie qui élimine les quantificateurs. Les conditions suivantes sont équivalentes :

(1) $T$ a des fonctions de Skolem définissables.

(2) Si $A$ est un modèle de $T_\forall$, alors il existe un modèle $M$ de $T$ qui contient $A$ et est algébrique sur $A$, et rigide sur $A$.

*Démonstration.* (1) $\Rightarrow$ (2). Soit $A$ un modèle de $T_\forall$. Alors il existe un modèle $M$ de $T$ contenant $A$. Considérons $B = dcl(A)$. Notons que $B$ est clos par les fonctions définissables. Nous allons montrer que $B \prec M$. Appliquons le test de Tarski : soient $\varphi(x,y) \in \mathcal{L}$, $y$ une seule variable, $a$ un uplet de $B$, et supposons que $M \models \varphi(a,b)$ pour un $b \in M$. Alors $M \models \varphi(a, f_\varphi(a))$. Mais $f_\varphi(a) \in B$. Donc $B \prec M$, et $B$ est certainement rigide au-dessus de $A$.

(2) $\Rightarrow$ (1). Supposons que ce ne soit pas le cas, et soit $\varphi(x,y)$ une $\mathcal{L}$-formule qui n'ait pas de fonction de Skolem définissable. Pour simplifier les notations, nous ajoutons au langage un uplet $c$ de constantes, et considérons la formule $\varphi(c,y)$ ayant une seule variable libre $y$. Alors $T$ élimine encore les quanteurs dans ce nouveau langage, et satisfait aussi la condition (2). Notons aussi que si nous arrivons à trouver une formule dans ce nouveau langage qui satisfait les conditions (i), (ii) et (iii) de la définition, alors, cette formule s'écrira $\psi(c,y)$, où $\psi(x,y) \in \mathcal{L}$. Mais, si $\theta(x) \in \mathcal{L}$, alors $T \vdash \theta(c)$ est équivalent à $T \vdash \forall x\ \theta(x)$, puisque le uplet $c$ n'est pas dans $\mathcal{L}$. Nous aurons donc obtenu la contradiction voulue.

Soit $\Delta$ l'ensemble des formules $\psi(y)$ telles que $T \vdash \psi(y) \to \varphi(y)$ et $T \vdash \exists^{\leq 1} y\ \psi(y)$. Considérons maintenant l'ensemble $\Gamma = \{\forall y \neg\psi(y) \mid \psi \in \Delta\}$.

Supposons que $T \cup \Gamma \cup \{\exists y\ \varphi(y)\}$ soit consistant, et soit $M$ un modèle de cette théorie, et $A$ la sous-structure de $M$ engendrée par les constantes du langage. Par hypothèse, il existe un modèle $B$ de $T$ qui contient $A$, et est algébrique et rigide sur $A$. Comme $T$ élimine les quantificateurs, nous savons que $M$ et $B$ sont élémentairement équivalents dans le langage $\mathcal{L}(A)$. Comme $B$ est algébrique sur $A$, cela entraine, raisonnant élément par élément et utilisant le fait que si $b$ est un uplet de $B$, alors $tp(b/\emptyset) = tp(a/A)$ est isolé, que $M$ contient une copie de $B$, et sans perte de généralité, nous supposerons que $B \subset M$, c'est-à-dire, $B \prec M$. Nous savons aussi que $M \models \exists y\ \varphi(y)$, et donc il existe $b \in B$ tel que $B \models \varphi(b)$. Comme $B = dcl(A)$, si $\psi(y)$ est la $\mathcal{L}$-formule qui *isole* $tp(b/\emptyset)$ $(= tp(b/A))$, nous avons alors : $T \models \psi(y) \to \varphi(y)$, et $T \models \exists^{\leq 1} y\ \psi(y)$.

La théorie $T \cup \Gamma \cup \{\exists y\ \varphi(y)\}$ est donc inconsistante. Par compacité, il existe des formules $\psi_1(y), \ldots, \psi_k(y) \in \Delta$ telles que $T \vdash (\exists y \varphi) \to (\exists \psi_1(y) \vee \psi_2(y) \vee \cdots \vee \psi_k(y))$. Prenons maintenant la formule

$$\theta(y) = \psi_1(y) \vee (\neg\psi_1(y) \wedge \psi_2(y)) \vee \cdots \vee (\neg\psi_1(y) \wedge \cdots \wedge \neg\psi_{k-1}(y) \wedge \psi_k(y)),$$

Alors on observe que $T \vdash \theta(y) \to \varphi(y)$, que $T \vdash \exists^{\leq 1} y\ \theta(y)$ et que $T \vdash \exists y\ \varphi(y) \to \exists y\ \theta(y)$.

**5.22. Remarque**. La condition que $T$ élimine les quantificateurs n'est pas un problème du tout : on peut toujours trouver un langage dans lequel une extension par définitions de $T$ élimine les quantificateurs : il suffit de rajouter à $\mathcal{L}$, pour chaque $\mathcal{L}$-formule $\varphi(x)$, un symbole de relation $R_\varphi(x)$, et d'ajouter à $T$ les axiomes $\forall x\ \varphi(x) \leftrightarrow R_\varphi(x)$. Les ensembles définissables ne changent pas, seule la complexité des formules change.

**5.23. Non-exemple 1**. Soit $T$ la théorie des corps algébriquement clos dans le langage des anneaux. Nous savons qu'elle élimine les quantificateurs. De plus, si $A \subset M \models T$, alors la clôture algébrique du corps $B$ de fractions de $A$ est algébrique sur $A$ (évidemment). Cependant, si $B$ n'est pas séparablement clos, cette clôture algébrique sera loin d'être rigide sur $B$, puisque le groupe de Galois sera non-trivial.

**5.24. Exemple 2**. Soit $T$ la théorie des corps réels clos, dans le langage des anneaux. Elle est axiomatisée en disant que tout polynôme de degré impair a une racine, tout carré a une racine quatrième, et $-1$ n'est pas un carré. On sait d'autre part qu'un corps réel clos est ordonné, les éléments positifs étant les carrés non nuls. Cet ordre est donc définissable dans le langage des anneaux. On sait aussi que la théorie des corps réels clos élimine les quantificateurs dans le langage des anneaux ordonnés, appelons $T_1$ cette théorie (qui dira que les éléments positifs sont les carrés non nuls). Si $T_1$ a des fonctions de Skolem définissables, alors $T$ en aura aussi, puisque $<$ est définissable.

Soient $A \subset M \models T_1$. Si $B$ dénote le corps des fractions de $A$, alors $B \subset dcl(A)$, et $C = B^{alg} \cap M$ est un corps réel clos contenant $A$, et algébrique sur $A$. Soit $a \in C$, $a \notin B$, et soit $f(T)$ son polynôme minimal sur $B$, mettons de degré $n$. Alors les racines de $f(T)$ sont distinctes, et $C$ en contient $r \leq n$. Comme tout automorphisme du corps ordonné $C$ sur $A$ respecte l'ordre, il ne peut permuter les racines de $f(T)$, et est donc l'identité sur $C$.

**5.25. Exemple 3**. Soit $K$ une extension finie de $\mathbb{Q}_p$, et $T$ sa théorie dans le langage augmenté de deux symboles de constantes si $[K : \mathbb{Q}_p] > 1$, ces symboles étant interprétés comme dans 5.5. Alors $T$ a des fonctions de Skolem définissables.

*Démonstration.* Les symboles $P_n$ de $\mathcal{L}_{\mathrm{Mac}}$ sont définissables dans le langage des anneaux. Les résultats de 5.1 et 5.5 nous donnent une théorie $T_1$ qui élimine les quantificateurs (dans $\mathcal{L}_{\mathrm{Mac}}(c_1, c_2)$). Comme dans l'exemple 2, il suffit de montrer que $T_1$ a des fonctions de Skolem définissables.

Nous avons d'autre part vu que si $A$ est une sous-structure de $M \models T$, si $B$ est le corps de fractions de $A$, et $C = M \cap B^{alg}$, alors $C \prec M$. Il suffit maintenant de montrer que $C$ est rigide sur $A$ (ou sur $B \subset dcl(A)$). Supposons que non, et soit $\sigma$ un $\mathcal{L}_{\mathrm{Mac}}$-automorphisme de $C$ qui fixe les éléments de $A$ (et donc de $B$). Soit $D$ le sous-corps de $C$ fixé par $\sigma$.

Nous allons d'abord montrer que si $a \in D$ satisfait $P_n$ (dans $C$), alors $a$ a une racine $n$-ième dans $D$. Soit $b \in C$ tel que $b^n = a$, et soit $m \geq 2$ un entier quelconque.

Pour cela, nous commençons par prouver un lemme facile :

**5.26. Lemme**. Soit $M$ un corps valué élémentairement équivalent à une extension finie de $\mathbb{Q}_p$, et soit $B$ un sous-corps de $M$, $A = B \cap \mathcal{O}_M$, et supposons que $v(A)$ contienne le plus petit élément du groupe de valeurs de $M$, et que res $(A)$ égale le corps résiduel $k_M$ de $M$. Alors, si $a \in M$ et $m \in \mathbb{N}$, il existe $d \in A$, tel que $M \models P_m(da) \wedge d \neq 0$.

*Démonstration.* Il n'y a rien à prouver si $a = 0$, supposons $a \neq 0$. Passant à une extension élémentaire de $M$, nous pouvons supposer que $M$ est $\aleph_1$-saturé, et que la valuation admet une section multiplicative $s : \Gamma_M \to M$ (cf. Lemme 4.17). Notons que si $\gamma \in m\Gamma$, alors $M \models P_m(s(\gamma))$. Si $\ell = 2v(m) + 1$, on montre alors que

$$\begin{aligned} M \models P_m(a) &\iff v(a) \equiv_m 0 \wedge P_m(as(-v(a))) \\ &\iff v(a) \equiv_m 0 \wedge \exists y\ v(y^m - as(-v(a))) \geq \ell. \end{aligned}$$

Dit d'une autre façon, soit $\eta \in A$ tel que $v(\eta) = 1$, et $A_0 \subset A/\eta^\ell A$ l'ensemble des puissances $m$-ièmes d'éléments inversibles de $A/\eta^\ell A$ : alors un élément de $M$ est une puissance $m$-ième si et seulement si $v(a) \equiv_m 0$ et l'image de $as(-v(a))$ dans $A/\eta^\ell A$ est dans $A_0$ ; notez que cette dernière formulation ne dépend pas du choix de la section $s$.

Retournons au problème original. A l'aide de cette caractérisation, on voit qu'il suffit de multiplier $a$ d'abord par une puissance de $\eta$, $d_1$, pour que $v(a) \equiv_m 0$ ; puis par un élément $d_2$ de $A$ tel que l'image de $ad_1d_2s(-v(ad_1))$ dans $A/\eta^\ell A$ soit égale à 1. □

**5.27.** *Fin de la démonstration de 5.25.* Nous savons que $B$ a même corps résiduel que $K$, et que son groupe de valeurs contient le plus petit élément positif du groupe de valeurs de $K$. Fixons un entier $m$. Par le lemme précédent, il existe $d \in B$ tel que $C \models P_m(bd)$. Nous avons alors

$$C \models P_m\left(\frac{\sigma(bd)}{bd}\right), \quad \text{et } \frac{\sigma(bd)}{bd} = \frac{\sigma(b)d}{bd} = \frac{\sigma(b)}{b}.$$

D'autre part, $\frac{\sigma(b)}{b}$ est une racine $n$-ième de l'unité, et nous avons montré qu'elle a une racine $m$-ième dans $K$ pour tout $m \geq 2$. Le lemme 5.28 ci-dessous montre que ce n'est possible que si $\frac{\sigma(b)}{b} = 1$, i.e., $\sigma(b) = b$.

Nous avons donc montré que si $a$ a une racine $n$-ième dans $C$, alors il en a déja une dans $D$. Comme le groupe de valeurs de $C$ est contenu dans la clôture divisible du groupe de valeurs de $B$, cela entraîne qu'il est égal au groupe de valeurs de $D$. Donc $C$ est une extension immédiate de $D$, et c'est l'Hensélianisée de $D$. C'est-à-dire que le corps $C$ est obtenu en ajoutant des solutions à des équations ayant des solutions résiduelles simples. Mais nous avons vu qu'une telle solution était nécéssairement unique : si $f(T) \in \mathcal{O}_B[T]$ et $b \in \mathcal{O}_B$ sont tels que $v(f(b)) > 0 = v(f'(b))$ alors il existe un unique $a \in M$ tel que $f(a) = 0$ et $v(b - a) > 0$. Cela montre, de proche en proche, que tous les éléments de $C$ sont définissables sur $D$, et donc que $C$ est rigide sur $A$.

**5.28. Lemme**. Nous fixons un premier $p$, et travaillons dans une clôture algébrique de $\mathbb{Q}_p$.

(1) Soient $\mu_{p'}$ le groupe de racines primitives de l'unité d'ordre premier à $p$, et $M = \mathbb{Q}(\mu_{p'})$. Alors res définit un isomorphisme (multiplicatif) entre $\mu_{p'}$ et les éléments non nuls du corps résiduel $\mathbb{F}_p^{alg}$ de $M$.

(2) Soit $\zeta$ une racine primitive $p^n$-ième de l'unité. Alors l'indice de ramification de $\mathbb{Q}_p(\zeta)$ sur $\mathbb{Q}$ est $(p-1)p^{n-1}$.

(3) Si $K$ est une extension finie de $\mathbb{Q}_p$, alors $K$ ne contient qu'un nombre fini de racines primitives de l'unité.

*Démonstration.* (3) est une conséquence de (1) et (2): le corps résiduel de $K$ est fini, et l'indice de ramification $e(K/rat_p)$ aussi.

(1) Soit $\alpha \in \mathbb{F}_p^{alg}$, et soit $\ell$ son ordre ; alors $\ell$ est premier à $p$ (car il divise $q-1$ pour une puissance $q$ de $p$) ; si $K$ est n'importe quelle extension finie de $\mathbb{Q}_p$ ayant $\alpha$ dans son corps résiduel, alors $K$ contiendra une racine primitive $\ell$-ième de l'unité : $\alpha$ est une racine simple du polynôme $T^\ell - 1 = 0$, et, comme $K$ est Hensélien, $K$ contient un élément $a$ satisfaisant $\mathrm{res}\,(a) = \alpha$ et $a^\ell = 1$. L'application res induit donc bien une surjection $\mu_{p'} \to \mathbb{F}_p^{alg} \setminus \{0\}$.

Pour montrer que cette application est une injection, il suffit de montrer que le groups multiplicatif de $\mathbb{F}_p^{alg}$ contient des éléments d'ordre $\ell$, pour tout $\ell$ premier à $p$. Cela suit du théorème d'Euler : comme $\ell$ est premier à $p$, on a $p^{\varphi(\ell)} \equiv 1\ (\ell)$ ($\varphi(\ell)$ étant la fonction d'Euler, qui compte le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/\ell\mathbb{Z}$) ; cela veut dire que $\ell$ divise $p^{\varphi(\ell)} - 1$. Comme le groupe multiplicatif de $\mathbb{F}_{p^{\varphi(\ell)}}$ est cyclique d'ordre $p^{\varphi(\ell)} - 1$, cela donne le résultat.

(2) Nous allons montrer par induction sur $e \geq 1$ que si $\zeta$ est une racine primitive $p^e$-ième de l'unité, alors $v(\zeta - 1) = p^{-e+1}(p-1)^{-1}$. Si $u = \zeta - 1$, alors $v(u) > 0$, car 1 est la seule racine primitive $p^e$-ième de $\mathbb{F}_p^{alg}$.

Cas $e = 1$. Alors $(u+1)^p = 1$. Donc $u^p + \sum_{i=1}^{p-1} \binom{p}{i} u^i = 0$ ; comme $v(\binom{p}{i}) = v(p)$, et $v(u) > 0$, $v(\sum_{i=1}^{p-1} \binom{p}{i} u^i) = v(p) + v(u)$. Cela donne $v(p) + v(u) = v(u^p) = p(v(u))$, c'est-à-dire, $v(u) = (p-1)^{-1}$.

Cas général. Supposons le résultat montré pour $e-1$. Nous avons $\zeta^p - 1 = (u+1)^p - 1 = u^p + \sum_{i=1}^{p-1} \binom{p}{i} u^i$ ; comme $v(u) > 0$, $v(\sum_{i=1}^{p-1} \binom{p}{i} u^i) = v(p) + v(u)$ ; $v(u^p) \geq v(p) + v(u)$ entraîne $(p-1)v(u) \geq 1$, et donc $v(\zeta^p - 1) \geq pv(u) > 1$, ce qui contredit l'hypothèse d'induction. Donc $v(u^p) < v(p) + v(u)$, et $v(\zeta^p - 1) = pv(u)$, ce qui donne le résultat.

## 5.6 Dimensions, théories algébriquement bornées

**5.29. Dimensions**. Soit $M$ une $\mathcal{L}$-structure. Une *dimension* est une fonction $d$ définie sur les sous-ensemble définissables de $M^n$, $n \in \mathbb{N}$, à valeurs dans $\mathbb{N} \cup \{-\infty\}$, qui satisfait aux conditions suivantes :

Dim 1 $d(S) = -\infty \iff S = \emptyset$ ; $d(\{a\}) = 0$ ; $d(M) = 1$.

Dim 2 $d(S_1 \cup S_2) = \max\{d(S_1), d(S_2)\}$.

Dim 3 Si $\sigma$ est une permutation de $\{1, \ldots, n\}$, et $S \subset M^n$ alors $d(S^\sigma) = d(S)$, où $S^\sigma = \{(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) \mid (a_1, \ldots, a_n) \in S\}$.

Dim 4 Soit $S \subset M^{n+1}$, et pour $x \in M^n$, posons $S(x) = \{y \mid (x, y) \in S\}$, et $S^{(i)} = \{x \in M^n \mid d(S(x)) = i\}$, $i = 0, 1$. Alors les ensemble $S^{(i)}$ sont définissables, et $d(S) = \max\{d(S^{(i)}) + i\}$.

La plupart des structures n'ont pas de notions de dimension. En effet, notons par exemple que Dim 4 implique que s'il existe une bijection définissable entre deux ensembles, alors ces deux ensembles auront même dimension. En particulier, il ne peut exister d'injection définissable de $M^2$ dans $M$.

Notons que nous obtenons, par induction, une version plus générale de Dim 4 :

Dim 4' Soit $S \subset M^{n+m}$, et pout $x \in M^n$ soit $S(x) = \{y \in M^m \mid (x, y) \in S\}$. Pour $i = 0, \ldots, m$, posons $S^{(i)} = \{x \in M^n \mid d(S(x)) = i\}$. Alors les ensembles $S^{(i)}$ sont définissables et $d(S) = \max\{d(S^{(i)}) + i\}$.

**5.30. Exemple de dimension**. Considérons la théorie des corps algébriquement clos, et prenons pour dimension la dimension algébrique de la clôture de Zariski d'un ensemble. Nous obtenons alors une notion de dimension qui vérifie les axiomes ci-dessus. J'appelle cette dimension la dimension algébrique.

On peut en fait définir dans n'importe quel corps $K$ une fonction $d$ en posant, pour $S \subset K^n$ un ensemble définissable, $d(S) = \dim(\bar{S})$, où $\bar{S}$ dénote la clôture de Zariski de $S$. Mais en général cette fonction $d$ ne satisfait pas les axiomes que nous exigeons d'une dimension. La propriété d'algébricité bornée, définie ci-dessous, nous permettra de donner plusieurs exemples de théories pour lesquelles la dimension algébrique définit une bonne notion de dimension.

**5.31. Exercice**. Soit $K$ un corps. On définit la topologie de Zariski sur $K^n$ en prenant comme ensembles fermés de base les ensembles

$$V(f_1, \ldots, f_m) = \{a \in K^n \mid f_1(a) = \cdots = f_m(a)\},$$

où $f_1, \ldots, f_m \in K[X]$, $X$ un $n$-uplet de variables. Notez que si $I$ est l'idéal de $K[X]$ engendré par les $f_i$, alors $V(f_1, \ldots, f_m) = V(I)$. Comme l'anneau $K[X]$ est Noethérien, cela entraine que toute suite strictement décroissante de fermés est finie, et que tout fermé est de la forme ci-dessus.

(1) Soit $S \subset K^n$, et soit $(f_1, \ldots, f_m)$ un système de générateurs pour l'idéal $I(S) = \{f \in K[X] \mid \forall a \in S\ f(a) = 0\}$. Montrez que $V(f_1, \ldots, f_m)$ est la clôture (de Zariski) de $S$.

(2) Soit $U$ une composante irréductible de $\bar{S}$. Montrez que $U \cap S$ est Zariski dense dans $U$.

**5.32. Proposition**. Soit $K$ un corps, $S \subset K^n$ un ensemble définissable. Alors sa dimension algébrique est $\geq \ell$ si et seulement s'il existe une extension élémentaire $K^*$ de $K$, et un uplet $a \in S(K^*)$ tel que $tr.deg(K(a)/K) \geq \ell$.

*Démonstration.* C'est immédiat quand on explicite la définition de la clôture de Zariski (et en utilisant l'exercice ci-dessus). Soit $\bar{S}$ la clôture de Zariski de $S$, $U$ une de ses composantes irréductibles de dimension maximale, et $I \subset K[X]$ l'idéal des polynômes qui s'annulent sur $U$. Alors $U \cap S$ est Zariski dense dans $U$, et le type partiel

$$\{x \in U\} \cup \{f(x) \neq 0 \mid f(X) \notin I\}$$

est finiment satisfaisable dans $U(K)$. Cela montre que $S(K^*)$ contient un générique de $U$, et montre une direction. Pour l'autre, soit $a \in S(K^*)$ de degré de transcendance $d$ sur $K$ ; le plus petit fermé de Zariski défini sur $K$ et contenant $a$ est alors de dimension $d$ ; d'autre part, comme $S$ est défini sur $K$, sa clôture de Zariski l'est aussi, et elle contient $a$, d'où elle doit être de dimension $\geq d$.

**5.33. Définition**. Soit $\mathcal{L}$ un langage contenant le langage des anneaux, et $T$ une théorie contenant la théorie des anneaux commutatifs intègres ; soit $C$ l'ensemble des constantes du langage. On dit que $T$ est *algébriquement bornée* si pour toute formule $\varphi(x, y)$, $y$ une seule variable, il existe des polynômes $f_1(X, Y), \ldots, f_m(X, Y) \in \mathbb{Z}[C, X, Y]$[1] tels que :
pour tout modèle $M$ de $T$ et uplet $a$ in $M$, si l'ensemble $\varphi(a, M) = \{b \in M \mid M \models \varphi(a, b)\}$ est fini, alors il existe $k$ tel que $f_k(a, Y)$ n'est pas identiquement nul sur $M$, et $M \models \varphi(a, y) \rightarrow f_k(a, y) = 0$.

**Remarque**. On voit qu'on peut étendre facilement cette propriété à des uplets $y$.

**5.34. Théorème**. Soit $T$ une théorie algébriquement bornée. Alors dans tout modèle de $T$, la dimension algébrique (notée $d$) vérifie les propriétés données dans 5.29.

De plus, la définition de cette dimension est uniforme, c'est-à-dire : pour chaque $\mathcal{L}$-formule $\varphi(x, y)$, $x$ un $n$-uplet de variables, $y$ un $m$-uplet de variables, et pour chaque $d \in \{0, 1, \ldots, m, -\infty\}$, il existe une formule $\psi_{\varphi,d}(x)$ telle que, dans tout modèle $M$ de $T$, la formule $\psi_{\varphi,d}$ définit l'ensemble des $n$-uplets $a$ tels que $\varphi(a, M^m)$ soit de dimension $d$. (Nous prenons toujours $\psi_{\varphi,-\infty}(x) = \forall y\ \neg\varphi(x, y)$.)

*Démonstration.* Soient $f_1(X, Y), \ldots, f_r(X, Y) \in \mathbb{Z}[X, Y]$ les polynômes associés à la formule $\varphi(x, y)$ et satisfaisant la conclusion de 5.33. Soit $S$ l'ensemble défini par $\varphi$, et $S^{(0)}$, $S^{(1)}$ comme dans Dim 4. Remarquons tout d'abord que si $N$ est un entier qui majore les degrés en $Y$ des polynômes $f_1, \ldots, f_r$, alors nous savons que pour tout modèle $M$ de $T$ et tout uplet $a$ de $M^n$

$$|\varphi(a, M)| < \infty \iff |\varphi(a, M)| \leq N. \tag{1}$$

Comme nous avons $d(\varphi(a, M)) = 0 \iff \varphi(a.M)$ est fini, cela montre la définissabilité uniforme de $S^{(i)}$, $i = 0, 1$.

[1] Attention, la définition n'est pas celle que j'ai donnée dans le cours, j'ai agrandi l'anneau sur lequel on prend les polynômes ; voir aussi le commentaire en fin de section.

Les axiomes Dim 1, 2 et 3 sont clairs. Si $\pi : M^{n+1} \to M^n$ est la projection, et $S_i = \pi^{-1}(S^{(i)}) \cap S$, pour vérifier l'axiome Dim 4, il nous reste donc à montrer que $dim\bar{S}_i = dim\overline{S^{(i)}} + i$ pour $i = 0, 1$. C'est clair pour $i = 1$ : on a toujours $dim\bar{S}_i \leq dim\overline{S^{(i)}} + 1$ ; de plus, si $a \in S^{(1)}$, alors $S(a)$ est infini. Par 5.32, nous pouvons prendre $(a, b)$ dans $K^*$ tel que $tr.deg(K(a)/K) = dim(S^{(1)})$ et $b$ soit transcendant sur $K(a)$.

Il nous reste à regarder le cas de $S^{(0)}$. On peut donc supposer que $S$ est tel que, pour tout $a \in \pi(S)$, $S(a)$ est contenu dans l'ensemble des zéros de $f(a, Y)$, où $f(X, Y) \in \mathbb{Z}[X, Y]$ et $f(a, Y)$ n'est pas identiquement nul. Il nous faut montrer que $dim(S) = dim(\pi(S))$. Mais si $(a, b) \in S(K^*)$, alors $f(a, b) = 0$, i.e., $tr.deg(K(a, b)/K) = tr.deg(K(a)/K)$.

Nous montrons la deuxième assertion par induction sur $m$. Pour $m = 1$, nous l'avons déjà fait plus haut. Supposons le résultat montré pour $m$, et soit $\varphi(x, y, z)$ une formule, $x$ un $n$-uplet de variables, $y$ un $m$-uplet de variables, et $z$ une seule variable. Soit $M$ un modèle de $T$, et $a$ un $n$-uplet de $M$, $S \subset M^{m+1}$ l'ensemble défini par $\varphi(a, y, z)$, et $S^{(i)}$, $i = 0, 1$, les ensembles donnés par l'axiome Dim 4 (appliqué à la projection $(x, y, z) \mapsto (x, y)$). Nous supposons $S \neq \emptyset$. Nous savons, par le premier cas, que $S^{(0)}$ et $S^{(1)}$ sont définissables par une formule $\theta_i(a, y)$, $i = 0, 1$, où $\theta_i(x, y) \in \mathcal{L}$. Par hypothèse d'induction, pour chaque $j = 0, \ldots, m$, nous avons des formules $\psi_{i,j}(x)$ qui définissent (dans tout modèle $M$ de $T$) l'ensemble des uplets $a$ tels que $d(\theta_i(a, M^m)) = j$. La formule $\psi_{\varphi,d}(x)$ sera donc $\bigvee_{i+j=d} \psi_{i,j}(x)$.

**5.35. Remarque**

Le seul ingrédient utilisé pour la définissabilité de la dimension est le suivant : le fait que pour toute $\mathcal{L}$-formule $\varphi(x, y)$ il existe un entier $N = N(\varphi)$ tel que dans tout modèle $M$ de $T$, pour tout uplet $a$ de $M$, on ait

$$|\varphi(a, M)| < \infty \iff |\varphi(a, M)| \leq N. \tag{1}$$

Dans ce cas, on dira que $T$ *élimine le quantificateur* $\exists^\infty$. Cette propriété n'est cependant pas suffisante pour garantir l'axiome Dim 4.

**5.36. Lemme**. Soit $K$ une extension finie de $\mathbb{Q}_p$, et $\varphi(x)$ une formule de $\mathcal{L}_{\mathrm{Mac}}(c_1, c_2)$, $A$ l'anneau $\mathbb{Z}[c_1, c_2]$, où $c_1$, $c_2$ sont les éléments définis dans 5.5 (avec $v(c_2)$ le plus petit élément du groupe de valeurs de $K$). Alors, modulo $T = \mathrm{Th}(K, c_1, c_2)$, $\varphi(x)$ est équivalente à une disjonction de formules de la forme

$$\bigwedge_i P_n^*(f_i(x)) \wedge \bigwedge_j g_j(x) = 0,$$

où les $f_i(X), g_j(X) \in A[X]$, et telles que les formules de cette disjonction sont deux à deux inconsistantes. Ici, $P_n^*(x) \leftrightarrow P_n(x) \wedge x \neq 0$.

*Démonstration.* Par le théorème 5.5, nous savons que $\varphi(x)$ est équivalente, modulo $T$, à une combinaison Booléenne de formules atomiques. On peut écrire cette combinaison Booléenne comme une disjonction (exclusive) de conjonctions de formules atomiques et négations d'atomiques.

Les formules atomiques sont de la forme $P_n^*(t(x))$, $t_1(x) \operatorname{div} t_2(x)$ et $t_1(x) = t_2(x)$, pour $t, t_1, t_2$ des termes du langage, c'est-à-dire des éléments de $A[X]$. On remarque d'abord que pour tout $n$, il existe un ensemble fini $A_n \subset A$ contenant 1 et tel que

$$K \models \forall x\ x = 0 \vee (\bigvee_{i \in A_n} P_n^*(ix) \wedge \bigwedge_{i \neq j \in A_n} \neg(P_n^*(ix) \wedge P_n^*(jx))).$$

On prend tout simplement pour $A_n$ un système de représentants des cosets $K^\times/(K^\times)^n$ contenant 1 et dans $A$. (Un tel ensemble existe car $A$ contient $c_1$ et $c_2$). Nous avons donc, modulo $T$ :

$$\begin{aligned} \forall x\ \neg P_n^*(x) &\leftrightarrow (x = 0 \vee \bigvee_{1 \neq i \in A_n} P_n^*(ix)) \\ \forall x\ x \neq 0 &\leftrightarrow \bigvee_{i \in A_n} P_n^*(ix). \end{aligned}$$

De plus, on vérifie que

$$x \operatorname{div} y \leftrightarrow y = 0 \vee \begin{cases} P_2^*(x^2 + c_2 y^2) & \text{si } p > 2, \\ P_3^*(x^3 + c_2 y^3) & \text{si } p = 2. \end{cases}$$

[Je vais faire le cas $p \neq 2$ : tout d'abord, en divisant par $x^2$, on peut se ramener au cas $x = 1$. Si $v(a) \geq 0$, alors $v(c_2 a^2) \geq v(c_2) > v(2) = 0$, $v(1 + c_2 a^2) = 0$, et il existe $b \in K$ tel que $v(b-1) = v(c_2 a^2)$ et $b^2 = 1 + c_2 a^2$. Dans l'autre direction : si $v(a) < 0$, alors $v(1 + c_2 a^2) = v(c_2 a^2) = v(c_2) + 2v(a)$ n'est pas divisible par 2 dans $\Gamma_K$, ce qui entraîne que $a + c_2 a^2$ n'est pas un carré.] Cela nous permet donc d'écrire $\varphi$ en utilisant seulement des formules positives, et sans utiliser la relation div. On remarque aussi que $P_{nm}^*(x^m) \leftrightarrow P_n^*(x)$ ; une formule $\bigwedge_i P_{n_i}^*(f_i(x))$ sera donc équivalente à une disjonctions de formules $\bigwedge_j P_n^*(g_j(x))$, où $n$ est un entier divisible par tous les $n_i$. [Attention, nous avons bien que $P_n^*(x) \to P_{mn}^*(x^m)$, mais la réciproque n'est pas nécessairement vraie, par exemple si $a^m = 1 \neq a$ ; pour montrer ce résultat il faut utiliser un sous-ensemble de $A_{nm}$]

**5.37. Théorème** Soit $K$ une extension finie de $\mathbb{Q}_p$. Alors sa théorie est algébriquement bornée.

*Démonstration.* C'est en fait un corollaire du Lemme 5.36. Soit $\varphi(x, y)$ une formule, $y$ une seule variable. Nous savons que, modulo $Th(K)$, $\varphi(x, y)$ est équivalente à une disjonction exclusive de formules de la forme $\bigwedge_i P_m^*(g_i(x, y)) \wedge \bigwedge_j f_j(x, y) = 0$, où les $g_i(X, Y)$, $f_j(X, Y) \in A[X, Y]$, et nous pouvons supposer qu'elle est de cette forme. Si l'ensemble des indices $j$ est non vide, alors les $f_j(X, Y)$ sont les polynômes souhaités. En effet, nous allons montrer

**Assertion**. Pour tout uplet $(a, b)$ dans $K$, si $g(X, Y) \in A[X, Y]$ et $K \models P_m^*(g(a, b))$, alors il existe $\gamma$ tel que tout élément de $B(b; \gamma)$ satisfasse $P_m^*(g(a, y))$.

Cette assertion se réduit aux deux remarques suivantes :

- Si $K \models P_m^*(c)$, et si $v(d - c) > v(c) + 2v(m)$, alors aussi $K \models P_m^*(c)$.

- Tout polynôme de $K[Y]$ définit une fonction continue $K \to K$. Etant donnés $g(Y) \in K[Y]$ et $b \in K$, $m \in \mathbb{Z}$, il existe donc $N$ tel que $c \in B(b; N)$ implique $g(c) \in B(g(b); m)$. (Le nombre $N$ peut d'ailleurs être calculé explicitement).

Il suit que pour tout uplet $a$ de $K$, l'ensemble défini par $\bigwedge_i P_m^*(g_i(a, y))$ est ouvert, et donc infini s'il est non vide. Donc, $\varphi(a, K)$ est fini si et seulement si l'un des polynômes $f_j(a, Y)$ est non trivial.

**5.38. Remarques**. En fait, essentiellement la même preuve montre que la clôture de Zariski de l'ensemble défini par $\varphi(x, y)$ est définie par les équations $\bigwedge_j f_j(x, y) = 0$.

L'avantage des prédicats $P_n^*$ sur les prédicats $P_n$ est qu'ils sont ouverts, ce qui n'est pas le cas de $P_n$ : par exemple, toute boule ouverte contenant 0 contiendra des éléments de valeur non divisible par $n$.

**5.39. Commentaires**. Le résultat montré par Van den Dries est en fait bien plus fort. Il utilise d'autres résultats d'élimination des quantificateurs pour montrer que la conclusion de 5.37 est valide pour **tous** les corps Henséliens de caractéristique 0. On peut aussi montrer que les corps algébriquement clos, les corps réels clos, et les corps pseudo-finis (ultraproduits de corps finis) sont algébriquement bornés. Voir l'article de L. van den Dries, *Dimension of definable sets, algebraic boundedness and Henselian fields*, Annals of Pure and Applied Logic 45 (1989), 189 – 209.

En fait la définition que je donne n'est pas celle donnée par Van den Dries dans son article. Il parle de "structure algébriquement bornée" : il s'agit d'un anneau intègre $D$, tel que $\mathrm{Th}_{\mathcal{L}(D)}(D)$ soit algébriquement bornée, $\mathcal{L}$ étant un langage contenant celui des anneaux.

# 6 Un peu d'intégration $p$-adique

## 6.1 La mesure

**6.1. Mesures de Haar sur un corps local**. Soit $K$ une extension finie de $\mathbb{Q}_p$. A l'aide de la valuation, nous avons défini une topologie sur $K$, dont les ouverts de base sont les boules ouvertes $B(a; \gamma)$. On remarque que comme le groupe de valeurs est discret, et le corps résiduel est fini, alors le (fermé) $\mathcal{O}_K$ est compact.

En effet, nous avons vu que, si $\pi$ est une uniformisante (c'est-à-dire, $v(\pi)$ est le plus petit élément positif du groupe de valeurs), et si $S$ est un système de représentants du corps résiduel, alors tout élément de $\mathcal{O}_K$ s'écrit de façon unique $\sum_{i=0}^{\infty} a_i \pi^i$. L'application qui à un élément $a$ de $\mathcal{O}_K$ associe la suite $(a_i)_i$ telle que $a = \sum a_i \pi^i$, est un homéomorphisme entre $\mathcal{O}_K$ et l'espace compact $S^{\mathbb{N}}$, $S$ étant muni de la topologie discrète. (Ce résultat n'est donc vrai que parce que le corps résiduel de $K$ est fini).

On considère la $\sigma$-algèbre $\mathcal{B}$ engendrée par tous les compacts de $K$ (close par complémentaires et unions dénombrables). Alors il existe une (unique) fonction $\mu : \mathcal{B} \to \mathbb{R}$ qui satisfait les propriétés suivantes :

(i) $\mu(\mathcal{O}_K) = 1$, $\mu(\emptyset) = 0$.

(ii) Si $B_i$, $i \in \mathbb{N}$, est une suite d'éléments de $\mathcal{B}$ qui sont deux-à-deux disjoints, alors $\mu(\bigcup_{i\in\mathbb{N}} B_i) = \sum_{i=0}^{\infty} \mu(B_i)$.

(iii) Si $B \in \mathcal{B}$ et $a \in K$, alors $\mu(a + B) = \mu(B)$.

(iv) Pour tout $B \in \mathcal{B}$ et $\varepsilon > 0$, il existe un ouvert $U$ et un fermé $C$ tels que $C \subseteq B \subseteq U$ et $\mu(U \setminus C) < \varepsilon$.

On étend la $\sigma$-algèbre $\mathcal{B}$ à la $\sigma$-algèbre $\hat{\mathcal{B}}$ engendrée par $\mathcal{B}$ et par tous les sous-ensembles $A$ de $K$ qui sont contenus dans un $C \in \mathcal{B}$ avec $\mu(C) = 0$. On étend $\mu$ à $\hat{\mathcal{B}}$, la fonction obtenue est appelée la *mesure de Haar normalisée sur $K$*. Elle est uniquement déterminée par les propriétés (i) – (iv).

**6.2. Quelques propriétés**. On voit tout de suite que si $q = p^f$ est la taille du corps résiduel, alors $\mu(\mathcal{M}_K) = 1/q$ : en effet, $\mathcal{O}_K$ est la réunion disjointe des ouverts $\mathcal{M}_K$ et $i + \mathcal{M}_K$, où $i$ parcourt l'ensemble des racines primitive $(q-1)$-ièmes de l'unité. Similairement on a $\mu(\mathcal{M}_K^n) = 1/q^n$, et $\mu(B(a;n)) = q^{-n-1}$, $\mu(\bar{B}(a;n)) = q^{-n}$.

On vérifie, grâce à la $\sigma$-additivité, que si $A_i$, $i \in \mathbb{N}$, est une suite croissante d'éléments de $\hat{\mathcal{B}}$, alors $\mu(\bigcup_i A_i) = \lim_i \mu(A_i)$, et pareillement si $A_i$ est une suite décroissante.

Sur $K^m$ on peut aussi définir une mesure, en prenant le produit de la mesure $\mu$ sur $K$. Cela nous permet alors d'intégrer, en se servant des valeurs absolues $p$-adiques introduites dans le chapitre 1. Si $v$ est la valuation sur $K$, et $e = v(p)$, alors on définit $|x|_p = p^{-v(x)/e}$ (on aura alors $|p|_p = p^{-1}$). Si $f : K^n \to K$ est une fonction et $B \in \hat{\mathcal{B}}$, l'expression $\int_B |f(x)|_p d\mu$ aura alors un sens (ou n'en aura pas). Comme avec l'intégrale de Lebesgue, on partitionne $B$ en des ensembles mesurables de plus en plus petits, et on regarde les sommes de la forme $\sum |f(x_C)|_p \mu(C)$ où $C$ parcourt l'ensemble des membres de la partition, et $|f(x_C)|_p = \min\{|f(x)|_p \mid x \in C\}$. Puis on définit $\int_B |f(x)|_p d\mu_x$ comme étant la limite supérieure de toutes ces sommes. Si $\mu(B)$ est fini et $|f(x)|_p$ est bornée sur $B$, alors ce nombre sera fini.

Denef utilise la notation $|dx|_p$ au lieu de $d\mu_x$, et j'utiliserai plutôt sa notation.

**Remarque**. Notons que si des égalités polynômiales non triviales apparaissent dans la définition de $C$, alors sa mesure est nulle. Nous pourrons donc négliger $C$ quand nous intègrerons sur $S$.

## 6.2 Les deux séries de Poincaré

**6.3.** Soient $f_1(X), \ldots, f_r(X) \in \mathbb{Z}_p[X]$ ($X$ un $m$-uplet). Pour $n \in \mathbb{N}$, soit $\tilde{N}_n$ le nombre d'éléments de l'ensemble $\{a \in \mathbb{Z}_p^m \mid v(f_i(a)) \geq n \text{ pour } i = 1, \ldots, r\}$, et soit $N_n$ le nombre d'éléments de l'ensemble $\{a \in \mathbb{Z}_p^m \mid \exists b \in \mathbb{Z}_p^m \ f_1(b) = \cdots = f_r(b) = 0 \wedge v(b-a) \geq n\}$. [Si $a = (a_1, \ldots, a_m)$ et $b = (b_1, \ldots, b_m)$, $v(b-a) \geq n$ veut dire : $v(b_i - a_i) \geq n$ pour tout $i = 1, \ldots, m$.] A ces deux suites de nombres nous associons les deux séries

$$\tilde{P}(T) = \sum_{n=0}^{\infty} \tilde{N}_n T^n \quad \text{et} \quad P(T) = \sum_{i=0}^{\infty} N_n T^n.$$

Le nombre $\tilde{N}_n$ compte donc les solutions du système $\bigwedge_i f_i(x) = 0$ dans $(\mathbb{Z}/p^n\mathbb{Z})^m$, tandis que $N_n$ nous donne la cardinalité de l'image modulo $p^n$ des solution (dans $\mathbb{Z}_p^m$) de $\bigwedge_i f_i(x) = 0$. Igusa et Meuser ont montré que $\tilde{P}(T)$ est une fonction rationnelle de $T$ (c'est-à-dire, est dans $\mathbb{Q}(T)$). Denef donne une preuve de la rationalité de $P(T)$ et de $\tilde{P}(T)$, en prouvant un résultat plus général. La remarque fondamentale qui lui permet de montrer ces résultats, est la suivante :

**6.4. Lemme**. Soient $f_1(X), \ldots, f_r(X) \in \mathbb{Z}_p[X]$, et $P(T)$ la série qui leur est associée. Soit

$$D = \{(x, w) \in \mathbb{Z}_p^{m+1} \mid \exists y \in \mathbb{Z}_p^m \; v(x-y) \geq v(w), f_1(y) = \cdots = f_r(y) = 0\}.$$

Pour chaque $s \in \mathbb{R}^{s>0}$, considérons

$$I(s) = \int_D |w|_p^s |dx||dw|.$$

Alors

$$I(s) = \frac{p-1}{p} P(p^{-m-1}p^{-s}).$$

*Démonstration.*

$$\begin{aligned}
I(s) &= \sum_{n=0}^{\infty} \int_{D, v(w)=n} p^{-ns} |dx||dw| \\
&= \sum_{n=0}^{\infty} p^{-ns} \int_{(x,p^n)\in D, v(w)=n} |dx||dw| \\
&= \sum_{n=0}^{\infty} p^{-ns} \Big(\int_{(x,p^n)\in D} |dx|\Big)\Big(\int_{v(w)=n} |dw|\Big) \\
&= \sum_{n=0}^{\infty} p^{-ns} \frac{N_n}{p^{nm}} \left(\frac{1}{p^n} - \frac{1}{p^{n+1}}\right) \\
&= \frac{p-1}{p} \sum_{n=0}^{\infty} N_n (p^{-s}p^{-m-1})^n.
\end{aligned}$$

Pour prouver le résultat de Denef, il suffira donc de montrer le résultat suivant :

**6.5. Théorème**. Soit $S \subset \mathbb{Q}_p^m$ un ensemble définissable, qui est contenu dans un compact, et soit $h : S \to \mathbb{Q}_p$ une fonction définissable, telle que $|h(x)|_p$ soit borné sur $S$. Soit $e \in \mathbb{N}^{\geq 1}$ tel que pour tout $x \in S$, $v(h(x))$ soit divisible par $e$ (ou bien égale $\infty$). Alors

$$Z(s) = \int_D |h(x)|^{s/e} |dx|$$

est une fonction rationnelle de $p^{-s}$ (pour $s \in \mathbb{R}^{>0}$). C'est-à-dire, il existe $Q(T) \in \mathbb{Q}(T)$ tel que $Z(s) = Q(p^{-s})$ pour tout $s \in \mathbb{R}^{>0}$.

En effet, nous avons une série $P(T)$ (à coefficients des entiers non négatifs) et une fonction rationnelle $Q(T)$ qui sont égales sur l'intervalle ouvert $(0, 1)$ (notation anglaise pour $]0, 1[$). Elles sont donc égales (dans $\mathbb{Q}((T))$).

**6.6.** Le théorème 6.5 permet aussi d'obtenir la rationalité de la série $\tilde{P}(T)$. Plus généralement, soit $\varphi(x)$ une formule du langage des anneaux ($x$ un $m$-uplet) augmenté par des symboles pour les éléments de $\mathbb{Z}_p$, et pour chaque $n \geq 0$ définissons

$N_{\varphi,n}$ : la cardinalité de l'image par la projection naturelle $\mathbb{Z}_p^m \to (\mathbb{Z}/p^n\mathbb{Z})^m$ de l'ensemble $\{a \in \mathbb{Z}_p^m \mid \mathbb{Z}_p \models \varphi(a)\}$,

$\tilde{N}_{\varphi,m}$ : la cardinalité de l'ensemble $\{a \in (\mathbb{Z}/p^n\mathbb{Z})^m \mid \mathbb{Z}/p^n\mathbb{Z} \models \varphi(a)\}$,

puis posons

$$P_\varphi(T) = \sum_{n=0}^{\infty} N_{\varphi,n} T^n, \qquad \tilde{P}_\varphi(T) = \sum_{n=0}^{\infty} \tilde{N}_{\varphi,n} T^n.$$

[Pour la définition de $\tilde{N}_{\varphi,n}$, nous interprétons les constantes du langage par leur image dans $\mathbb{Z}/p^n\mathbb{Z}$.]

Soit $\tilde{\varphi}(x,w)$ la formule obtenue à partir de $\varphi(x)$ en remplaçant chaque instance du symbole "=" par "congru modulo $p^{v(w)}$", c'est-à-dire, la sous-formule $f(x) = 0$, $f(X) \in \mathbb{Z}_p[X]$, sera remplacée par $v(f(x)) \geq v(w)$, et la formule $f(X) \neq 0$ par $v(f(x)) < v(w)$.

Considérons les ensembles

$$\begin{aligned} D_\varphi &= \{(x,w) \in \mathbb{Z}_p^{m+1} \mid \mathbb{Z}_p \models \exists y\ \varphi(y) \wedge v(x-y) \geq v(w)\} \\ \tilde{D}_\varphi &= \{(x,w) \in \mathbb{Z}_p^{m+1} \mid \mathbb{Z}_p \models \tilde{\varphi}(x,w)\}. \end{aligned}$$

Comme dans le lemme 6.4, on montre alors que

$$\begin{aligned} \int_{D_\varphi} |w|^s |dx||dw| &= \frac{p-1}{p} P_\varphi(p^{m-1}p^{-s}), \\ \int_{\tilde{D}_\varphi} |w|^s |dx||dw| &= \frac{p-1}{p} \tilde{P}_\varphi(p^{m-1}p^{-s}). \end{aligned}$$

## 6.3 Exemples de calcul d'intégrales $p$-adiques

**6.7. Un exemple simple**. Soit $p > 2$. On considère l'ensemble $S$ des carrés de $\mathbb{Z}_p$, et la fonction $h(x) = x^3$. Calculons

$$\int_S |h(x)||dx|.$$

Nous savons qu'un élément non nul $a \in \mathbb{Z}_p$ est un carré si et seulement si $v(a) = n \in 2\mathbb{Z}$, et $p^{-n}a$ est un carré modulo $p$. Combien y a-t-il de carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$? Comme $p$ est impair, 2 divise $p-1$, et donc l'homomorphisme multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, $x \mapsto x^2$, a un noyau de taille 2. La cardinalité de son image est donc $(p-1)/2$.

Nous avons donc

$$\begin{aligned} \int_S |x^3|_p |dx| &= \sum_{n=0}^{\infty} \frac{p-1}{2p} p^{-8n} \\ &= \frac{p-1}{2p} \frac{1}{1-p^{-8}}. \end{aligned}$$

En effet, nous avons $\mu(S \cap v(x) = 2n) = \mu(S \cap v(x) = 0)p^{-2n} = \frac{p-1}{2p}p^{-2n}$. Si $a \in S$ et $v(a) = 2n$, alors $|h(a)|_p = p^{-6n}$. Cela donne le résultat. Notons que nous avons enlevé l'élément 0 de $S$ : $\mu(\{0\}) = 0$.

Supposons maintenant que $p = 2$, et soient $S$ et $h$ définis comme ci-dessus. Nous savons que $a \in S$ si et seulement si $v(a) = n \in 2\mathbb{Z}$ et l'image de $p^{-n}a$ dans $\mathbb{Z}/8\mathbb{Z}$ est un carré. Comme $v(p^{-n}a) = 0$, cette image sera en fait un élément de $(\mathbb{Z}/8\mathbb{Z})^\times$, les éléments inversibles de l'anneau $\mathbb{Z}/8\mathbb{Z}$. Mais on calcule facilement que 1 est le seul carré de $(\mathbb{Z}/8\mathbb{Z})^\times$, car $3^2 = 9 \equiv 1\ (8)$. Nous obtenons donc $\mu(S \cap v(a) = 0) = 1/8$, puis

$$\int_S |h(x)|_p |dx| = \frac{1}{8}\sum_{n=0}^{\infty} 2^{-8n} = \frac{1}{8}\frac{1}{1-2^{-8}}.$$

**6.8. Remarque de calcul**. A part le fait que la mesure est invariante par translation, nous utilisons aussi la propriété suivante : soit $S \subset \mathbb{Q}_p$ un ensemble mesurable et $n \in \mathbb{Z}$. Alors $\mu(p^n B) = p^{-n}\mu(B)$. Ce résultat se généralise aux sous-ensembles mesurables de $\mathbb{Q}_p^m$, mais il ne faut pas oublier de tenir compte du $m$ : si $S \subset \mathbb{Q}_p^m$, alors $\mu(p^n S) = p^{-nm}\mu(S)$.

**6.9. Deuxième exemple, un peu plus compliqué**. Nous supposons $p > 2$. Soit $S$ l'ensemble des carrés de $\mathbb{Z}_p$, et $h(x) = x + 1$. Si $v(a) > 0$, alors $|h(a)|_p = 1$ (car $v(a+1) = v(1) = 0$). Si $v(a) = 0$, deux cas sont possibles : $|h(a)|_p = 1$ si $v(a+1) = 0$ ; et $|h(a)|_p < 1$ sinon.

Si $-1$ n'est pas un carré modulo $p$, alors pour tout $a \in S$ nous avons $|h(a)|_p = 1$. Or, $-1$ est un carré modulo $p$ si et seulement si $p \equiv 1\ (4)$. Nous obtenons donc, si $p \equiv 3\ (4)$, alors $\int_S |h(x)|_p |dx| = \mu(S) = \frac{p}{2(p+1)}$.

Supposons maintenant que $p \equiv 1\ (4)$. Nous allons partitionner $S$ en deux morceaux, $S_1$ et $S_2$, avec $S_2 = S \cap B(-1;0)$, et $S_1 = S \setminus S_2$. On s'aperçoit que en fait $B(-1;0)$ est contenu dans $S$ : soit $a$ une racine carrée de $-1$, et $b \in B(-1;0)$. Alors l'équation $X^2 - b$ a une racine résiduelle simple ($a$, car $p > 2$), et a donc une racine dans $\mathbb{Z}_p$. Nous avons alors, en faisant un changement de variable :

$$\begin{aligned}
\int_{x \in B(-1;0)} |x+1|_p |dx| &= \int_{y \in B(0;0)} |y|_p |dy| \\
&= \sum_{n=1}^{\infty} \frac{p-1}{p^{n+1}} p^{-n} \\
&= \frac{p-1}{p^3}\sum_{n=0}^{\infty} p^{-2n} \\
&= \frac{p-1}{p^3(1-p^{-2})},
\end{aligned}$$

d'où (puisque $\mu(B(-1;0) = p^{-1})$),

$$\int_S |h(x)|_p |dx| = \mu(S) - \frac{1}{p} + \frac{p-1}{p^3(1-p^{-2})} = \frac{p}{2(p+1)} - \frac{1}{p} + \frac{p-1}{p^3(1-p^{-2})}.$$

**6.10.** Plus généralement, toujours avec $x$ une seule variable. Supposons que l'on puisse trouver une partition de notre domaine $S$ en cellules $C$ telles que pour tout $x \in C$, on ait $v(h(x)) = \alpha v(x-c) + \beta$, où $\alpha, \beta \in \mathbb{Q}$, $c \in \mathbb{Z}_p$. Supposons de plus que $C$ soit définie de la façon suivante : $a \in C$ si et seulement si $v(a) \equiv_n i$ et l'image de $p^{-v(a)}a$ dans $\mathbb{Z}/p^m\mathbb{Z}$ satisfait une certaine formule $\varphi$ dans $\mathbb{Z}/p^m\mathbb{Z}$. Soit $A$ la cardinalité de l'ensemble des éléments de $\mathbb{Z}/p^m\mathbb{Z}$ satisfaisant $\varphi$. Alors

$$\mu(C \cap v(x) = k) = \begin{cases} Ap^{-m-k} & \text{si } k \equiv i \ (n), \\ = 0 & \text{sinon,} \end{cases}$$

et cela donne

$$\int_C |h(x)|^s |dx| = \sum_{j=0}^{\infty} Ap^{-m-i-jn} p^{-\beta s} |x-c|_p^{\alpha s}.$$

Si $c \notin C$, alors nous aurons, pour $x \in C$, $|x-c|_p = \max\{|x|_p, |c|_p\}$, et donc notre intégrale se divisera en deux morceaux facilement calculables. Si par contre $c \in C$, alors il faudra subdiviser $C \cap v(x) = v(c)$ en sous-ensembles sur lesquels la valeur de $|x-c|_p$ sera constante, et dont le volume est facilement calculable, donc de préférence, des boules.

Cela donne une idée de la stratégie pour calculer une intégrale sur un sous-ensemble définissable $S$ de $\mathbb{Z}_p$. Tout d'abord il faut montrer qu'il existe une partition finie de $S$ telle que sur chaque morceau, la fonction $|h(x)|_p$ soit donnée par une fonction $p^{-\beta}|x-c|_p^{\alpha}$ pour un $c \in \mathbb{Z}_p$. Puis subdiviser chaque morceau en un nombre fini d'ensembles définissables de la forme ci-dessus. De plus, nous voulons que ces constructions soient suffisamment uniformes pour que nous puissions appliquer une induction sur le nombre de variables et montrer le résultat pour des sous-ensembles définissables de $\mathbb{Z}_p^n$.

## 6.4 La preuve de Denef

**6.11. Définition**. Soit $S$ un sous-ensemble définissable de $\mathbb{Q}_p^m$, et $\theta : S \to \mathbb{Z} \cup \{\infty\}$ une fonction. Alors $\theta$ est *simple* s'il existe une partition finie de $S$ en sous-ensembles définissables $A$, telle que pour chaque $A$, il existe des polynômes $f[X], g[X] \in \mathbb{Q}_p[X]$ et un entier $e > 0$ tels que pour tout $x \in A$,

$$\theta(x) = \frac{1}{e}(v(f(x)) - v(g(x))).$$

**Théorème**. Soit $S \subset \mathbb{Q}_p^{m+1}$ un ensemble définissable, et supposons que pour tout $a \in \mathbb{Q}_p^m$, l'ensemble $\{v(y) \mid (a,y) \in S\}$ a au plus un élément, que nous noterons $\theta(a)$. Alors la fonction qui à un $m$-uplet $a$ de $S' = \{x \in \mathbb{Q}_p^m \mid \exists y \ (x,y) \in S\}$ associe $\theta(a)$, est simple.

*Démonstration.* Soient $Z = \{x \in \mathbb{Q}_p^m \mid (x,0) \in S\}$, et $Z' = S' \setminus Z$. Sur $Z$, $\theta(x)$ égale $\infty$. Observons maintenant que puisque $\mathrm{Th}(\mathbb{Q}_p)$ a des fonctions de Skolem définissables, nous pouvons supposer que pour tout $a \in \mathbb{Q}_p^m$, $|S(a)| \leq 1$.

Par le lemme 5.36, nous pouvons écrire $Z'$ comme une union disjointe d'ensembles définissables $C$, chaque ensemble $C$ étant défini par une conjonction d'équations en $x, t$ et une conjonction

de formules de la forme $P_n^*(g(x,t))$, $g(X,T) \in \mathbb{Q}_p[X,T]$. En regroupant les sous-formules qui ne dépendent pas de $t$, $C$ sera donc défini par une formule

$$\psi(x) \wedge \bigwedge_i (f_i(x,t) = 0) \wedge \bigwedge_j P_n^*(g_j(x,t)),$$

où $\psi(x) \in \mathcal{L}_{\mathrm{Mac}}$ a ses variables libres dans $x$, et les $f_i$, $g_j$ sont des polynômes à coefficients dans $\mathbb{Q}_p$. En fait, en les multipliant par des puissances de $p$, on peut supposer que leurs coefficients sont dans $\mathbb{Z}_p$. Nous pouvons aussi supposer que $\psi(x)$ entraîne que les polynômes $f_i(x,T)$ ne sont pas identiquement nuls.

On remarque ensuite que comme pour tout $m$-uplet $a$, $|C(a)| \leq 1$, nécessairement notre formule contiendra une équation, par l'assertion faite en 5.37. Passant à un ensemble définissable $C$ plus petit si nécéssaire, il existe donc $f(X,T) \in \mathbb{Z}_p[X,T]$ tel que $\varphi(a,t)$ entraine $f(a,t) = 0$, et $f(a,T)$ n'est pas identiquement nul. Ecrivons

$$f(X,T) = \sum_{i=0}^{m} c_i(X)T^i.$$

Alors $f(x,t) = 0$ entraine qu'il existe $i < j$ tels que $v(c_i(x)) + iv(t) = v(c_j(x)) + jv(t)$, c'est-à-dire, $v(t) \in \{\frac{v(c_i(x))-v(c_j(x))}{j-i} \mid 0 \leq i < j \leq m\}$. On partitionne donc $C$ en des sous-ensembles $C_{i,j}$, $0 \leq i < j \leq m$, avec

$$C_{i,j} = \{(x,t) \in C \mid v(t) = \frac{v(c_i(x)) - v(c_j(x))}{j-i}\}.$$

Cela nous donne le résultat.

**6.12.** Voici un petit lemme que nous avons déja implicitement montré plusieurs fois, mais je crois que nous ne l'avons jamais formellement énoncé. Les hypothèses du lemme sont en particulier vérifiées si la caractéristique résiduelle de $K$ est nulle ; si la caractéristique résiduelle est $p > 0$, alors elles sont vérifiées si le groupe de valeurs de $K$ a un plus petit élément positif, et $v(p)$ est un multiple entier de ce plus petit élément (cf théorèmes 3.26 et 3.27).

**Lemme**. Soit $(K,v)$ un corps Hensélien, et $L$ une extension algébrique finie de $K$. Supposons que $[L:K] = n$ soit le produit du degré de ramification et du degré inertiel. Alors il existe une base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ du $K$-espace vectoriel $L$ tel que pour tout $c_1, \ldots, c_n \in K$, $v(\sum_{i=1}^n c_i\alpha_i) = \min_i v(c_i\alpha_i)$.

*Démonstration.* Soient $e = e(L/K)$ et $f = f(L/K)$. La démonstration du lemme 3.7 montre que si $a_1, \ldots, a_f \in L$ sont tels que $\operatorname{res} a_1, \ldots, \operatorname{res} a_f$ forment une base du $k_K$-espace vectoriel $k_L$, et si $b_1, \ldots, b_e \in L$ sont tels que $\Gamma_L$ est l'union disjointe des cosets $v(b_i) + \Gamma_K$ de $\Gamma_K$ dans $\Gamma_L$, alors $\{a_ib_j \mid 1 \leq i \leq f,\ 1 \leq j \leq e\}$ forme une base du $K$-espace vectoriel $L$, et satisfait à la condition demandée.

**6.13. Lemme**. Soit $f(X,T) \in \mathbb{Q}_p[X,T]$, $X = (X_1, \ldots, X_m)$, $T$ une seule variable, et soit $n \in \mathbb{N}^{>0}$. Il existe une partition finie de $\mathbb{Q}_p^{m+1}$ en sous-ensembles $A$ de la forme

$$A = \{(x,t) \in \mathbb{Q}_p^{m+1} \mid x \in C \text{ et } v(t - c_j(x)) \prec_{\ell,j} v(a_{\ell,j}(x)),\ j \in S,\ \ell \in S_j\}, \tag{1}$$

où $C \subset \mathbb{Q}_p^m$ est définissable, $\prec_{i,j}$ dénote $\leq$, $\geq$, $>$ ou $<$, $S$ et les $S_j$ sont finis, et $c_j(x), a_{\ell,j}(x)$ sont des fonctions définissables $\mathbb{Q}_p^m \to \mathbb{Q}_p$, et qui sont tels que, pour tout $(x,t) \in A$, on a

$$f(x,t) = u(x,t)^n h(x) \prod_{j \in S} (t - c_j(x))^{e_j}, \tag{2}$$

avec $v(u(x,t)) = 0$, $h(x)$ une fonction définissable de $\mathbb{Q}_p^m$ dans $\mathbb{Q}_p$, $u(x,t)$ une fonction définissable de $\mathbb{Q}_p^{m+1}$ dans $\mathbb{Q}_p$, et $e_j \in \mathbb{N}$.

*Démonstration.* Ecrivons $f(X,T) = \sum_i a_i(X)T^i$. Nous pouvons partitionner $\mathbb{Q}_p^m$ en sous-ensembles définissables sur lesquels le degré de $f(x,T)$ en $T$ est constant. Nous fixons ce degré, $d$, travaillons sur $C \times \mathbb{Q}_p$, et supposons que sur $C \subset \mathbb{Q}_p^m$, le polynôme $f(x,T)$ est constant de degré $d$. Si $d = 0$ ou $d = 1$, il n'y a rien à montrer.

On sait que $\mathbb{Q}_p$ n'a qu'un nombre fini d'extensions de degré $\leq d$, et on prend pour $K$ le corps composite de toutes ces extensions. Pour tout $x \in C$, les racines $\beta_1(x), \ldots, \beta_d(x)$ de $f(x,T)$ seront donc dans $K$.

On choisit une base de $K$ sur $\mathbb{Q}_p$, $\alpha_1 = 1, \alpha_2, \ldots, \alpha_N$ ($N = [K : \mathbb{Q}_p]$) telle que si $i \geq 2$ alors $0 < v(\alpha_i) \leq 1 = v(p)$, et si $b_1, \ldots, b_N \in \mathbb{Q}_p$, alors $v(\sum_i b_i\alpha_i) = \min_i\{v(b_i\alpha_i)\}$. [C'est possible en utilisant le lemme 6.12 : on choisit $a_1, \ldots, a_f$ comme dans le lemme et avec $a_1 = 1$ ; on remarque que $\Gamma_K$ est engendré par un élément $v(\pi)$ avec $ev(\pi) = v(p) = 1$, et on prend $\{1, \pi, \ldots, \pi^{e-1}\}$ ; les éléments $a_i\pi^j$ forment donc une base de $K$ sur $\mathbb{Q}_p$ satisfaisant la conclusion du lemme 6.12. On prend maintenant comme base $\{1, pa_2, \ldots, pa_f, a_i\pi^j \mid 1 \leq i \leq f, 0 < j < e\}$ ; elle satisfait toujours la conclusion de 6.12]. Notons que nous avons alors les propriétés suivantes :

> 1 est le seul indice $i$ tel que $v(\alpha_i) = 0$ ; il existe $f - 1$ indices $i$ avec $v(\alpha_i) = 1$ ; si $\gamma$ est un multiple de $1/e$ compris strictement entre 0 et 1, alors il existe $f$ indices $i$ tels que $v(\alpha_i) = \gamma$.

Le groupe additif du corps $K$ est tout simplement l'espace vectoriel $\oplus_i \alpha_i\mathbb{Q}_p$ ; on peut définir, sur $\mathbb{Q}_p^N$ à l'aide de polynômes sur $\mathbb{Q}_p$, une loi $*$ telle que $(\mathbb{Q}_p^N, +, *) \simeq (K, +, \cdot)$, l'isomorphisme étant donné par $(a_1, \ldots, a_N) \mapsto \sum_i a_i\alpha_i$. Nous gardons $v(p) = 1$, et utiliserons ainsi la valuation $p$-adique normalisée sur $K$.

Puisque la théorie de $\mathbb{Q}_p$ a des fonctions de Skolem définissables, cela entraîne qu'il existe des fonctions définissables $b_{i,j} : \mathbb{Q}_p^m \to \mathbb{Q}_p$ telles que pour tout $a \in C$, les éléments $\beta_j(a) = \sum_{i=1}^N b_{i,j}(a)\alpha_i$, $j = 1, \ldots, d$, sont les racines de $f(a,T) = 0$. Pour tout $t \in \mathbb{Q}_p$, on aura donc

$$f(a,t) = a_d(a) \prod_{j=1}^{d} (t - \beta_j(a)).$$

Soit $\lambda = 2v(n) + 1$. Nous utiliserons sans cesse les trois conséquences suivantes de l'exercice 3.15 :

– si $v(u) \geq \lambda$, alors $P_n^*(1+u)$ ;

– si $v(b) \geq v(a) + \lambda$, alors il existe $u \in \mathbb{Q}_p$ tel que $v(u) = 0$ et $a + b = au^n$ [car $v(b/a) \geq \lambda$] ;

– si $a \in \mathbb{Q}_p$, $a \neq 0$, et $u \in \mathbb{Q}_p$ est tel que $v(a-u^n) \geq v(a)+\lambda$, alors $P_n^*(a)$.

Nous partitionnons maintenant $C \times \mathbb{Q}_p$ en sous-ensembles définissables $A$ (de la forme voulue), tels que sur chaque $A$, nous avons une partition $I_1 \cup I_2 \cup I_3$ de $\{1,\ldots,d\}$ et une application $i : I_2 \to \{2,\ldots,N\}$, avec, pour tout $a \in A$,

$$\begin{aligned} |t-\beta_j(a)|_p &= |t-b_{1,j}(a)|_p \neq 0, \quad \text{si } j \in I_1, \\ &= |b_{i(j),j}(a)\alpha_{i(j)}|_p \text{ si } j \in I_2, \text{ avec } i(j) \geq 2, \\ &= 0 \text{ si } j \in I_3. \end{aligned}$$

On exige de plus que si $j \in I_1$, alors $|t-\beta_i(a)|_p < |b_{i,j}(a)\alpha_i|_p$ pour tout $i \geq 2$. Ces ensembles sont bien de la forme voulue : la condition $j \in I_1$ s'exprime en disant $v(t-b_{1,j}(a)) < v(b_{i,j}(a))+v(\alpha_i)$ pour $i \geq 2$ (l'inégalité stricte est nécéssaire pour que les fonctions de l'équation (8) ci-dessous prennent leurs valeurs dans $\mathbb{Z}_p$) ; la condition $j \in I_2$ s'exprime en disant que nous avons $v(b_{i(j),j}(a))+v(\alpha_{i(j)}) \leq v(b_{k,j}(a))+v(\alpha_k)$ pour $k \neq i(j), 1$ et $v(b_{i(j),j}(a))+v(\alpha_{i(j)}) \leq v(t-b_{1,j}(a))$ ; et la condition $j \in I_3$ s'exprime en disant que $v(t-b_{1,j}(a)), v(b_{2,j}(a)), \ldots, v(b_{N,j}(a)) \geq v(0)$.

Si $I_3 \neq \emptyset$, alors pour tout $(a,t) \in A$, nous avons $f(a,t) = 0$, et (2) est évident. Nous pouvons donc supposer que $I_3 = \emptyset$. Fixons un tel $A$, avec $I_1$ et $I_2$ les ensembles associés, ainsi que la fonction $i$ définie sur $I_2$. Si $(a,t) \in A$ on peut écrire

$$f(a,t) = a_d(a) \prod_{j \in I_1} (t-b_{1,j}(a)) \prod_{j \in I_2} b_{i(j),j}(a) \prod_j C_j(a,t),$$

où

$$C_j(a,t) = \begin{cases} (t-\beta_j(a))(t-b_{1,j}(a))^{-1} & \text{si } j \in I_1, \\ (t-\beta_j(a))b_{i(j),j}(a)^{-1} & \text{si } j \in I_2. \end{cases}$$

Notons que si $j \in I_1$, alors $v(C_j(a,t)) = 0$ ; si $j \in I_2$, alors $v(C_j(a,t)) = v(\alpha_{i(j)})$. Si $C(a,t) = \prod_j C_j(a,t)$, nous avons donc $0 \leq v(C(a,t)) \leq d$.

Nous regardons maintenant les classes modulo $p^{\lambda+d}$ des éléments

$$\frac{b_{i,j}(a)}{t-b_{1,j}(a)}, \qquad j \in I_1,\ 2 \leq i \leq N \tag{8}$$

et

$$\frac{t-b_{1,j}(a)}{b_{i(j),j}(a)}, \quad \frac{b_{i,j}(a)}{b_{i(j),j}(a)}, \qquad j \in I_2,\ 1 \leq i \leq N. \tag{9}$$

Notons que les conditions sur les éléments de $J_1$, ainsi que la façon dont sont définis les éléments $\alpha_i$, entraînent que ces éléments sont dans $\mathbb{Z}_p$.

Nous partitionnons $A$ en des sous-ensembles définissables $B$ de telle façon que les images de toutes ces fonctions dans $\mathbb{Z}_p/p^{\lambda+d}\mathbb{Z}$ soient constantes. Soient $(a,t)$, $(a',t')$ dans un même ensemble $B$ de la partition. Alors nous avons

$$C_j(a,t)-C_j(a',t') = \begin{cases} \sum_{i=2}^N \left(\frac{b_{i,j}(a)}{t-b_{1,j}(a)} - \frac{b_{i,j}(a')}{t'-b_{1,j}(a')}\right)\alpha_i & \text{si } j \in I_1, \\ \frac{t-b_{1,j}(a)}{b_{i(j),j}(a)} - \frac{t'-b_{1,j}(a')}{b_{i(j),j}(a')} + \sum_{i=2}^N \left(\frac{b_{i,j}(a)}{b_{i(j),j}(a)} - \frac{b_{i,j}(a')}{b_{i(j),j}(a')}\right)\alpha_i & \text{si } j \in I_2, \end{cases}$$

ce qui entraîne $v(C_j(a,t) - C_j(a',t')) \geq \lambda + d$. L'image de $C(a,t)$ dans $\mathbb{Z}_p/p^{\lambda+d}\mathbb{Z}$ sera donc constante, égale à celle d'un entier $g$, et nous aurons $v(g) \leq d$. Puisque $v(C(a,t)-g) \geq v(g)+\lambda$, nous aurons donc $P_n^*(g^{-1}C(a,t))$.

Si nous définissons $h(x) = g\prod_{j\in I_2} b_{i(j),j}(x)$, et $u(x,t)$ l'unique racine $n$-ième de $g^{-1}C(x,t)$ congrue à 1 modulo $p^\lambda$, nous obtenons une équation comme dans (2).

Cependant, il faut vérifier que les sous-ensembles définissables $B$ sont bien de la forme imposée par (1).

Si $g$ est un entier et $j \in I_2$, alors on a

$$v\left(\frac{t-b_{1,j}(a)}{b_{i(j),j}(a)} - g\right) \geq \lambda + d \iff v(t - b_{1,j}(a) - gb_{i(j),j}(a)) \geq \lambda + d + v(b_{i(j),j}(a)).$$

La condition $v\big(\frac{b_{i,j}(a)}{b_{i(j),j}(a)} - g\big) \geq \lambda + d$ ne porte que sur $a$ et est donc de la forme voulue.

Si $g$ est un entier et $j \in I_1$, alors, en multipliant par $-(t - b_{1,j}(a))g^{-1}$, on obtient que

$$v\left(\frac{b_{i,j}(a)}{t-b_{1,j}(a)} - g\right) \geq \lambda + d \iff v(t - b_{1,j}(a) - \frac{b_{i,j}(a)}{g}) \geq \lambda + d + v(t - b_{1,j}(a)) - v(g).$$

Comme $v(g) \leq d < \lambda + d$, la partie gauche entraîne

$$v\left(\frac{b_{i,j}(a)}{t-b_{1,j}(a)}\right) = v(g), \quad \text{c'est-à-dire, } v(t - b_{1,j}(a)) = v(b_{i,j}(a)) - v(g). \tag{11}$$

Donc, la condition voulue est équivalente à la conjonction de (11) et de

$$v\left(t - b_{1,j}(a) - \frac{b_{i,j}(a)}{g}\right) \geq \lambda + d + v(b_{i,j}(a)) - 2v(g).$$

**6.14. Théorème**. Soient $f_i(X,T) \in \mathbb{Q}_p[X,T]$, $i = 1,\ldots,r$, $T$ une seule variable, et $n$ un entier positif. Alors il existe une partition finie de $\mathbb{Q}_p^{m+1}$ en sous-ensembles $A$ de la forme

$$\{(a,t) \in \mathbb{Q}_p^{m+1} \mid a \in C,\ v(a_1(a)) \prec_1 v(t - c(a)) \prec_2 v(a_2(a))\}, \tag{1}$$

où $C$ est un sous-ensemble définissable de $\mathbb{Q}_p^m$, $\prec_1$ et $\prec_2$ sont $\leq$ ou $<$[2], les fonctions $a_1(x)$, $a_2(x)$ et $c(x)$ sont définissables : $\mathbb{Q}_p^m \to \mathbb{Q}_p$, et pour tout $(a,t) \in A$, et $i = 1.,\ldots,r$, nous avons

$$f_i(a,t) = u_i(a,t)^n h_i(a)(t - c(a))^{f_i} \tag{2},$$

avec $v(u_i(a,t)) = 0$, les fonctions $h_i$ et $u_i$ sont définissables, et $f_i \in \mathbb{N}$. Nous permettons à la condition de gauche d'être vide, c'est-à-dire, que $v(a_1(a)) = -\infty$.

*Démonstration.* Nous pouvons partitionner $\mathbb{Q}_p^{m+1}$ en des sous-ensembles $A$ de la forme donnée dans 6.13(1), et tels que la condition 6.13(2) soit vérifiée pour chaque $f_i(X,T)$. Il y a cependant plusieurs fonctions définissables $c_j(x)$ et $a_{\ell,j(x)}$ qui apparaissent, et nous n'en voulons qu'une

[2]En utilisant le fait que dans $\mathbb{Q}_p$ on a $v(a) \leq v(b) \iff v(a) < v(pb)$, on peut supposer que $\prec_1 = \prec_2 = <$.

seule fonction $c_j$, et au plus deux fonctions $a_{\ell,j}$. La dernière condition n'est pas difficile à satisfaire : étant données des conditions $\bigwedge_\ell (t - c(a)) \leq a_\ell(a)$, on peut partitionner $\mathbb{Q}_p^m$ en des sous-ensembles définissables sur lesquels le type d'ordre de la suite $(v(a_\ell(a)))_\ell$ est constant. La conjonction des conditions sera remplacée par une seule condition.

Nous allons montrer que si $c_1(x)$ et $c_2(x)$ sont des fonctions définissables $\mathbb{Q}_p^m \to \mathbb{Q}_p$, alors il existe une partition de $\mathbb{Q}_p^{m+1}$ en sous-ensembles définissables $A$ de la forme exigée par (1), faisant intervenir une fonction définissable $c(x)$, et tels que sur $A$, les fonctions $t - c_1(x)$ et $t - c_2(x)$ s'écrivent $u_i(x,t)h_i(x)(t - c(x))^{e_i}$, avec $h_i$, $u_i$, $e_i$, satisfaisant les conditions données par (2). Cela nous permettra d'éliminer les fonctions $c_j(x)$ une par une.

Tout d'abord, nous enlevons de $\mathbb{Q}_p^{m+1}$ l'ensemble $A_0$ des uplets $(a,t)$ tels que $c_1(a) = c_2(a)$. C'est un ensemble définissable de la forme donnée dans (1).

Pour simplifier les notations, nous posons $\lambda = 2v(n) + 1$, et

$$U(a) = \frac{t - c_1(a)}{c_2(a) - c_1(a)}, \qquad V(a) = p^\lambda \frac{t - c_2(a)}{c_2(a) - c_1(a)} = p^\lambda U(a) - p^\lambda.$$

Soit $A_1$ l'ensemble défini par $v(t - c_1(a)) \geq v(c_2(a) - c_1(a)) + \lambda$. Il est donc défini par $v(t - c_1(a)) \geq v(p^\lambda(c_2(a) - c_1(a)))$ et est de la forme désirée. Sur $A_1$, nous avons, comme $t - c_2(a) = t - c_1(a) - (c_2(a) - c_1(a))$, qu'il existe une fonction définissable $u(a,t)$ telle que $t - c_2(a) = -(c_2(a) - c_1(a))u(a,t)^n$, avec $v(u(a,t)) = 0$.

Soit $A_2$ l'ensemble défini par $v(t - c_1(a)) < v(c_2(a) - c_1(a)) - \lambda$. Comme ci-dessus, $A_2$ est de la forme désirée. Cette fois-ci, nous obtenons qu'il existe une fonction définissable $u(a,t)$, telle que sur $A_2$ nous avons $t - c_2(a) = u(a,t)^n(t - c_1(a))$, et $v(u(a,t)) = 0$.

Il nous reste à traiter le cas où $-\lambda \leq v(U(a)) < \lambda$, c'est-à-dire, $0 \leq v(p^\lambda U(a)) < p^{2\lambda}$. Nous allons en fait nous servir de $V(a)$.

Soit $A_3$ l'ensemble défini par $v(t - c_2(a)) \geq v(c_2(a) - c_1(a)) + 2\lambda$. Alors, comme dans le cas $A_1$, nous avons que sur $A_3$, $t - c_1(a) = (c_1(a) - c_2(a))u(a,t)^n$, avec $v(u(a,t)) = 0$.

Enfin, pour chaque entier positif $e$ inférieur à $p^{3\lambda}$ et tel que $e \not\equiv 0 \bmod p^{2\lambda}$, $e \not\equiv -p^\lambda \bmod p^{2\lambda}$, nous considérons l'ensemble $A_{4,e}$ défini par $v(V(a) - e) \geq 3\lambda$. Montrons d'abord que si $(a,t) \notin A_0 \cup A_1 \cup A_2 \cup A_3$, et si $e \in \mathbb{N}$, $e \leq p^{3\lambda}$, est tel que $v(V(a) - e) \geq 3\lambda$, alors $e$ satisfait les conditions ci-dessus.

Comme $(a,t) \notin A_3$, nous savons que $v(V(a)) < 2\lambda$, c'est-à-dire, que $v(e) < 2\lambda$, et donc $e \not\equiv 0 \bmod p^{2\lambda}$. Nous savons aussi que, modulo $p^{3\lambda}$, $p^\lambda U(a)$ est congru à un entier $e'$ qui n'est pas divisible par $p^{2\lambda}$ (puisque $(a,t) \notin A_0 \cup A_1 \cup A_2$). Donc, $p^{2\lambda}$ ne divise pas $e' = e + p^\lambda$, c'est-à-dire, $e \not\equiv -p^\lambda \bmod p^{2\lambda}$.

Certainement les $A_{4,e}$ sont deux à deux disjoints, et sont disjoints de $A_3$. D'autre part, si $(a,t) \in A_1$, alors $v(p^\lambda U(a)) \geq 2\lambda$, et donc $V(a) \equiv -p^\lambda \bmod p^{2\lambda}$, ce qui montre que $A_1$ est disjoint de $A_3$ et des $A_{4,e}$. Si $(a,t) \in A_2$, alors $v(V(a)) = v(p^\lambda U(a)) < 0$, et $A_2$ est disjoint de $A_3$ et des $A_{4,e}$. Nous avons bien une partition de $\mathbb{Q}_p^{m+1}$.

Regardons maintenant ce qui se passe sur l'ensemble $A_{4,e}$, $e$ fixé. Dans ce cas nous avons

$$0 < v(p^\lambda U(a)) < 2\lambda, \text{ et } v(p^\lambda U(a) - (e + p^\lambda)) \geq 3\lambda,$$

ce qui entraine que $p^\lambda U(a) = (e+p^\lambda)u_1(a,t)^n$ pour une fonction définissable $u_1(a,t)$ de valuation nulle sur $A_{4,e}$, et donc

$$t - c_1(a) = p^{-\lambda}(c_2(a) - c_1(a))(e + p^\lambda)u_1(a,t)^n.$$

De même, nous avons

$$0 \leq v(V(a)) < 2\lambda, \text{ et } v(V(a) - e) \geq 3\lambda,$$

ce qui entraine que $V(a) = eu_2(a,t)^n$ pour une fonction définissable $u_2(a,t)$ de valuation nulle sur $A_{4,e}$, et que

$$t - c_2(a) = p^{-\lambda}(c_2(a) - c_1(a))eu_2(a,t)^n.$$

La définition de $A_{4,e}$ est donnée par $v(p^\lambda(t - c_2(a))(c_2(a) - c_1(a))^{-1} - e) \geq 3\lambda$, c'est-à-dire, divisant par $p^\lambda(c_2(a) - c_1(a))^{-1}$, par

$$v(t - c_2(a) - p^{-\lambda}e(c_2(a) - c_1(a))) \geq 2\lambda + v(c_2(a) - c_1(a)).$$

Cela nous permet donc de trouver des ensembles définissables $A$, qui sont définis par des conditions de type $x \in C$ et $v(t - c(x)) \prec_j v(a_i(x))$, où $C$ est définissable, les $a_i$ sont des fonctions définissables, $\prec_j \in \{\leq, \geq, <, >\}$, et sur lesquels chaque $f_i$ s'écrit de la façon désirée. En partitionnant $C$, nous pouvons ensuite nous ramener à une condition de la forme $v(a_1(x)) \prec_1 v(t - c(x)) \prec_2 v(a_2(x))$, ce qui nous donne le résultat.

**6.15. Théorème**. Soient $S \subset \mathbb{Q}_p^m$ un ensemble définissable, $e \geq 1$, et $g(x) : S \to \mathbb{Q}_p$ une fonction définissable, telle que si $a \in S$ alors $v(g(a)) \in e\mathbb{Z} \cup \{\infty\}$, et $|g(x)|_p$ est bornée sur $S$. Pour $s \in \mathbb{R}^{>0}$, posons

$$Z(s) = \int_S |g(x)|_p^{s/e} |dx|_p.$$

Alors il existe $P(T) \in \mathbb{Q}(T)$ telle que $Z(s) = P(p^{-s})$.

*Démonstration.* La démonstration est par induction sur $m$. Si $m = 0$ il n'y a rien à montrer. Supposons le résultat prouvé pour $m$, et soit $S \subset \mathbb{Q}_p^{m+1}$ un ensemble définissable, et $g : S \to \mathbb{Q}_p$ satisfaisant les hypothèses du théorème. Les variables libres apparaissant dans la formule définissant $S$ seront notées $(x,t)$, $x$ un $m$-uplet, $t$ une seule variable. Tout d'abord, par le théorème 6.11, nous pouvons supposer que $g$ est une fonction rationnelle : nous remplaçons $|g(x,t)|^{1/e}$ par $|g_1(x,t)/g_2(x,t)|^{1/e'}$. Puis, en utilisant le lemme 5.36, nous pouvons supposer que $S$ est défini par une formule de la forme

$$x \in C \wedge \bigwedge_i f_i'(x,t) = 0 \wedge \bigwedge_i P_n^*(f_i(x,t))$$

où $C$ est définissable, les $f_i'$ et $f_i$ sont des polynômes sur $\mathbb{Q}_p$. Si $C_0$ est l'ensemble des $m$-uplets $a \in C$ tels que l'un des polynômes $f_i'(a,T)$ n'est pas identiquement nul, alors on aura $\mu(S \cap (C_0 \times \mathbb{Q}_p)) = 0$, et nous pouvons donc supposer que $C_0 = \emptyset$. $S$ est donc défini par

$$x \in C \wedge \bigwedge_{i=1}^{r} P_n^*(f_i(x,t)). \tag{1}$$

Nous appliquons maintenant le théorème 6.14 aux polynômes $f_1, \ldots, f_r, g_1, g_2$, et partitionnons $S$ en sous-ensembles $S \cap A$, avec $A$ comme dans 6.14(1), c'est-à-dire,

$$A = \{(x,t) \in \mathbb{Q}_p^{m+1} \mid x \in B, v(a_1(x)) \prec_1 v(t - c(x)) \prec_2 v(a_2(x))\} \tag{2}$$

pour un ensemble définissable $B$ et des fonctions définissables $a_1, a_2$ et $c$, et $\prec_i \in \{\leq, <\}$. Nous pouvons aussi supposer qu'aucune des fonctions $f_1, \ldots, f_r, g_1, g_2$ n'a de zéro dans $A$ (sinon on les enlève).

De plus, sur $S \cap A$, les polynômes $f_1, \ldots, f_r, g_1, g_2$ s'écriront comme dans 6.14(2). Notons tout de suite que pour tout $(a,t) \in S \cap A$, nous aurons

$$|g(a,t)|_p^{1/e} = |g_0(a)|_p^{1/e'} |t - c(a)|_p^{\nu/e'}, \tag{3}$$

où $\nu \in \mathbb{Z}$, et $g_0(x)$ est une fonction définissable.

Il nous reste à regarder la définition de $S \cap A$ d'un peu plus près. Nous savons que sur $A$, chaque $f_i$ s'écrit $h_i(x)u_i(x,t)^n(t-c(x))^{e_i}$. Donc $P_n^*(f_i(x,t))$ est équivalent à $P_n^*(h_i(x)(t-c(x))^{e_i})$, et sur $A$, $S$ sera défini par

$$P_n^*(h_i(x)(t - c(x))^{e_i}),\ i = 1, \ldots, r. \tag{4}$$

Nous savons que $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times n}$ est fini. Nous partitionnons $S \cap A$ en des sous-ensembles plus petits, tels que pour chaque élément $T$ de la partition, les fonctions qui à chaque $h_i(x)$ et à $t - c(x)$ associent leur image dans $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times n}$, soient constantes. Si $M \subset \mathbb{Z}$ est un système de représentants de $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times n}$, alors on aura

$$P_n^*(h_i(x)(t - c(x))^{e_i}) \iff \bigvee_{k \in M} (P_n^*(k^{-1}(t - c(x))) \wedge P_n^*(k^{e_i} h_i(x)).$$

Chaque $T$ sera donc défini par :

$$\bigwedge_i P_n^*(k^{e_i} h_i(x)) \wedge (x,t) \in S \cap A \wedge P_n^*(k^{-1}(t - c(x)))$$

pour un certain entier $k$. Chaque élément de cette partition finie de $S$ est de la forme

$$T = \{(x,t) \in \mathbb{Q}_p^{m+1} \mid x \in D, v(a_1(x)) \prec_1 v(t - c(x)) \prec_2 v(a_2(x)), P_n^*(k^{-1}(t - c(x))\} \tag{5}$$

pour un sous-ensemble définissable $D$ de $\mathbb{Q}_p^m$. Nous avons alors

$$\begin{aligned} \int_T |g(x,t)|_p^{s/e} |dx||dt| &= \int_D \left( |g_0(x)|_p^{s/e'} \int_{t \in T(x)} |t - c(x)|_p^{s\nu/e'} |dt| \right) |dx| \\ &= \int_D \left( |g_0(x)|_p^{s/e'} \sum_{\ell \in Q(x)} p^{-\ell s \nu / e'} \int_{\substack{v(t-c(x))=\ell \\ P_n^*(m_0(t-c(x)))}} |dt| \right) |dx|, \end{aligned} \tag{6}$$

où $Q(x) = \{\ell \in \mathbb{Z} \mid v(a_1(x)) \prec_1 \ell \prec_2 a_2(x)\}$. Si on écrit maintenant $t - c(x) = p^\ell u$, nous avons

$$\int_{\substack{v(t-c(x))=\ell \\ P_n^*(k^{-1}(t-c(x)))}} |dt| = p^{-\ell} \int_{\substack{v(u)=0 \\ P_n^*(m_0 p^\ell u)}} |du| \tag{7}$$

(car $|dt| = |p^\ell|_p |du| = p^{-\ell}|du|$). L'intégrale de droite est 0 si $v(k^{-1}) + \ell$ n'est pas divisible par $n$, c'est-à-dire, si $\ell \not\equiv v(k) \bmod n$ ; et sinon, elle est constante, égale disons à $N$, où $N$ est la mesure de $\{a \in \mathbb{Z}_p \mid v(a) = 0 \wedge P_n^*(a)\}$. (En fait on peut montrer que $N = [\mathbb{Q}_p^\times : \mathbb{Q}_p^{\times n}]^{-1}$).

Nous avons donc

$$\sum_{\ell \in Q(x)} p^{-\ell s\nu/e'} \int_{\substack{v(t-c(x))=\ell \\ P_n^*(m_0(t-c(x)))}} |dt| = N \sum_{\substack{\ell \in Q(x) \\ \ell \equiv v(k) \bmod n}} p^{-\ell s\nu/e'} p^{-\ell}, \tag{8}$$

Nous en déduisons que

$$Z_T(s) = M \sum_{\ell \equiv v(k) \bmod n} p^{-\ell(s\nu/e'+1)} \int_{F(\ell)} |g_0(x)|^{s/e'} |dx|, \tag{9}$$

où $F(\ell)$ est l'ensemble $\{x \in D,\, v(a_1(x)) \prec_1 \ell \prec_2 v(a_2(x))\}$. Il y a cependant un petit problème : nous avons une somme infinie d'intégrales dont les domaines dépendent de $\ell$. Il faut donc montrer que ces intégrales sont suffisamment uniformes.

Pour cela, nous écrivons $x = (y, z)$, $z$ une seule variable, et répétons la procédure pour éliminer maintenant la variable $z$. C'est à dire, en appliquant le théorème 6.14 aux fonctions utilisées pour définir $D$, et aux fonctions $g_0(x)$, $a_1(x)$ et $a_2(x)$, nous pouvons partitionner $\mathbb{Q}_p^m$ en des sous-ensembles

$$T' = \{x \in \mathbb{Q}_p^m \mid y \in D'\ v(b_1(y)) \prec_1 v(z - c'(y)) \prec_2 v(b_2(x)), P_{n'}^*(m_0'(z - c'(y)))\}$$

sur lesquels les valeurs $|g_0(x)|_p$, $|a_1(x)|_p$ et $|a_2(x)|_p$ sont de la forme donnée dans l'équation (3), c'est-à-dire

$$|g_0(x)|_p = |g_0'(y)|_p |z - c'(y)|^{\nu_0},\ |a_i(x)|_p = |a_i'(y)|_p |z - c'(y)|_p^{\nu_i} \quad i = 1, 2.$$

La condition $x \in F(\ell)$ devient alors

$$v(a_1'(y)) + \nu_1 v(z - c'(y)) \prec_1 \ell \prec_2 v(a_2'(y)) + \nu_2 v(z - c'(y)),$$

et nous voulons évaluer

$$Z_{T'}(s) = M' \sum_{\substack{\ell \equiv v(k) \bmod n, \\ \ell_1 \equiv v(k_1^{-1}) \bmod n'}} p^{-\ell(s\nu/e'+1) - \ell''(\alpha a + \beta)} \int_{F'(\ell,\ell')} |g_0'(y)|^{s/e'} |dy|,$$

où $\alpha, \beta$ sont des rationnels, et $F(\ell, \ell')$ est défini maintenant par des conditions de la forme $v(a_i'(y)) \prec \ell - \nu_i \ell'$. (En fait, $\beta = 1$)

En itérant suffisamment la procédure, nous obtenons enfin que notre intégrale de départ $Z_S(s)$ est une $\mathbb{Q}$-combinaison linéaire de séries convergentes de la forme

$$\sum_{\substack{(\ell_0,\dots,\ell_m)\in\Lambda \\ \ell_i\equiv k_i \bmod n_i}} p^{(-q_0\ell_0-\cdots-q_m\ell_m)s-\ell_0-\cdots-\ell_m} \tag{10}$$

où $q_0,\dots,q_m \in \mathbb{Q}$, $k_i \in \mathbb{Z}$, $n_i \in \mathbb{N}$, et $\Lambda$ est l'ensemble des uplets $(\ell_0,\dots,\ell_m) \in \mathbb{Z}^{m+1}$ satisfaisant un système d'inégalités linéaires à coefficients entiers.

Nous avons maintenant besoin d'un lemme (que je ne prouverai pas) :

**6.16. Lemme**. Soit $\Lambda$ l'ensemble de tous les entiers $k_1,\dots,k_n$ satisfaisant un système fini d'inégalités linéaires à coefficients entiers. Soient $A_1(s),\dots,A_n(s)$ des polynômes de $\mathbb{Z}[s]$ de degré $\leq 1$, et soit $p \in \mathbb{N}^{>1}$. Si la série

$$J(s) = \sum_{k_1,\dots,k_n\in\Lambda} p^{-\sum_i k_i A_i(s)}$$

converge pour tout $s$ dans un ouvert $U$ de $\mathbb{R}$, alors il existe $P(T) \in \mathbb{Q}(T)$ tel que $J(s) = P(p^{-s})$ pour tout $s \in U$.

Pour la preuve, voir l'article de Denef : J. Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety*, Inventiones Math. 77 (1984), 1 – 23.

**6.17.** *Fin de la démonstration.* Nous savons que pour tout $s > 0$, notre intégrale $Z_S(s)$ est définie : puisque $\mu(S) < \infty$, et $|h(x)|_p$ est bornée sur $S$. D'autre part, nous avons exprimé notre intégrale de la forme donnée dans le lemme, sauf que les coefficients des $A_i$ sont rationnels.

Si $d$ est le dénominateur commun des rationnels $q_j$ apparaissant dans l'équation (10), nous obtenons donc que $Z_S(s) = P(p^{-s/d})$, pour $P$ donné par le lemme 6.16. D'un autre côté, pour chaque $n \in \mathbb{Z}$, soit $a_n$ la mesure de l'ensemble des $(x,t) \in \mathbb{Q}_p^{m+1}$ tels que $v(h(x,t)) = n$. Alors $Z_S(s) = \sum_{k=k_0}^{\infty} a_n p^{-ks}$. Cela entraine que la série $\sum_{k=k_0}^{\infty} a_n T^n$ est égale à $P(T^{1/d})$. Elle est donc égale à $Q(T)$ pour un $Q(T) \in \mathbb{Q}(T)$, et cela donne le résultat.

**6.18. Remarques additionnelles**. On peut aussi montrer les résultats suivants :

(1) $P(T)$ s'écrit comme un polynôme en $T$ et $T^{-1}$, divisé par un produit de termes de la forme $(1 - p^a T^b)$ où $a, b \in \mathbb{Z}$ (donc cela dépend de $p$).

(2) Les pôles de $Z_S(s)$ ont multiplicité $\leq m + 1$.

(3) Théorème 6.15 s'étend à d'autres fonctions, définissables dans un langage plus riche contenant des fonctions analytiques. Voir J. Denef, L. van den Dries, *p-adic and real subanalytic sets*, Annals of Math, 128 (1988), 79 – 138.

(4) Il existe des résultats d'uniformité en $p$, qu'on peut trouver dans l'article de Pas déja cité [P], et dans : A. Macintyre, *Rationality of p-adic Poincaré series: uniformity in p*, Ann. of Pure and Applied Logic 49 (1990), 31 – 74. Dans le chapitre suivant, nous allons brièvement discuter les résultats de Pas, et comment ils impliquent une uniformité.

**6.19. Un résultat plus fort, et une autre preuve**. Quand on arrive à l'équation (8), on voit qu'on peut déja calculer l'intégrale en fonction de $v(a_1(x))$ et $v(a_2(x))$, et se réduire donc à calculer une intégrale qui ne dépend plus de $t$. Malheureusement la fonction à intégrer n'est pas de la forme désirée. On peut remédier à ce problème en renforçant l'énoncé du théorème. Je donne une esquisse de preuve ci-dessous.

**Théorème**. Soient $e \in \mathbb{N}^{>0}$, $d \in \mathbb{N}$, $S \subset \mathbb{Q}_p^m$ un ensemble définissable, et $g_0(x), \ldots, g_d(x)$ des fonctions définissables de $S$ dans $\mathbb{Q}_p$. Supposons que pour tout $i = 0, \ldots, d$, la fonction $x \mapsto v(g_i(x))$ soit bornée sur $S$ et prenne ses valeurs dans $e\mathbb{Z} \cup \{+\infty\}$. Pour $s \in \mathbb{R}^{>0}$, considérons alors l'intégrale

$$Z_{g,S}(s) = \int_S \prod_{i=0}^{d} |g_i(x)|_p^{s^i/e} |dx|.$$

Alors $Z_{g,S}(s)$ est une fonction rationnelle de $p, p^{-s}, \ldots, p^{-s^d}$.

*Démonstration.* Les étapes de la preuve sont identiques à celle de 6.15. J'utilise les notations de 6.15. Nous supposons le résultat vrai pour $m$, et allons le montrer pour $m+1$. Tout d'abord, par le théorème 6.11, nous pouvons supposer que les fonctions $g_i(x,t)$ sont des fonctions rationnelles (et n'ayant pas de pôles sur $S$). On se réduit ensuite à un ensemble $S$ défini par

$$x \in C \wedge \bigwedge_{i=1}^{r} P_n^*(f_i(x,t)) \tag{1}.$$

En appliquant le théorème 6.14 aux fonctions $f_1, \ldots, f_r$ et aux polynômes apparaissant dans l'écriture de $g_0, \ldots, g_d$, nous pouvons donc partitionner $\mathbb{Q}_p^{m+1}$ en des sous-ensembles $A$ de la forme

$$A = \{(x,t) \in \mathbb{Q}_p^{m+1} \mid x \in B, v(a_1(x)) \prec_1 v(t - c(x)) \prec_2 v(a_2(x))\} \tag{2}$$

pour un ensemble définissable $B$ et des fonctions définissables $a_1, a_2$ et $c$, et $\prec_i \in \{\leq, <\}$. Nous pouvons aussi supposer qu'aucune des fonctions $f_1, \ldots, f_r, g_0, \ldots, g_d$ n'a de zéro dans $A$ (sinon on les enlève).

Procédant comme dans la preuve de 6.14, nous nous réduisons donc à intégrer sur des ensembles définissables de la forme

$$T = \{(x,t) \in \mathbb{Q}_p^{m+1} \mid x \in D, v(a_1(x)) \prec_1 v(t - c(x)) \prec_2 v(a_2(x)), P_n^*(m_0(t - c(x))\} \tag{5}$$

pour un sous-ensemble définissable $D$ de $\mathbb{Q}_p^m$ et un entier $m_0$ non nul. De plus sur $T$, les fonctions $g_0, \ldots, g_d$ n'ont ni zéros ni pôles, et nous avons

$$|g_i(x,t)|_p = |g_i'(x)|_p |t - c(x)|_p^{\nu_i},\ i = 0, \ldots, d,\ \nu_i \in \mathbb{N} \tag{3}$$

Nous avons alors

$$Z_{g,T}(s) = \int_D \left( |G(x)|_p^{1/e} \sum_{k \in Q(x)} p^{-kH(s)} \int_{\substack{v(t-c(x))=k \\ P_n^*(m_0(t-c(x)))}} |dt| \right) |dx| \tag{6}$$

où

$$\begin{aligned} G(x) &= \prod_{i=0}^{d} g_i'(x)^{s^i}, \qquad H(s) = \frac{1}{e}\sum_{i=0}^{d} \nu_i s^i, \\ Q(x) &= \{k \in \mathbb{Z} \mid v(a_1(x)) \prec_1 k \prec_2 v(a_2(x)), k \equiv -v(m_0) \bmod n\}. \end{aligned}$$

Remarquez que la définition de $Q(x)$ que j'ai prise est un peu différente de celle donnée dans 6.15, puisque j'y ai rajouté la condition de congruence. Nous pouvons de plus partitionner $D$ en des ensembles plus petits sur lesquels : ou bien la fonction $a_2(x)$ est identiquement nulle, ou bien elle n'est jamais nulle ; les classes de congruence de $v(a_1(x))$ et $v(a_2(x))$ modulo $n$ sont constantes. Il existe donc des entiers $i$ et $j$ plus petits que $n$, tels que $v(a_1(x)) + i$ soit le plus petit élément de $Q(x)$, et $v(a_2(x)) - j$ soit le plus grand. C'est-à-dire,

$$Q(x) = \{v(a_1(x)) + i + \ell n \mid 0 \leq \ell \leq (v(a_2(x)) - v(a_1(x)) + i - j)/n\}.$$

Si $k \in Q(x)$, nous avons aussi

$$\int_{\substack{v(t-c(x))=k \\ P_n^*(m_0(t-c(x)))}} |dt| = p^{-k} \int_{\substack{v(u)=0 \\ P_n^*(m_0 p^k u)}} |du| = M p^{-k}. \tag{7}$$

On calcule facilement que

$$\sum_{k \in Q(x)} p^{-k(H(s)+1)} = \frac{p^{-(v(a_1(x))+i)(H(s)+1)} - p^{-(v(a_2(x))-j+n)(H(s)+1)}}{1 - p^{-n(H(s)+1)}}$$

(avec $p^{-\infty} = 0$). Par hypothèse, sur $T$, $v(g_i(x,t)) \in e\mathbb{Z} \cup \infty$. Donc, pour tout $i$, $x \in D$ et $k \in Q(x)$, $e$ divise $v(g_i'(x)) + \nu_i k$. Donc pour tout $k \in Q(x)$, le polynôme (en $s$) $k(H(s)+1) + \sum_{i=0}^{d} v(g_i'(x))s^i/e$ a ses coefficients dans $\mathbb{Z}$.

Si $N(x) = (v(a_2(x)) - v(a_1(x)) + i - j)/n$ est borné sur $D$, alors, en passant à une partition de $D$, nous pouvons supposer que $N$ est constant sur $D$, ce qui nous donne que

$$Z_{g,T}(s) = \sum_{\ell=0}^{N} p^{-\ell n} \int_D |G(x)|_p^{1/e} |p^i a_1(x)|^{H(s)+1} |dx|,$$

et nous pouvons appliquer l'hypothèse d'induction pour conclure.

Si $N(x)$ n'est pas borné sur $D$, on remarque que $e$ divise $n\nu_i$ pour tout $i$. Donc $nH(s)$ a ses coefficients dans $\mathbb{Z}$, et on en déduit que, puisque

$$Z_{g,T}(s) = \frac{M}{1 - p^{-n(H(s)+1)}} \int_D |G(x)|_p^{1/e} \big(|p^i a_1(x)|^{H(s)+1} - |p^{n-j} a_2(x)|^{H(s)+1}\big) |dx|, \tag{9}$$

nous pouvons ici aussi appliquer l'hypothèse d'induction pour conclure.

# 7 Intégrales $p$-adiques - uniformité en $p$

**7.1.** Nous travaillons dans le langage de Pas, $\mathcal{L}_{\text{Pas}}$, qui est un langage à trois sortes : $\mathcal{L}_{\text{c.val}}$, $\mathcal{L}_{\text{gp}}$ et $\mathcal{L}_{\text{c.rés}}$. Nous agrandissons le langage de la sorte du groupe de valeurs en y ajoutant une constante 1 et les relations binaires $\equiv_n$, $n \geq 2$, pour obtenir les langages $\mathcal{L}'_{\text{gp}}$ et $\mathcal{L}'_{\text{Pas}}$. Nous utiliserons aussi la fonction res bien qu'elle ne soit pas dans notre langage (rappelons que sur les éléments de valuation 0, elle coïncide avec $\overline{\text{ac}}$, et que sur ceux de valuation positive elle est égale à 0).

Les structures que nous considérons sont des $\mathcal{L}_{\text{Pas}}$-structures $(K, \Gamma, k)$, avec $k$ de caractéristique 0, et $K$ un corps Hensélien de corps résiduel $k$ et de groupe de valeurs $\Gamma$. En général, le groupe de valeurs $\Gamma$ sera un $\mathbb{Z}$-groupe (en fait, ce sera même $\mathbb{Z}$), ce qui explique le choix de $\mathcal{L}'_{\text{gp}}$, puisque nous savons que $\text{Th}(\mathbb{Z})$ élimine les quantificateurs dans ce langage.

Nous considérons les $\mathcal{L}_{\text{Pas}}$-théorie $T_0$ et $\mathcal{L}'_{\text{Pas}}$-théorie $T'_0$ définies comme suit : (voir 4.1) $T_0$ est obtenue en prenant la théorie dont les modèles sont les $\mathcal{L}_{\text{Pas}}$-structures à 3 sortes associées à des corps valués Henséliens $(K, v)$ de caractéristique résiduelle nulle, c'est-à-dire : on dit que $K$ est un corps, que l'application $v$ est une application de $K$ dans $\Gamma \cup \{\infty\}$, qui définit une valuation sur $K$, de groupe de valeurs $\Gamma$, et que $K$ est Hensélien pour cette valuation. De plus l'application $\overline{\text{ac}} : K \to k$ satisfait les conditions suivantes : $\overline{\text{ac}}(0) = 0$ ; sa restriction à $K^\times$ définit un morphisme de groupe (multiplicatif) à valeurs dans $k^\times$ ; si on définit res : $\mathcal{O}_v \to k$ en posant

$$\text{res}\, x = \begin{cases} \overline{\text{ac}}(x) & \text{si } v(x) = 0, \\ 0 & \text{si } v(x) > 0, \end{cases}$$

alore l'application res est un morphisme d'anneau qui est surjectif et a pour noyau l'idéal $\mathcal{M}_v$ ; le corps $k$ est de caractéristique 0. Pour obtenir la $\mathcal{L}'_{\text{Pas}}$-théorie $T'_0$, nous ajoutons à $T_0$ les axiomes disant que $\xi \equiv_n \zeta \iff \exists \sigma\ n\sigma = (\xi - \zeta)$, et que $\Gamma$ est un $\mathbb{Z}$-groupe ordonné avec plus petit élément positif 1.

J'essaierai d'utiliser les notations suivantes : les lettres latines $(a, b, c, x, y, \dots)$ dénoteront des uplets d' éléments ou de variables de la sorte du corps valué, les lettres latines surlignées $(\bar{a}, \bar{b}, \bar{x}, \dots)$ dénoteront des uplets d'éléments ou de variables du corps résiduel, et les lettres grecques $(\alpha, \beta, \xi, \rho, \dots)$ des uplets d'éléments ou de variables du groupe de valeurs.

Voici quelques définitions introduites par Pas, mais que nous n'utiliserons pas :

**Définitions**. (1) Une $\mathcal{L}_{\text{Pas}}$-formule est *simple* si elle ne contient pas de quantificateurs sur la sorte du corps valué. Elle est $\Gamma$-*simple* si de plus elle ne contient pas de quantificateurs sur la sorte du groupe de valeurs.

(2) Une fonction $h : K^m \times k^\ell \to K$ est *fortement définissable* (resp. *fortement* $\Gamma$-*définissable*) si son graphe est définissable (resp., $\Gamma$-définissable).

Nous savons déja que toute $\mathcal{L}_{\text{Pas}}$-formule est équivalente, modulo la théorie $T_0$ introduite dans 4.1(1), à une formule simple. Dans le cas où le groupe de valeurs est un $\mathbb{Z}$-groupe, toute formule est équivalente modulo $T'_0$ à une $\mathcal{L}'_{\text{Pas}}$-formule $\Gamma$-simple : tout simplement parce que la théorie du groupe ordonné $\mathbb{Z}$ élimine les quantificateurs dans $\mathcal{L}'_{\text{gp}}$ (voir 4.12).

**7.2. Définition des cellules**. Let $x = (x_1, \ldots, x_m)$, $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_n)$ des variables, et $C$ un sous-ensemble définissable de $K^m \times k^n$. Soient $b_1(x, \bar{x})$, $b_2(x, \bar{x})$, $c(x, \bar{x})$ des fonctions définissables à valeurs dans $K$, $\ell$ un entier positif, et $\prec_i \in \{\leq, <\}$ (ou bien pas de condition). Pour $\bar{a} = (\bar{a}_1, \ldots, \bar{a}_n) \in k^n$, posons

$$A(\bar{a}) = \{(x,t) \in K^{m+1} \mid (x,\bar{a}) \in C, v(b_1(x,\bar{a})) \prec_1 \ell v(t - c(x,\bar{a})) \prec_2 v(b_2(x,\bar{a})), \\ \bar{a}c(t - c(x,\bar{a})) = \bar{a}_1\}$$

Si de plus, pour $\bar{a} \neq \bar{b}$ on a $A(\bar{a}) \cap A(\bar{b}) = \emptyset$, alors $A = \bigcup_{\bar{a} \in k^n} A(\bar{a})$ est appellée une *cellule de $K^{m+1}$, de paramètre $\bar{x}$, et centre $c(x, \bar{x})$*. $A(\bar{a})$ est appellée une *fibre de la cellule*.

**Remarque**. Il est clair que chaque fibre $A(\bar{a})$ est définissable. La cellule $A$ l'est aussi : $(x,t) \in A$ si et seulement $\exists \bar{x} \in k^n$ $(x,t) \in A(\bar{x})$.

**7.3. Théorème**. Soient $f_1(X,T), \ldots, f_r(X,T) \in \mathbb{Z}[X,T]$ des polynômes. Alors $K^{m+1}$ peut être décomposé en cellules $A$ qui satisfont :

Il existe des fonctions $h_i(x,\bar{x})$, $i = 1, \ldots, r$, des entiers non négatifs $e_1, \ldots, e_r$, et une fonction $\mu : \{1, \ldots, r\} \to \{1, \ldots, n\}$ telles que :

sur chaque fibre $A(\bar{a})$ de $A$, pour tout $(x,t) \in A(\bar{a})$ et $i = 1, \ldots, r$,

$$v(f_i(x,t)) = v(h_i(x,\bar{a})) + e_i v(t - c(x,\bar{a})), \quad \overline{\mathrm{ac}}(f_i(x,t)) = a_{\mu(i)}.$$

**7.4.** Pour prouver ce résultat, on regarde d'abord le cas d'un seul polynôme $f(X,T)$. On décompose alors $K^{m+1}$ en cellules $A$ comme ci-dessus, et on trouve des indices $i_0$ et $j_0$, tels que, pour tout $\bar{a} \in k^n$ et $(x,t) \in A(\bar{a})$, si on effectue la division euclidienne de $f(x,T)$ par $T - c(x,\bar{a})$ et écrit $f(x,T) = \sum_{i=0}^{d} a_i(x,\bar{a})(T - c(x,\bar{a}))^i$, alors $v(f(x,t)) = v(a_{i_0}(x,\bar{a})) + i_0 v(t - c(x,\bar{a}))$ et $\overline{\mathrm{ac}}(f(x,t)) = \bar{a}_{j_0}$.

Il faut remarquer que Pas utilise la décomposition en cellules pour montrer son résultat d'élimination des quantificateurs. Ses preuves sont longues (celle du résultat préliminaire prend plusieurs pages). Il utilise une induction sur le degré $d$ en $T$ du polynôme $f(X,T)$. Je ne crois pas que le fait de savoir déja que la théorie élimine les quantificateurs la raccourcisse beaucoup.

**7.5. Théorème**. Soit $h(X) \in \mathbb{Z}[X]$, et $\psi(x)$ une $\mathcal{L}_{\mathrm{Pas}}$-formule. Supposons que pour tout premier $p$, le sous-ensemble de $\mathbb{Q}_p^m$ défini par $\psi(x)$ soit borné. Alors, pour tout premier $p$, l'intégrale

$$Z_\psi(s,p) = \int_{W_p} |h(x)|_p^s |dx|_p$$

est une fonction rationnelle de $p^{-s}$, et les degrés du numérateur et dénominateur de cette fonction sont bornés indépendamment de $p$.

**7.6. Idée de la preuve**. On équipe bien sûr $\mathbb{Q}_p$ de la $\mathcal{L}'_{\mathrm{Pas}}$-structure naturelle. La composante angulaire est définie par $\overline{\mathrm{ac}}(a) = \mathrm{res}\,(p^{-v(a)}a)$.

On utilise le théorème 7.3 pour obtenir une décomposition cellulaire de l'ensemble défini par $\psi(x)$ (dans $K$). La démonstration du reśultat final est ensuite plus simple que celle de Denef,

et est faite en 7.11. Elle utilise de façon cruciale la décomposition cellulaire donnée ci-dessus, et aussi quelques lemmes faciles. Notons que la $\mathcal{L}'_{\text{Pas}}$-structure $(\mathbb{Q}_p, \mathbb{Z}, \mathbb{F}_p)$ est modèle de tous les axiomes de $T_0$, à l'exception des axiomes qui disent que le corps résiduel est de caractéristique 0. La preuve que $\psi(x)$ est équivalente modulo $T_0$ à une disjonction de formules définissant des cellules, n'utilise qu'un nombre fini d'axiomes. Cette équivalence sera donc vraie dans toutes les $\mathcal{L}'_{\text{Pas}}$-structures $\mathbb{Q}_p$ pour $p$ suffisamment grand. Disons pour tout $p > M$.

Cela nous donne donc un résultat d'uniformité sur les degrés des différents polynômes qui évaluent l'intégrale. Comme il n'y a qu'un nombre fini de premiers $< M$, et que nous connaissons aussi le résultat pour ceux-cis, nous obtenons le théorème.

Il faut noter que la démonstration donnée dans 6.19 nous permet de donner une borne sur le nombre de facteurs de la fraction rationnelle associée à l'intégrale. Cependant, vous noterez que dans le dénominateur apparaît $(1 - p^{-ns})$, et que a priori, $n$ peut croître avec $p$.

**7.7. Lemme**. Soient $y$, $\rho$ et $\bar{y}$ des uplets de variables de corps valué, de groupe de valeurs et de corps résiduel. Soient $x$ un $m$-uplet de variables de corps valué, $t$ une seule variable de corps valué. Soit enfin $\psi(x, t, y, \rho, \bar{y})$ une $\mathcal{L}'_{\text{Pas}}$-formule. Supposons que pour presque tout $p$, et pour tous uplets $(b, \beta, \bar{b}) \in \mathbb{Q}_p^? \times (\mathbb{Z} \cup \infty)^? \times \mathbb{F}_p^?$ l'ensemble $W_p(b, \gamma, \bar{b}) \subset \mathbb{Q}_p^{m+1}$ défini par $\psi(x, t, b, \beta, \bar{b})$ soit borné. Soit

$$I_p(b, \beta, \bar{b}) = \int_{W_p(b,\beta,\bar{b})} |dx||dt|.$$

Il existe des $\mathcal{L}'_{\text{Pas}}$-formules $\varphi_i(x, \bar{x}, \sigma, y, \rho, \bar{y})$, $i = 1, \dots N$, telles que pour presque tout premier $p$

$$I_p(b, \beta, \bar{b}) = \frac{1}{p} \sum_{i=1}^{N} \sum_{\bar{a} \in \mathbb{F}_p^?} \sum_{\gamma \in \mathbb{Z}} p^{-\gamma} \int_{E_i} |dx|$$

où $E_i = E_i(\bar{a}, \gamma, b, \beta, \bar{b}) = \{x \in \mathbb{Q}_p^m \mid \mathbb{Q}_p \models \varphi_i(x, \bar{a}, \gamma, \bar{b}, \beta, \bar{b})\}$.

*Démonstration.* Nous travaillons dans une $\mathcal{L}'_{\text{Pas}}$-structure $\mathcal{K} = (K, \Gamma, k)$ qui est a priori un modèle arbitraire de $T'_0$, mais pourra aussi être la $\mathcal{L}'_{\text{Pas}}$-structure associée à $\mathbb{Q}_p$ pour $p$ suffisamment grand. L'hypothèse sur la formule $\psi$ est du premier ordre : on dit tout simplement : $\forall y, \rho, \bar{y}\, \exists \sigma\, \forall x, t\ (\psi(x, t, y, \rho, \bar{y}) \to v(x) \geq \sigma \wedge v(t) \geq \sigma)$.

Par le théorème 4.1, notre formule $\psi(x, t, y, \rho, \bar{y})$ est équivalente, modulo $T'_0$, à une disjonction (exclusive) de formules de la forme

$$\psi_1(x, y, \rho, \bar{y}) \wedge \psi_2(\rho, v(F(x, t, y))) \wedge \psi_3(\bar{y}, \overline{\text{ac}}(G(x, y, t))) \tag{1}$$

où $\psi_1 \in \mathcal{L}'_{\text{Pas}}$, $\psi_2 \in \mathcal{L}'_{\text{gp}}$, $\psi_3 \in \mathcal{L}_{\text{c.rés}}$, et $F, G$ sont des uplets de polynômes à coefficients dans $\mathbb{Z}$. Notez que modulo $T_0$ la formule $f(x, t, y) = 0$ est équivalente à $\overline{\text{ac}}(f(x, t, y)) = 0$, c'est pourquoi $t$ n'apparaît pas dans $\psi_1$. Puisque $T'_0$ élimine les quantificateurs, nous pouvons supposer que $\psi_2$ est sans quantificateurs. L'équivalence de $\psi$ avec cette disjonction sera vraie pour tout $p$ suffisamment grand, et nous pouvons donc supposer que $\psi$ est de la forme donnée par (1).

Nous appliquons aux polynômes apparaissant dans $F, G$ la décomposition cellulaire donnée par 7.3, et obtenons une partition finie du $(x, t, y)$-espace $K^?$ en des cellules définissables

$A_1, \ldots, A_N$. Sur chaque cellule $A_i$, et pour tout uplet $\bar{a}$ du corps résiduel $k$, si $f(x,t,y)$ est un des polynômes de $F \cup G$, alors nous savons que

$$\overline{\mathrm{ac}}(f(x,t,y)) = \bar{a}_\mu \qquad v(f(x,t,y)) = v(h(x,y,\bar{a}))) + \nu v(t - c(x,y,\bar{a}))$$

pour des entiers $\mu = \mu_{f,i}$, $\nu = \nu_{f,i}$ et des fonctions définissables $h = h_{f,i}$ et $c : K^? \times k^? \to K$. Pour chaque $i$ il existe donc une formule $\theta_i(x, \bar{x}, \sigma, y, \rho, \bar{y})$ telle que, pour tout $(\beta, \bar{b}) \in \mathcal{K}$ et $\bar{a}$ dans $k^?$, un uplet $(x,t,y) \in A_i(\bar{a})$ satisfera $\psi(x,t,y,\beta,\bar{b})$ si et seulement si $(x, \bar{a}, v(t - c(x,y,\bar{a})), b, \beta, \bar{b})$ satisfait $\theta_i$.

Si $A_{i,p}$ est la cellule de $\mathbb{Q}_p^{m+1}$ définie par la formule définissant $A_i$, la même conclusion est vraie pour $p$ suffisamment grand. Si $A_i$ est définie au moyen de l'ensemble définissable $C$ (dans le $(x,y,\bar{x})$-espace), de l'entier $\ell$ et des fonctions définissables $b_1(x,y,\bar{x})$ et $b_2(x,y,\bar{x})$, soit $\varphi_i(x,\bar{x},\sigma,y,\rho,\bar{y})$ la formule :

$$(x,y) \in C \wedge v(b_1(x,y,\bar{x})) \prec_1 \ell\sigma \prec_2 v(b_2(x,y,\bar{x})) \wedge \theta_i(x,\bar{x},\sigma,y,\rho,\bar{y}).$$

Alors pour tout $b, \beta, \gamma, \bar{a}, \bar{b}$ et $(x,t) \in K^{m+1}$, si nous posons $\gamma = v(t - c(x,b,\bar{a}))$, et $B_i(y)(\bar{x}) = \{(x,t) \in K^{m+1} \mid (x,t,y) \in A_i(\bar{x})\}$, $B_i(y) = \bigcup_{\bar{x}} B_i(y)(\bar{x})$, nous aurons

$$(x,t) \in B_i(b)(\bar{a}) \text{ et } \mathcal{K} \models \psi(x,t,b,\beta,\bar{b}) \leftrightarrow$$
$$\mathcal{K} \models \varphi_i(x,\bar{a},\gamma,b,\beta,\bar{b}) \wedge \overline{\mathrm{ac}}(t - c(x,b,\bar{a})) = \bar{a}_1 \wedge v(t - c(x,b,\bar{a})) = \gamma.$$

Prenant maintenant $K = \mathbb{Q}_p$ pour $p$ suffisamment grand, et des uplets $(b, \beta, \bar{b}) \in \mathbb{Q}_p^? \times \mathbb{Z}^? \times \mathbb{F}_p^?$, nous obtenons

$$\int_{W_p \cap B_i(b)} = \sum_{\bar{a} \in \mathbb{F}_p^?} \sum_{\gamma \in \mathbb{Z}} \int_{\varphi_i(x,\bar{a},\gamma,b,\beta,\bar{b})} \left( \int_{\substack{v(t-c(a,b,\bar{a}))=\gamma \\ \overline{\mathrm{ac}}(t-c(a,b,\bar{a}))=\bar{a}_1}} |dt| \right) |dx| \tag{2}$$

On a aussi

$$\int_{\substack{v(t-c(a,b,\bar{a}))=\gamma \\ \overline{\mathrm{ac}}(t-c(a,b,\bar{a}))=\bar{a}_1}} |dt| = p^{-(\gamma+1)},$$

et en mettant tout ensemble nous obtenons le résultat.

**7.8. Remarque**. Que nous donne ce résultat ? Il nous permet de réduire le calcul du volume d'un sous-ensemble définissable $W \subset \mathbb{Q}_p^{m+1}$ à une somme de volumes d'ensembles définissables $E_i \subset \mathbb{Q}_p^m$. De plus, cette réduction est uniforme en les paramètres servant à définir l'ensemble $W$, c'est-à-dire, on peut itérer la procédure : si on écrit $x = (y,z)$, $z$ une seule variable, on obtient que $\int_{E_i} |dx|$ est une somme finie de termes de la form $p^{-1} \sum_{\delta \in \mathbb{Z}} p^{-\delta} \int_{F_j} |dy|$.

**7.9. Lemme**. Soit $\varphi(\xi, \bar{x})$ une formule ne contenant pas de variables de corps valué. Alors modulo $T_0$, $\varphi$ est équivalente à une disjonction de formules de la forme $\varphi_2(\xi) \wedge \varphi_3(\bar{x})$, où $\varphi_2(\xi) \in \mathcal{L}'_{\mathrm{gp}}$ et $\varphi_3(\bar{x}) \in \mathcal{L}_{\mathrm{c.rés}}$.

*Démonstration.* Nous savons, par le théorème 4.1, que modulo $T_0$, $\psi(\xi, \bar{x})$ est équivalent à une disjonction de formules de la forme

$$\varphi_1 \wedge \varphi_2(\xi) \wedge \varphi_3(\bar{x})$$

où $\varphi_1 \in \mathcal{L}_{\text{c.val}}$ est une formule sans quantificateurs (et sans variables libres, donc un énoncé), et $\varphi_2(\xi)$, $\varphi_3(\bar{x})$ sont de la forme désirée.

Mais comme $\varphi_1$ est sans quantificateurs, nous avons : ou bien $T_0 \vdash \varphi_1$, ou bien $T_0 \vdash \neg\varphi_1$.

**7.10. Lemme**. Soit $\psi(\xi, \zeta)$ une $\mathcal{L}'_{\text{Pas}}$-formule (peut-être avec paramètres), $\xi$ un $m$-uplet, et $\zeta$ une seule variable, les seules variables libres étant des variables de groupe. Posons $E = \{(\ell, n) \in \mathbb{Z}^{m+1} \mid \psi(\ell, n)\}$, et supposons que pour tout premier $p$ suffisamment grand, la série

$$J(s) = \sum_{(\ell,n)\in E} p^{-ns-\ell_1-\cdots-\ell_m}$$

converge pour tout réel $s$ dans un sous-ensemble ouvert $U$ de $\mathbb{R}$. Il existe alors des polynômes $Q, R \in \mathbb{Z}[X, Y]$ tels que pour presque tout $p$, et pour tout $s \in U$,

$$J(s) = \frac{Q(p, p^{-s})}{R(p, p^{-s})}.$$

*Démonstration.* En prenant une partition de $E$, et en utilisant l'élimination des quantificateurs de $\text{Th}(\mathbb{Z})$ dans le langage $\mathcal{L}'_{\text{gp}}$, nous pouvons supposer que $E$ est défini par une conjonction de congruences modulo $n$, et par un système d'inégalités de combinaisons linéaires. En faisant un changement de variables, on se ramène à un ensemble défini par des inégalités de combinaisons linéaires, et on peut alors utiliser le résultat de Denef (ou plutôt sa preuve) déja mentionné dans 6.16.

**7.11.** *Démonstration du théorème 7.5.* Toutes les assertions sont pour $p$ suffisamment grand. Nous savons que

$$\begin{aligned} Z_\psi(s,p) &= \int_{W_p} |h(x)|_p^s |dx| \\ &= \sum_{n\in\mathbb{Z}} p^{-ns} \int_{\substack{x\in W_p \\ v(h(x))=n}} |dx|. \end{aligned}$$

En appliquant $m$ fois 7.7, on obtient que $\int_{\substack{x\in W_p \\ v(h(x))=n}} |dx|$ est une somme finie d'expressions de la forme

$$\frac{1}{p^m} \sum_{\bar{a}\in\mathbb{F}_p^?} \sum_{\substack{\gamma\in\mathbb{Z}^m \\ \varphi(\bar{a},\gamma,n)}} p^{-(\gamma_1+\cdots+\gamma_m)}.$$

Par le lemme 7.9, en passant à une partition finie, nous pouvons supposer que la formule $\varphi(\bar{a}, \gamma, n)$ est de la forme $\varphi_2(\gamma, n) \wedge \varphi_3(\bar{a})$, ce qui nous donne que $Z_\psi(s, p)$ est une somme finie d'expressions de la forme

$$\frac{1}{p^m} \sum_{\substack{\bar{a}\in\mathbb{F}_p^? \\ \mathbb{F}_p\models\varphi_3(\bar{a})}} \sum_{\substack{(\gamma,n) \\ \mathbb{Z}\models\varphi_2(\gamma,n)}} p^{-ns-(\gamma_1+\cdots+\gamma_m)}$$

et le lemme 7.10 nous donne alors le résultat.

**7.12. Clôtures algébriques**. Je renvoie à 5.17 pour la définition de la clôture algébrique et de la clôture définissable d'un sous-ensemble d'un modèle. J'utiliserai la caractérisation qui en est donnée en termes d'orbites du groupe d'automorphismes d'un modèle saturé : Si $A \subset M$ et $M^*$ est une extension élémentaire de $M$ qui est saturée de cardinalité $\geq |A|^+$, alors $a \in acl(A)$ si et seulement si l'orbite de $a$ par $\mathrm{Aut}(M^*/A)$ est finie ; et $a \in dcl(A)$ si et seulement si cette orbite est réduite à $\{a\}$.

Nous savons déja que si $A \subset \mathbb{Q}_p$, et $B$ est le sous-corps de $\mathbb{Q}_p$ engendré par $A$, alors $acl(A) = B^{alg} \cap \mathbb{Q}_p$. Nous allons étendre ce résultat aux $\mathcal{L}'_{\mathrm{Pas}}$-structures modèles de $T_0$.

**Commentaires**. (1) Remarquons que la notion de clôture algébrique d'un sous-ensemble $A$ d'une $\mathcal{L}$-structure $M$, dépend non seulement de la $\mathcal{L}$-théorie de $M$, mais de la $\mathcal{L}(A)$-théorie de $M$.

(2) A priori, si on ne suppose pas l'hypothèse généralisée du continu, l'existence d'un modèle saturé (c'est-à-dire, un modèle $\kappa$-saturé de cardinal $\kappa$) contenant $\mathcal{A}$ dépend de l'existence de certains grands cardinaux. [En effet, par exemple si $M$ est la droite réelle avec l'ordre, il faudra trouver un cardinal $\kappa$ régulier (c'est-à-dire, aucune suite de cardinalité $< \kappa$ n'est cofinale dans $\kappa$), $\kappa > 2^{\aleph_0}$, et tel que pour tout $\lambda < \kappa$ on ait $2^\lambda \leq \kappa$.]

Ce problème n'en est pas vraiment un, car on pourrait tout aussi bien dire : $a \in acl(A)$ si et seulement si, dans tout extension élémentaire $M^*$ de $M$, l'orbite de $a$ par $\mathrm{Aut}(M^*/A)$ est finie. On a aussi la propriété suivante : si $f : A \to B$ est un isomorphisme élémentaire (au sens de $M$) entre deux sous-structures de $M$, alors il existe une extension élémentaire $M^*$ de $M$ dans laquelle $f$ s'étend à un automorphisme de $M^*$. J'utilise donc l'hypothèse de saturation par commodité, on peut s'en passer (voir les exercices 7.15 et 7.16 ci-dessous).

**7.13. Lemme**. Soit $\mathcal{K} = (K, \Gamma, k)$ un modèle de $T_0$, et $\mathcal{A} = (A, \Gamma_A, k_A)$ une sous-structure de $\mathcal{K}$. Nous supposerons que $A$ et $k_A$ sont des corps. Je dénote par $acl(\mathcal{A})$ les éléments de $K \cup \Gamma \cup k$ qui sont algébriques sur $\mathcal{A}$ (au sens ci-dessus) et par $A^{alg}$ les éléments (d'une clôture algébrique au sens de la théorie des corps algébriquement clos) qui satisfont une équation non triviale à coefficients dans $A$.

(1) Si $\alpha \in acl(\mathcal{A}) \cap \Gamma$, alors $\alpha$ est algébrique au-dessus de $\Gamma_A$ au sens de $\mathrm{Th}(\Gamma)$.

(2) Si $\bar{a} \in acl(\mathcal{A}) \cap k$, alors $\bar{a}$ est algébrique au-dessus de $k_A$ au sens de $\mathrm{Th}(k)$. Si $\bar{a} \in dcl(\mathcal{A}) \cap k$, alors $\bar{a}$ est définissable au-dessus de $k_A$ au sens de $\mathrm{Th}(k)$.

(3) Si $a \in acl(\mathcal{A}) \cap K$, alors $a \in A^{alg} \cap K$.

*Démonstration.* Pour utiliser la caractérisation de la clôture algébrique, nous allons supposer que $(K, \Gamma, k)$ est saturé, de cardinalité supérieure à celle de $A$.

(1) Nous savons que le groupe de valeurs de $A$ est contenu dans $\Gamma_A$. Il est clair que si $\alpha$ est algébrique sur $\Gamma_A$ au sens de $\mathrm{Th}(\Gamma)$, alors $\alpha \in acl(\mathcal{A})$. Réciproquement, supposons que $\alpha \in \Gamma$ ne soit pas algébrique sur $\Gamma_A$ au sens de $\mathrm{Th}(\Gamma)$. Par saturation de $\Gamma$, il existe donc une suite $(\alpha_i)_{i \in \mathbb{N}}$ d'éléments distincts de $\Gamma$, chaque $\alpha_i$ satisfaisant les mêmes $\mathcal{L}_{\mathrm{gp}}(\Gamma_A)$-formule que $\alpha$ ; il existe donc des $\mathcal{L}_{\mathrm{gp}}$-automorphismes $\sigma_i \in \mathrm{Aut}(\Gamma/\Gamma_A)$ tels que $\sigma_i(\alpha) = \alpha_i$ pour $i \in \mathbb{N}$. Soit $\langle \Gamma_A, \alpha \rangle$ le sous-groupe de $\Gamma$ engendré par $\Gamma_A$ et $\alpha$.

Pour $i \in \mathbb{N}$, on définit $\tau_i$ sur la sous-structure $\mathcal{A}' = (A, \langle \Gamma_A, \alpha \rangle, k_A)$ en posant $\tau_i(\alpha) = \alpha_i$, $\tau_i$ étant l'identité sur $A \cup k_A$ (et sur $\Gamma_A$ par hypothèse). Comme $\tau_i$ coïncide avec $\sigma_i$ sur $\langle \Gamma, \alpha \rangle$, par le théorème 4.1, les applications $\tau_i$ sont élémentaires au sens de $\mathrm{Th}(\mathcal{K})$, et donc se prolongent à des automorphismes de $\mathcal{K}$ puisque $\mathcal{K}$ est saturé. Cela montre que l'orbite de $\alpha$ par $\mathrm{Aut}(\mathcal{K}/\mathcal{A})$ est infinie, et donc que $\alpha \notin acl(\mathcal{A})$.

(2) On procède de la même façon pour $k_A$ : si $\bar{a}$ n'est pas algébrique sur $k_A$ au sens de $\mathrm{Th}(k)$, alors il existe des automorphismes $\sigma_i \in \mathrm{Aut}(k/k_A)$, $i \in \mathbb{N}$, tels que les éléments $\sigma_i(\bar{a})$ soient tous distincts. Si l'on définit $\tau_i$ sur $(A, \Gamma_A, k_A(\bar{a}))$ en posant $\tau_i(\bar{a}) = \sigma_i(\bar{a})$, et $\tau_i|_{\mathcal{A}} = id$, nous obtenons alors des isomorphismes partiels élémentaires, qui s'étendent à des automorphismes de $\mathrm{Aut}(\mathcal{K}/\mathcal{A})$, et $\bar{a} \notin acl(\mathcal{A})$. La preuve pour la clôture définissable est similaire (en prenant $i = 1, 2$).

(3) Nous pouvons remplacer $A$ par $A^{alg} \cap K$, et donc supposer que $A = A^{alg} \cap K$. Si $\Gamma'_A$ dénote $v(A^\times)$, et $k'_A$ le corps résiduel de $A$, alors $\Gamma/\Gamma'_A$ est sans torsion, et ${k'_A}^{alg} \cap k = k'_A$ (attention : clôture algébrique au sens des corps algébriquement clos).

**Cas 1**. $v(A(a)^\times) \not\subset \Gamma'_A$.

Soit $b \in A(a)$ tel que $v(b) = \beta \notin \Gamma'_A$. Comme $\Gamma/\Gamma'_A$ est sans torsion, nous savons que si $a_0, \ldots, a_n \in A$ alors les éléments $v(a_i) + i\beta$ sont tous distincts. Si $i_0$ est l'indice pour lequel $v(a_i) + i\beta$ est minimal, nous aurons donc

$$v(\sum_{i=0}^{n} a_i b^i) = v(a_{i_0}) + i_0\beta, \quad \overline{\mathrm{ac}}(\sum_{i=0}^{n} a_i b^i) = \overline{\mathrm{ac}}(a_{i_0})\overline{\mathrm{ac}}(b)^{i_0}.$$

Si $b' \in K$ est tel que $v(b-b') > \beta = v(b')$, alors $\overline{\mathrm{ac}}(b) = \overline{\mathrm{ac}}(b')$, les corps valués $A(b)$ et $A(b')$ sont $A$-isomorphes, et cet isomorphisme s'étend à un isomorphisme entre $(A(b), \langle \Gamma_A, \beta \rangle, k_A(\overline{\mathrm{ac}}(b)))$ et $(A(b'), \langle \Gamma_A, \beta \rangle, k_A(\overline{\mathrm{ac}}(b)))$. (Pour plus de détails, voir l'étape 5 de 4.5). Cet isomorphisme est donc élémentaire, et s'étend à un élément de $\mathrm{Aut}(\mathcal{K}/\mathcal{A})$. Comme il existe une infinité de tels $b'$, nous obtenons que $b \notin acl(\mathcal{A})$. Comme $b \in A(a)$, $a \notin acl(\mathcal{A})$.

**Cas 2**. $v(A(a)^\times) = \Gamma'_A$, $\overline{\mathrm{ac}}(A(a)) \not\subset k'_A$.

Nous raisonnons de la même façon. Soit $b \in A(a)$ tel que $\overline{\mathrm{ac}}(b) \notin k'_A$. Nous pouvons supposer que $v(b) = 0$ (puisque le groupe de valeurs de $A(a)$ est le même que celui de $A$). Nous savons que si $a_0, \ldots, a_n \in A$, alors $v(\sum_{i=0}^{n} a_i b^i) = \min\{v(a_i)\}$. Si $I$ est l'ensemble des indices sur lesquels cette valeurs minimale est atteinte, alors $\overline{\mathrm{ac}}(\sum_{i=0}^{m} a_i b^i) = \sum_{i \in I} \overline{\mathrm{ac}}(a_i)\overline{\mathrm{ac}}(b)^i$. Si $b' \in K$ satisfait $v(b - b') > 0 = v(b')$, alors $\overline{\mathrm{ac}}(b) = \overline{\mathrm{ac}}(b')$, et nous obtenons un isomorphisme partiel élémentaire entre $(A(b), \Gamma_A, k_A(\overline{\mathrm{ac}}(b)))$ et $(A(b'), \Gamma_A, k_A(\overline{\mathrm{ac}}(b)))$, qui s'étend à un automorphisme de $\mathrm{Aut}(\mathcal{K}/\mathcal{A})$ (voir l'étape 4 de 4.5). Donc $b \notin acl(\mathcal{A})$, et $a \notin acl(\mathcal{A})$.

**Cas 3**. $v(A(a)^\times) = \Gamma'_A$, $\overline{\mathrm{ac}}(A(a)) = k'_A$.

$A$ est alors une extension immédiate de $A$. Par saturation de $K$, il existe une infinité d'éléments $a' \in K$ tels que pour tout $b \in A$, $v(a' - b) = v(a - b)$ (il suffit de trouver $c \neq 0$ tel que $v(c) > \Gamma'_A$, et de prendre $a' = a + c$), et un tel élément réalise le même type que $a$ sur $\mathcal{A}$. Donc $a \notin acl(\mathcal{A})$.

**7.14. Remarque**. Comme $\Gamma$ est un groupe ordonné, tout élément qui est algébrique sur $\Gamma_A$ est aussi définissable. Par contre, le résultat ne s'étend pas à la sorte du corps valué. Par

exemple, si $K$ est algébriquement clos, alors tout sous-corps de $K$ est définissablement clos (au sens de la théorie des corps algébriquement clos), mais la valuation sur $K$ permet de distinguer les éléments de $A^{alg}$ si $A$ n'est pas Hensélien.

**7.15. Exercice**. Soit $M$ une $\mathcal{L}$-structure, et $f : A \to B$ un isomorphisme élémentaire (au sens de $M$) entre deux sous-structures de $M$. En utilisant le théorème de Keisler-Shelah donné ci-dessous, montrez qu'il existe une extension élémentaire $M^*$ de $M$ dans laquelle $f$ se prolonge à un automorphisme.

**Théorème** (Keisler-Shelah). Soient $\mathcal{L}$ un langage, $M$ et $N$ des $\mathcal{L}$-structures. Alors

$$M \equiv N \iff M^I/\mathcal{U} \simeq N^I/\mathcal{U}$$

pour un ultrafiltre $\mathcal{U}$ sur un ensemble $I$.

**7.16. Exercice**. Nous utiliserons le critère suivant de la clôture algébrique, pour $A \subset M$ :

$a \in acl(A)$ si et seulement si dans tout extension élémentaire $M^*$ de $M$, l'orbite de $a$ par $\mathrm{Aut}(M^*/A)$ est finie.

Expliquez en détail comment prouver 7.13(1) sans utiliser l'hypothèse de l'existence d'un modèle saturé contenant $\mathcal{A}$.

**7.17. Corollaire/Exercice**. Soient $\mathcal{K} = (K, \Gamma, k)$ un modèle de $T_0'$, $\mathcal{A} = (A, \Gamma_A, k_A)$ une sous-structure de $\mathcal{K}$ telle que $A$ et $k_A$ soient des corps, et $S \subset K^n \times (\Gamma \cup \{\infty\})^m \times k^\ell$ un ensemble définissable dans $\mathcal{L}'_{\mathrm{Pas}}(\mathcal{A})$.

(1) Si $\theta : S \to \Gamma \cup \{\infty\}$ est une fonction définissable (avec paramètres dans $\mathcal{A}$), alors il existe une partition finie de $S$ en sous-ensembles définissables $S_i$ tels que sur chaque $S_i$ :

   (a) ou bien $\theta$ est constante,

   (b) ou bien il existe $e \in \mathbb{N}^{>0}$, $\alpha \in \Gamma_A$ et une fonction linéaire $L$ telle que pour tout $(x, \xi, \bar{x}) \in S_i$,
   $$\theta(x, \xi, \bar{x}) = (L(\xi) + \alpha)/e,$$

   (c) ou bien il existe $e \in \mathbb{N}^{>0}$, $\alpha \in \Gamma_A$, une fonction linéaire $L$ et des polynômes $f_1(X)$, $f_2(X)$ à coefficients dans le corps engendré par $A$, tels que pour tout $(x, \xi, \bar{x}) \in S_i$,
   $$\theta(x, \xi, \bar{x}) = (L(\xi) + \alpha + v(f_1(x)) - v(f_2(x)))/e.$$

(2) Si $g : S \to k$ est une fonction définissable (avec paramètres dans $\mathcal{A}$), alors il existe une partition finie de $S$ en sous-ensembles définissables $S_i$ tels que sur chaque $S_i$,

   (a) ou bien $g$ est constante,

   (b) ou bien il existe une fonction définissable $f : k^{\ell+r} \to k$ (dans le langage $\mathcal{L}_{\mathrm{c.rés}}(k_A)$) et des polynômes $f_1(X), \ldots, f_r(X)$ à coefficients dans le sous-corps de $K$ engendré par $A$, tels que pour tout $(x, \xi, \bar{x}) \in S_i$,
   $$g(x, \xi, \bar{x}) = f(\bar{x}, \overline{\mathrm{ac}}(f_1(x)), \ldots, \overline{\mathrm{ac}}(f_r(x))).$$

**7.18.** Ce résultat permet de généraliser les résultats d'intégration à des fonctions définissables $S \to \Gamma$. Supposons que $k$ soit muni d'une mesure $\bar{\mu}$, suffisamment uniforme, et ayant de bonnes propriétés (par exemple, si $k$ est un ultraproduit de corps finis, on sait qu'une telle mesure existe ; elle est définie sur les sous-ensembles définissables de $k^n$, et a des propriétés de définissabilité). Prenons maintenant un réel $r > 1$. On peut alors définir une mesure sur $k((t))$, en définissant $\mu(k[[t]]) = \bar{\mu}(k)$, et si $A \subset k$ est définissable, et $S = \{x \in k((t)) \mid \overline{\mathrm{ac}}(x) \in A,\ v(x) = n\}$, alors $\mu(S) = \bar{\mu}(A)r^{-n}$. Puis définir des intégrales de fonctions définissables, et obtenir des résultats similaires à ceux de 7.5. Mais en fait, rien n'interdit de remplacer $r$ par un élément $\mathbb{T}$, et au lieu de prendre une mesure $\bar{\mu}$, de prendre n'importe quelle fonction $\bar{\mu}$ définie sur les sous-ensembles définissables de $k$ (ou de $k^n$), et à valeurs dans un anneau ayant de bonnes propriétés. C'est ce qu'on fait en intégration motivique. Pour des applications du théorème de Pas à l'intégration motivique, voir les nombreux articles de Denef et Loeser, puis de Cluckers et Loeser, accessibles sur la page Web de Loeser (`http://www.dma.ens.fr/∼loeser/`).

# 8 Corps valués avec un automorphisme - le résultat de Bélair-Macintyre-Scanlon

Nous avons vu dans la sous-section 5.3 que si $A$ est un anneau de valuation discret, qui est complet, d'idéal maximal engendré par $p$ et tel que $k = A/(p)$ est parfait, alors il existe un unique sous-ensemble multiplicatif $S$ de $A$ tel que la projection $A \to k$ induit une bijection entre $S$ et le corps $k$. De plus, tout élément de $A$ s'écrit de façon unique comme $\sum_{i=0}^{\infty} a_i p^i$, où $a_i \in S$. L'anneau $A$ est appelé l'*anneau de Witt* à coefficients dans $k$, et noté $W[k]$. Je note son corps de fraction $W(k)$, on aura $W(k) = W[k][1/p]$. Tout élément $a$ de $W(k)$ s'écrit donc $\sum_{i \geq i_0} a_i p^i$, où $i_0 = v(a) \in \mathbb{Z}$.

L'automorphisme de Frobenius $x \mapsto x^p$ se relève de façon unique en un automorphisme $\sigma$ de $W(k)$, en posant $\sigma(\sum_{i \geq i_0} a_i p^i) = \sum_{i \geq i_0} a_i^p p^i$.

L. Bélair, A. Macintyre et T. Scanlon étudient la théorie de ce corps valué avec automorphisme, et montrent une élimination des quantificateurs dans un langage inspiré du langage de Pas[3]. Je vais donner une partie de la preuve.

## 8.1 Corps aux différences

**8.1. Définitions et notations**.

(1) Un corps aux différence est un corps muni d'un automorphisme distingué, que je noterai en général $\sigma$.

(2) Soit $K$ un corps aux différence. L'anneau des polynômes aux différence sur $K$ (en 1 variable), noté $K[X]_\sigma$, est l'anneau de polynômes en $X = X_0, X_1, \ldots$, auquel on étend $\sigma$

[3]L. Bélair, A. Macintyre et T. Scanlon, *Model Theory of the Frobenius on the Witt vectors*, Amer. J. of Math., vol. 129 No. 3(2007), 665 – 721.

en posant $\sigma(X_i) = X_{i+1}$ pour $i \in \mathbb{N}$. (Cette définition se généralise à plusieurs variables de la manière évidente).

(3) Pour des questions de notation, si $f(X) = F(X_0, \ldots, X_n) \in K[X]_\sigma$ et $i \in \mathbb{Z}$, nous allons noter $\sigma^i(f)(X)$ le polynôme $\sigma^i(F)(X_0, \ldots, X_n)$, le polynôme obtenu en appliquant $\sigma^i$ aux coefficients de $F$. On a alors $\sigma^i(f(X)) = \sigma^i(f)(\sigma^i(X))$.

(4) Si $\ell = (\ell_0, \ldots, \ell_n) \in \mathbb{N}^{n+1}$ est un multi-indice, nous noterons $X^\ell$ le monôme $\prod_{i=0}^n X_i^{\ell_i}$, et pour un élément $a$, $a^\ell$ l'élément $\prod_{i=0}^n \sigma^i(a^{\ell_i})$. Le module de $\ell$, $|\ell|$, est égal à $\sum_{i=0}^n \ell_i$.

(5) Nous utiliserons aussi le développement de Taylor en plusieurs variables, une généralisation de celui introduit en 3.1. Fixons un entier $n$, et deux multi-indices $j, \ell \in \mathbb{N}^{n+1}$. Nous définissons $D_\ell(X^j)$ comme le coefficient de $Y^\ell$ dans le développement de $(X+Y)^j$, où $X = (X_0, \ldots, X_n)$, $Y = (Y_0, \ldots, Y_n)$. Si $R$ est un anneau, nous étendons par linéarité aux éléments de $R[X]$, et nous avons alors, si $f(X) \in R[X]$,

$$f(X+Y) = \sum_{\ell \in \mathbb{N}^{n+1}} D_\ell(f)(X) Y^\ell.$$

En caractéristique 0, $D_\ell(f)(X)$ est un multiple rationnel de $\frac{\partial^{|\ell|} f}{\partial X^\ell}(X)$. Dans tous les cas, on calcule cependant qu'on a

$$D_\ell(D_j(f)) = \binom{\ell + j}{j} D_{\ell+j}(f),$$

avec

$$\binom{\ell}{j} = \binom{\ell_0}{j_0}\binom{\ell_1}{j_1}\cdots\binom{\ell_n}{j_n}.$$

**8.2. Quelques propriétés faciles**. Soient $K \subset L$ des corps de différence, et $a \in L$. Si $f(X) \in K[X]_\sigma$, le plus petit entier tel que $f(X)$ s'écrive $F(X_0, \ldots, X_n)$ est appelé *ordre de* $f$ ; on définit alors $f(a) := F(a, \sigma(a), \ldots, \sigma^n(a))$.

Supposons qu'il existe $f(X) \neq 0$ qui s'annule en $a$, et prenons un tel $f$ d'ordre minimal. Alors le polynôme associé dépend de $X_0$ : sinon, alors $f(a) = F(\sigma(a), \ldots, \sigma^n(a))$ pour un $F(X) \in K[X_1, \ldots, X_n]$. Si on pose $g(X) = \sigma^{-1}(f(X))$, alors on a $g(a) = 0$, et $g$ est d'ordre $n-1$, ce qui contredit la minimalité de l'ordre de $f$.

On remarque ensuite que pour tout $i \in \mathbb{Z}$, on a $\sigma^i(f(a)) = 0 = \sigma^i(f)(\sigma^i(a))$. On montre alors de proche en proche que $K(\sigma^i(a))_{i\in\mathbb{Z}} \subset K(a, \sigma(a), \ldots, \sigma^{n-1}(a))^{alg}$, et est donc de degré de transcendance $n$ sur $K$.

S'il n'existe pas de tel $f(X)$, les éléments $\sigma^i(a)$, $i \in \mathbb{Z}$, sont algébriquement indépendants sur $K$. Dans le premier cas on dira que $a$ est *transformellement algébrique sur* $K$ (ou *$\sigma$-algébrique*), dans le deuxième, que $a$ est *transformellement transcendant* (*$\sigma$-transcendant*) sur $K$.

## 8.2 Description des corps considérés, du langage, et des théories

**8.3. Coefficients angulaires d'ordre supérieur**. Soit $K$ un corps valué dont le groupe de valeurs $\Gamma$ a un plus petit élément positif 1. Si $\pi \in K$ est de valuation 1, et $\mathcal{O}$ est l'anneau de valuation de $K$, on a alors des applications naturelles

$$\mathrm{res}_n : \mathcal{O} \to \mathcal{O}/\pi^n\mathcal{O}, \qquad \pi_{n,m} : \mathcal{O}/\pi^m\mathcal{O} \to \mathcal{O}/\pi^n\mathcal{O} \qquad \text{pour } n < m,$$

satisfaisant $\mathrm{res}_n = \pi_{n,m} \circ \mathrm{res}_m$. Pour $n = 1$, nous obtenons alors notre application résiduelle habituelle res .

Un coefficient angulaire d'ordre $n$ est une application multiplicative $\overline{\mathrm{ac}}_n : K \to \mathcal{O}/\pi^n\mathcal{O}$ satisfaisant $\overline{\mathrm{ac}}_n(x) = 0 \iff x = 0$, et qui, sur $\mathcal{O}$, coïncide avec $\mathrm{res}_n$. Nous imposons de plus des compatibilités avec les fonctions résiduelles : si $n < m$, alors $\pi_{n,m} \circ \overline{\mathrm{ac}}_m = \overline{\mathrm{ac}}_n$. Dans le cas de $K = \mathbb{Q}_p$, on utilisera $\overline{\mathrm{ac}}_n(x) = \mathrm{res}_n(p^{-v(x)}x)$.

**8.4. Remarque** Il suffit de connaître les coefficients angulaires sur un ensemble $S_0$ tel que $v(S_0)$ engendre le groupe de valeurs de $K$. En effet, la condition de multiplicativité entraîne que nous connaissons alors les coefficients angulaires sur le sous-groupe multiplicatif $S$ engendré par $S_0$ ; puis on utilise que tout élément non nul de $K$ s'écrit comme le produit d'un élément de $S$ par un élément de valuation 0.

**8.5. Contexte de l'étude**. Nous étudions des corps $(K, v, \sigma)$ ayant les propriétés suivantes :

(1) $(K, v)$ est un corps valué de caractéristique 0, d'anneau de valuation $\mathcal{O}$, de corps résiduel $k$ et de groupe de valeurs $\Gamma$, muni d'une application coefficient angulaire $\overline{\mathrm{ac}} : K \to k$.

(2) $\sigma \in \mathrm{Aut}(K)$, et pour tout $x$, $v(\sigma(x)) = v(x)$. On notera $\bar{\sigma}$ l'automorphisme de $k$ induit par $\sigma$.

(3) ($K$ a suffisamment de constantes) $\forall x\ \exists y\ \sigma(y) = y \wedge v(x) = v(y)$.

(4) ($k$ est linéairement $\sigma$-clos) Pour tout $n \in \mathbb{N}$, $\forall a_0, \ldots, a_n, b \in k\ \exists y \in k\ \sum_i a_i\sigma^i(y) = b$.

($5_p$) Si la caractéristique de $k$ est $p > 0$, alors $v(p)$ est le plus petit élément positif de $\Gamma$, et $K$ est muni de coefficients angulaires $\overline{\mathrm{ac}}_n : K \to \mathcal{O}/p^n\mathcal{O}$, $n \in \mathbb{N}$, qui satisfont $\overline{\mathrm{ac}}_n(p) = 1$.

($6_0$) Si la caractéristique de $k$ est nulle, alors pour tout $n \in \mathbb{N}$ et $f(Y) \in k[Y]_\sigma$ d'ordre $\leq n$, $\forall a_0, \ldots, a_n, b \in k\ \exists y \in k\ \sum_i a_i\sigma^i(y) = b \wedge f(y) \neq 0$.

($6_p$) Si la caractéristique de $k$ est $p > 0$, alors $\bar{\sigma}(x) = x^p$.

(7) ($\sigma$-Hensel) Si $f(X) \in \mathcal{O}_v[X]_\sigma$, $f(X) = F(X_0, \ldots, X_n)$, et $a \in \mathcal{O}$ est tel que pour un indice $i \leq n$, $v(f(a)) = \gamma > 0 = v(\frac{\partial F}{\partial X_i}(a))$, alors il existe $b \in \mathcal{O}$, $v(b - a) = \gamma$, et tel que $f(b) = 0$.

(8) Si $a \in k$ n'est pas nul, alors il existe $b \in k$ non nul tel que $\sigma(b) = ab$.

**8.6. Remarque** Si la caractéristique de $k$ est $p > 0$, l'anneau $\mathcal{O}/p^n\mathcal{O}$ est appelé l'anneau des *vecteurs de Witt de longueur* $n$, est noté $W_n(k)$, et est interprétable dans $k$. Cela suit de la discussion faite en 5.11, mais voir aussi les textes classiques pour plus de détails.

Cependant, l'application $\mathrm{res}_n : \mathcal{O} \to \mathcal{O}/p^n\mathcal{O} = W_n(k)$ n'est pas nécéssairement définissable dans le langage. Elle l'est cependant dans notre contexte :

**Lemme**. Soit $K$ un corps valué avec un automorphisme, de caractéristique résiduelle $p > 0$, et satisfaisant les axiomes (1) – (7) ci-dessus. Alors la formule $\sigma(x) = x^p$ définit un ensemble $S$ sur lequel la fonction res définit une bijection avec $k$.

*Démonstration.* On voit tout d'abord que si $\sigma(a) = a^p$ et $a \neq 0$, alors $v(a) = 0$. On considère maintenant l'équation $\sigma(X) - X^p = 0$ ; si $a \in \mathcal{O}$ est de valuation 0, alors $v(\sigma(a) - a^p) > 0$, la dérivée en $\sigma(X)$ est 1, et par $\sigma$-Hensel, il existe donc $b \in \mathcal{O}$ tel que $\sigma(b) = b^p$, et $v(a - b) > 0$. Cela montre que tout élément de $k$ est atteint, il reste maintenant à montrer que res est injective sur $S$. Pour cela il suffit de montrer que si $v(a - 1) > 0$ et $\sigma(a) = a^p$ alors $a = 1$ : écrivons $a = 1 + u$ avec $v(u) > 0$. Alors $\sigma(a) = (1 + u)^p = 1 + \sigma(u)$, d'où $u^p + \sum_{i=1}^{p-1} \binom{p}{i} u^i = \sigma(u)$. Mais comme $\binom{p}{i}$ est divisible par $p$ pour $0 < i < p$, et que $v(\sigma(u)) = v(u)$, on obtient que nécessairement $u = 0$. □

On peut alors définir $s : \mathcal{O} \to k^n$, en posant $s(a) = (a_1, \ldots, a_n)$, où l'on définit $a_1, \ldots, a_n$ par induction de la façon suivante : $a_1 = \mathrm{res}\,(a)$ ; supposons $a_1, \ldots, a_i$ définis, et prenons $b_1, \ldots, b_i \in \mathcal{O}$ satisfaisant $\sigma(x) = x^p$ et $\mathrm{res}\,(b_j) = a_j$ pour $j = 1, \ldots, i$, puis définissons $a_{i+1} = \mathrm{res}\,(p^{-i}(a - \sum_{j=1}^{i} b_j p^{j-1}))$.

Notons que les applications $\pi_{n,m}$ correspondent tout simplement à la projection $k^m \to k^n$ sur les $n$ premières coordonnées.

**8.7. Le langage utilisé**. Nous travaillerons dans une variante de langage à 3 sortes de Pas. Nous avons les 3 sortes habituelles : celle du corps valué $K$, de son groupe de valeurs $\Gamma$ et de son corps résiduel $k$. Les langages sont des langages étendus :

- $\mathcal{L}'_{\text{c.val}} = \{+, -, \cdot, 0, 1, \sigma\}$,
- $\mathcal{L}'_{\text{gp}}$ contient $\{+, -, 0, \infty\}$,
- $\mathcal{L}'_{\text{c.rés}}$ contient $\{+, -, \cdot, 0, 1, \bar{\sigma}\}$.

Dans le cas de caractéristique résiduelle $p > 0$, nous aurions pu omettre le symbole $\bar{\sigma}$, puisque $\bar{\sigma}$ sera définissable dans le langage de corps, mais nous ne le ferons pas.

Nous avons aussi des symboles de fonctions $v : K \to \Gamma \cup \{\infty\}$, $\overline{\mathrm{ac}} : K \to k$, res $: \mathcal{O} \to k$, et si la caractéristique est positive, des applications $\overline{\mathrm{ac}}_n : K \to k^n$ et $\mathrm{res}_n : \mathcal{O} \to k^n$. Comme remarqué ci-dessus, les applications $\pi_{n,m}$ correspondent aux projections naturelles $k^m \to k^n$ quand $n < m$.

**8.8. La théorie considérée**. Nous exprimons dans le langage décrit dans 8.7 les propriétés décrites dans 8.5. Pour exprimer les propriétés des coefficients angulaires quand la caractéristique résiduelle est positive, on se sert des remarques faites en 8.6. Ou bien, si on préfère, on peut aussi rajouter des sortes au langage : pour chaque $n$ on rajoute une sorte pour $\mathcal{O}/p^n\mathcal{O}$, ainsi que les fonctions $\overline{\mathrm{ac}}_n : K \to \mathcal{O}/\pi^n\mathcal{O}$, et $\pi_{n,m} : \mathcal{O}/p^m\mathcal{O} \to \mathcal{O}/p^n\mathcal{O}$ pour $n < m$. Cela nous donne une théorie $T_0$.

Enfin, nous ajoutons à cette théorie $\mathrm{Th}_{\mathcal{L}'_{\text{c.rés}}}(k) \cup \mathrm{Th}_{\mathcal{L}'_{\text{gp}}}(k)$ pour obtenir la théorie $T$.

**Théorème** (Bélair, Macintyre, Scanlon). La théorie $T$ décrite ci-dessus élimine les quantificateurs du corps valué, et est complète.

Remarquons tout de suite que la complétude résulte de l'élimination des quantificateurs : la théorie $T$ décrit précisément la structure engendrée par les constantes du langage : c'est une structure $(\mathbb{Z}, \Gamma_0, k_0)$, où $\Gamma_0$ et $k_0$ sont les structures engendrées par les constantes des langages $\mathcal{L}'_{\text{gp}}$ et $\mathcal{L}'_{\text{c.rés}}$ respectivement. Nous avons $v(p) = 0$ si la caractéristique résiduelle est nulle ; les fonctions $\overline{\text{ac}}$ et $\overline{\text{ac}}_n$ coïncident avec les fonctions res , res $_n$ sur les éléments de valuation 0, et quand $v(p) = 1$, nous savons que $\overline{\text{ac}}_n(p) = 1$ pour tout $n$.

La preuve est longue (c'est un euphémisme), le cas le plus difficile étant celui des extensions immédiates. Je vais essayer de vous montrer quelques points pas trop difficiles. Je vais commencer par montrer que certains corps de fractions de Witt sont modèles de la théorie $T$.

## 8.3 Quelques résultats annexes

**8.9. Une remarque simple et utile**. Soit $f(X) = F(X_0, \ldots, X_n) \in K[X]_\sigma$. Si $|\ell| = 1$, alors une seule coordonée de $\ell$ est non nulle, et est égale à 1. Si c'est la $i$-ième, alors

$$D_\ell(f)(X) = \frac{\partial F}{\partial X_i}(X).$$

**8.10. Proposition**. Soit $k$ un corps parfait de caractéristique $p > 0$, et n'ayant pas d'extension de degré $p$, et qui est clos par racine $(p-1)$-ième. Soit $\sigma \in \text{Aut}(W(k))$ le relèvement du Frobénius $x \mapsto x^p$. Alors $(W(k), \mathbb{Z}, k)$ est un modèle de $T$.

*Démonstration.* (1) – (3) sont clairs, puisque les puissances de $p$ sont fixées par $\sigma$. Pour (4) : comme $\bar{\sigma}$ est $x \mapsto x^p$, cela se réduit à montrer que les équations $\sum_{i=0}^n a_i X^{p^i} = b$ ont toujours une solution. Mais étant donné un corps $k$ de caractéristique $p$, le corps de décomposition d'une telle équation est de degré sur $k$ divisant $p^n$, et dans notre cas est donc de degré 1. $(6_p)$ est clair aussi. Il reste à montrer l'axiome de $\sigma$-Hensel.

Soit $f(X) = F(X_0, \ldots, X_n) \in W[k][X]_\sigma$, et $a \in W[k]$ tel que $v(f(a)) > 0$ et pour un indice $i$, on a $\frac{\partial F}{\partial X_i}(a)$ est de valuation nulle. Nous allons montrer que nous pouvons trouver $a_1$ tel que $v(a - a_1) = v(f(a)) < v(f(a_1))$.

Soit $i = v(f(a))$, et considérons $g(Y) = f(a + p^i Y)$. La formule de Taylor nous donne

$$g(Y) = f(a) + \sum_{|\ell|=1} D_\ell(f)(a) p^i Y^\ell + \sum_{|\ell|\geq 2} D_\ell(f)(a) p^{i|\ell|} Y^\ell,$$

et nous voyons que tous les coefficients ont valuation $\geq i$. Donc $p^{-i} g(Y) \in W[k][Y]_\sigma$. Nous voulons résoudre l'équation

$$p^{-i} f(a) + \sum_{|\ell|=1} D_\ell(f)(a) Y^\ell \equiv 0 \text{ mod } p.$$

C'est possible puisque $k$ satisfait l'axiome (4) ; si $c$ est une solution de cette équation, alors $a_1 = a + p^i c$ est l'élément cherché. De plus, en appliquant Taylor, on montre facilement que si

$g(X) \in \mathcal{O}[X]_\sigma$, et $a, a_1 \in \mathcal{O}$ sont tels que $v(a - a_1) > 0$, alors $v(g(a) - g(a_1)) > 0$. Dans notre cas, puisque $v(\frac{\partial F}{\partial X_i}(a)) = 0$, cela donne $v(\frac{\partial F}{\partial X_i}(a_1)) = 0$ aussi.

Nous pouvons donc répéter ce raisonnement, et construire par induction une suite $(a_n)$ d'éléments de $W[k]$ telle que $v(f(a_n)) = v(a_{n+1} - a_n) < v(f(a_{n+1})$. Comme le groupe de valeurs est $\mathbb{Z}$, cette suite est une suite de Cauchy, et elle a une limite dans notre corps complet $W[k]$. La limite, $b$, satisfait alors $f(b) = 0$ et $v(a - b) > 0$.

**8.11. Une autre version de $\sigma$-Hensel**. Voici une autre version de l'axiome (7), qui lui est équivalente :

(7′) Soient $f(X) = F(X_0, \ldots, X_n) \in K[X]_\sigma$, $a \in K$, et posons

$$\gamma = v(f(a)) - \min_{|\ell|=1} v(D_\ell(f)(a)).$$

Supposons de plus que pour tout multi-indice $\ell$ de module $j > 1$, on ait $v(f(a)) < j\gamma + v(D_\ell(f)(a))$. Alors il existe $b \in K$ tel que $v(a - b) = \gamma$, et $f(b) = 0$.

*Démonstration.* (7′) implique (7) est clair. Pour l'autre direction, prenons $c$ tel que $v(c) = \gamma$ et $\sigma(c) = c$. Nous voulons trouver $y$ de valuation nulle et tel que $f(a + cy) = 0$. Nous appliquons la formule de Taylor :

$$f(a + cY) = f(a) + \sum_{|\ell|=1} D_\ell(f)(a) c Y^\ell + \sum_{|\ell|>1} D_\ell(f)(a) c^{|\ell|} Y^\ell.$$

Ici nous utilisons que comme $\sigma(c) = c$, nous avons $(cY)^\ell = c^{|\ell|} Y^\ell$. Divisons par $c$, nous obtenons

$$g(Y) = c^{-1} f(a + cY) = c^{-1} f(a) + \sum_{|\ell|=1} D_\ell(f)(a) Y^\ell + \sum_{|\ell|>1} c^{|\ell|-1} D_\ell(f)(a) Y^\ell.$$

Alors, tous les coefficients sont de valuation $\geq 0$. De plus, $c^{-1} f(a)$ est de valuation nulle, et dans la première somme de droite nous avons aussi un coefficient de $Y^\ell$ de valuation nulle (par définition de $\gamma = v(c)$) ; par contre, tous les coefficients de $Y^\ell$ dans la deuxième somme de droite sont de valuation strictement positive. Si $\ell$ est de module 1 et tel que $v(D_\ell(f)(a)) = 0$, et si $i$ est l'unique coordonnée de $\ell$ qui est non nulle, nous avons donc que $v(\frac{\partial G}{\partial X_i}(0)) = 0 < v(g(0))$, c'est-à-dire, nous pouvons appliquer (7).

## 8.4 Début de la preuve du théorème 8.8

**8.12. Stratégie** La technique de preuve est celle utilisée pour la démonstration du théorème de Pas 4.1. Nous avons deux modèles $\kappa$-saturés $(K, \Gamma_K, k_K)$ et $(L, \Gamma_L, k_L)$ de notre théorie ($\kappa$ grand, $> 2^{\aleph_0}$ ?), ainsi que deux sous-structures $(A, \Gamma_A, k_A)$ et $(B, \Gamma_B, k_B)$ et un isomorphisme partiel $f$ entre ces deux sous-structures tel que $f|_{\Gamma_A}$ soit élémentaire au sens de $\mathrm{Th}_{\mathcal{L}'_{\mathrm{gp}}}(\Gamma_K)$, et $f|_{k_A}$ soit élémentaire au sens de $\mathrm{Th}_{\mathcal{L}'_{\mathrm{c.rés}}}(k_K)$. Nous avons une sous-structure élémentaire $(C, \Gamma_C, k_C)$ de $(K, \Gamma_K, k_K)$, de taille $< \kappa$, et nous voulons prolonger $f$ à $(C, \Gamma_C, k_C)$. Cela nous donnera le résultat.

**8.13. Etapes 0 à 3** Nous commençons par les étapes les plus faciles.

**Etape 0**. On peut supposer que $A$ et $k_A$ sont des corps aux différence.

Le fait que $f$ s'étende de façon unique au corps des fractions de $A$ et de $k_A$ en respectant les fonctions $v$ et $\overline{\text{ac}}$ est montré exactement comme dans 4.7. Pour montrer que $f$ s'étend à $\bigcup_n \bar{\sigma}^{-n}(k_A)$ et à $\bigcup_{n>0} \sigma^{-n}(A)$, il suffit de montrer qu'on peut l'étendre à $\bar{\sigma}^{-1}(k_A)$ et à $\sigma^{-1}(A)$. Mais c'est très simple : si $a \in A$, on pose $f(\sigma^{-1}(a)) = \sigma^{-1}(f(a))$, si $\bar{a} \in k_A$, on pose $f(\bar{\sigma}^{-1}(\bar{a})) = \bar{\sigma}^{-1}(f(\bar{a}))$. Comme $(\sigma, id, \bar{\sigma})$ définit un automorphisme de $(K, \Gamma_K, k_K)$, on obtient que $f$ est bien un isomorphisme.

**Etapes 1 et 2**. On peut supposer que $k_A = k_C$ et $\Gamma_A = \Gamma_C$.

Preuve identique à celle donnée dans 4.7.

**Etape 3**. On peut supposer que $A$ est Hensélien.

Nos hypothèses sur $K$ entraînent que la clôture Hensélienne $A^h$ d'un sous-corps $A$ de $K$ est l'unique extension immédiate maximale algébrique de $A$. L'isomorphisme $f|_A$ s'étend donc (uniquement) à un isomorphisme de corps valués entre $A^h$ et $B^h$ ; comme $A^h/A$ est immédiate, cette extension respecte les fonctions $\overline{\text{ac}}$ et $\overline{\text{ac}}_n$. Il reste à vérifier qu'elle respecte $\sigma$. Pour cela, on remarque que $A^h$ peut être construite comme une tour d'extensions, chaque extension étant obtenue en rajoutant une solution à une instance du lemme de Hensel, par exemple, pour la première extension : il existe $g(T) \in \mathcal{O}_A[T]$ et $a \in \mathcal{O}_A$ tels que $v(g(a)) > 0 = v(g'(a))$, et on ajoute l'unique solution $a' \in C$ de $g(T) = 0$ telle que $v(a - a') > 0$. Alors

- $\sigma(a')$ est l'unique solution de $g^\sigma(T) = 0$ telle que $v(T - \sigma(a)) > 0$,
- $f(a')$ est l'unique solution de $g^f(T) = 0$ telle que $v(T - f(a)) > 0$,
- $f(\sigma(a'))$ est l'unique solution de $g^{f\sigma}(T) = 0$ telle que $v(T - \sigma(f(a))) > 0$,

ce qui entraîne que $f(\sigma(a')) = \sigma(f(a'))$.

**8.14.** Nous aimerions maintenant prolonger $f$ à un sous-corps de $C$ ayant $k_C$ comme corps résiduel. Malheureusement, ça ne marche pas complètement. Notons $k'_A$ le corps résiduel de $A$, et choisissons $\bar{a} \in k_A$, $\bar{a} \notin k'_A$.

Voici le résultat partiel que l'on obtient :

**Etape 4 - a**. Nous pouvons trouver $a \in C$ et $b \in L$ tels que $\text{res}(a) = \bar{a}$ et $f|_A$ s'étend à un isomorphisme de corps valués de différence $A(a)_\sigma \to L$ (ici, $A(a)_\sigma$ dénote $A(\sigma^i(a))_{i\in\mathbb{Z}}$). Dans chacun des cas suivants, l'extension $A(a)_\sigma/A$ sera non ramifiée, ce qui entraîne que notre nouvel isomorphisme préserve aussi les fonctions coefficients angulaires.

(a) si $\bar{a}$ est $\sigma$-transcendant sur $k'_A$,

(b) si ($A$ est Hensélien et) $\bar{a}$ est algébrique sur $k'_A$,

(c) si $tr.deg(k'_A(\bar{a})_\sigma/k'_A) = n$, et $\bar{a} \in k'_A(\bar{\sigma}(\bar{a}), \ldots, \bar{\sigma}^n(\bar{a}))$, $\bar{\sigma}^n(\bar{a}) \in k'_A(\bar{a}, \ldots, \bar{\sigma}^{n-1}(\bar{a}))$,

(d) si $v(A^\times)$ est pur dans $\Gamma_C$, c'est-à-dire, si $\Gamma_C/v(A^\times)$ est sans torsion.

*Démonstration.* Supposons d'abord que $\bar{a}$ soit $\sigma$-transcendant sur $k'_A$, et prenons n'importe quel $a \in C$ tel que $\operatorname{res} a = \bar{a}$. Alors $a$ est $\sigma$-transcendant sur $A$, l'extension $A(a)_\sigma/A$ est purement transcendante et purement résiduelle. Si $b \in L$ est tel que $\operatorname{res} b = f(\bar{a})$, alors $b$ est $\sigma$-transcendant sur $B$, $B(b)_\sigma/B$ est purement transcendante et purement résiduelle. L'isomorphisme $f$ s'étend donc à $A(a)_\sigma$ en envoyant $a$ sur $b$.

Supposons maintenant que $\bar{a}$ soit $\bar{\sigma}$-algébrique sur $k'_A$, et soit $\bar{g}(X) = \bar{G}(X_0, \ldots, X_n) \in k'_A[X]_\sigma$ d'ordre minimal et irréductible (non nul) s'annulant en $\bar{a}$. Si $n = 0$, nous étendrons d'abord $f$ à $A^h$ en utilisant l'étape 3, c'est-à-dire, nous supposerons que $A$ est Hensélien.

Relevons $\bar{g}(X)$ en $g(X) = G(X_0, \ldots, X_n) \in \mathcal{O}_A[X]_\sigma$ de telle façon que tout coefficient non nul de $g(X)$ s'envoie par res sur un coefficient non nul de $\bar{g}(X)$. Remarquons ensuite que comme $k'_A$ est parfait, l'extension $k'_A(\bar{a}, \ldots, \bar{\sigma}^n(\bar{a}))/k'_A$ est séparable. Il existe donc un indice $i$ tel que

$$\frac{\partial \bar{G}}{\partial X_i}(\bar{a}) \neq 0,$$

et nous pouvons appliquer l'axiome de $\sigma$-Hensel à n'importe quel relèvement de $\bar{a}$ pour trouver un élément $a \in C$ tel que $g(a) = 0$ et $\operatorname{res} a = \bar{a}$.

Soit $b \in L$ satisfaisant $g^f(X) = 0$ et $\operatorname{res} b = f(\bar{a})$, et posons $f(\sigma^i(a)) = \sigma^i(b)$ pour $0 \leq i \leq n$. Nous allons montrer que $f$ s'étend à un isomorphisme de corps valués de différence défini sur $A(a)_\sigma$. Tout d'abord, $f$ définit un isomorphisme de corps valués entre $A(a, \ldots, \sigma^n(a))$ et $B(b, \ldots, \sigma^n(b))$. Cet isomorphisme s'étend en un isomorphisme $\tilde{f}$ de corps valués entre les clôtures algébriques de $A(a, \ldots, \sigma^n(a))$ et de $B(b, \ldots, \sigma^n(b))$. Il suffit de montrer que pour tout $i \in \mathbb{Z}$, nous avons $\tilde{f}(\sigma^i(a)) = \sigma^i(b)$. Comme $\bar{G}$ et $G$ sont irréductibles, nous savons que

$$\frac{\partial G}{\partial X_0}(a) \neq 0, \ \frac{\partial G}{\partial X_n}(a) \neq 0.$$

Dans le cas où la caractéristique résiduelle est nulle, ces deux éléments sont de valuation 0, et nous traiterons d'abord ce cas. Soit $H_n(T) = G(a, \ldots, \sigma^{n-1}(a), T)$. Nous savons que $\sigma^n(a)$ est l'unique solution de $H_n(T) = 0$ qui satisfasse $\operatorname{res}(T) = \bar{a}$. Donc, pour tout $i \in \mathbb{N}$, nous avons :

- $\sigma^i(a)$ est l'unique solution de $H_n^{\sigma^i}(T) = 0$ telle que $v(T - \sigma^i(a)) > 0$,
- $b$ est l'unique solution de $H_n^f(T) = 0$ telle que $v(T - f(a)) > 0$,
- $f(\sigma^i(b))$ est l'unique solution de $H^{f\sigma^i}(T) = 0$ telle que $v(T - \sigma^i(f(a))) > 0$,

ce qui montre, par induction sur $i$, que $\tilde{f}(\sigma^i(a)) = \sigma^i(b)$ pour $i \in \mathbb{N}$. On raisonne de la même façon avec $H_0(T) = G(T, \sigma(a), \ldots, \sigma^n(a))$ pour obtenir $\tilde{f}(\sigma^i(a)) = \sigma^i(b)$ pour $i < 0$.

Regardons maintenant le cas où la caractéristique résiduelle est $p > 0$. Si $\bar{G}$ est séparable en $X_n$, on raisonne comme précedemment pour conclure que $\tilde{f}(\sigma^i(a)) = \sigma^i(b)$ pour $i > n$ ; sinon il existe $m$ tel que $\bar{G}$ s'écrive comme un polynôme en $X_0, \ldots, X_{n-1}, X_n^{p^m}$. Le choix du relèvement $G$ de $\bar{G}$ entraîne alors qu'il existe $n \in \mathbb{N}$ et $H(T) \in \mathcal{O}_A[a, \sigma(a), \ldots, \sigma^{n-1}(a), T]$ tels que $\operatorname{res}(H)(T)$ soit séparable et $G(a, \ldots, \sigma^{n-1}(a), X_n) = H(X_n^{p^m})$. Alors

$$v\big(\frac{\partial G}{\partial X_n}(a)\big) = v(p^m H'(\sigma^n(a))) = m,$$

d'où nous déduisons que pour tout $i \geq 0$,

– $\sigma^{n+i}(a)$ est l'unique solution de $H^{\sigma^i}(T^{p^m}) = 0$ telle que $v(T - \sigma^{n+i}(a)) > m$,
– $b$ est l'unique solution de $H^f(T^{p^m}) = 0$ telle que $v(T - f(a)) > m$,
– $f(\sigma^{n+i}(b))$ est l'unique solution de $H^{f\sigma^i}(T^{p^m}) = 0$ telle que $v(T - \sigma^{n+i}(f(a))) > m$.

Raisonnant comme dans le cas précédent, nous obtenons le résultat.

Sans hypothèses nous avons donc montré que $f$ s'étend à un isomorphisme de corps valués aux différences, qui respecte d'ailleurs le langage à trois sortes (sans les coefficients angulaires). Si l'extension $A(a)_\sigma/A$ est non ramifiée, nous savons que cet isomorphisme respecte nécéssairement les fonctions coefficients angulaires.

Il est clair que $A(a)_\sigma/A$ est non ramifiée dans le cas (a) (car purement résiduelle), dans le cas (c) (car $A(a)_\sigma = A(a, \ldots, \sigma^n(a))$ qui est purement résiduelle), et dans le cas (d) (car $A(a)_\sigma \subset A(a, \ldots, \sigma^n(a))^{alg}$, ce qui entraîne que $v(A(a)_\sigma^\times)$ est contenu dans l'enveloppe divisible de $v(A(a, \ldots, \sigma^n(a))^\times)$ $(= v(A^\times))$ intersectée avec $\Gamma_C$.

Si $\bar{a}$ est algébrique sur $k'_A$, nous devons raisonner différemment. Rappelons que nous avions étendu $f$ d'abord à la clôture Hensélienne de $A$. Nous savons que $a$ est algébrique sur $A$, de polynôme minimal $g(T)$, et nous savons que $[A(a) : A] = [k'_A(\bar{a}) : k'_A]$. Comme $k'_A$ est parfait, $g(T)$ est séparable. Nous allons montrer que $A(a)_\sigma/A$ est purement résiduelle. Supposons le résultat montré pour $A' := A(\sigma^i(a), \ldots, \sigma^j(a))$, où $i \leq 0 \leq j$, et regardons par exemple $\bar{\sigma}^{j+1}(\bar{a})$, et prenons son polynome minimal $\bar{g}_1(T)$ sur le corps résiduel de $A'$ ; alors $\bar{g}^{\bar{\sigma}^{j+1}}(T) = \bar{g}_1(X)\bar{g}_2(T)$, avec $\bar{g}_2(T)$ et $\bar{g}_1(T)$ relativement premiers (car $\bar{\sigma}^{j+1}(\bar{a})$ est une racine simple de $\bar{g}^{\bar{\sigma}^{j+1}}(T)$). Comme $A$ est Hensélien, il existe des polynômes $g_1(T)$ et $g_2(T)$ sur $A'$, qui relèvent $\bar{g}_1(T)$ et $\bar{g}_2(T)$ respectivement, et tels que $g^{\sigma^{j+1}}(T) = g_1(T)g_2(T)$ (par 3.11(3)). Notre choix de $g$ entraîne que $g_1$ et $\bar{g}_1$ ont même degré, et donc que l'extension $A'(\sigma^{j+1}(a)/A'$ est purement résiduelle. La preuve que $A'(\sigma^{i-1}(a))/A'$ est purement résiduelle est similaire.

**8.15. Corollaire**. Soit $K$ un modèle de $T_0$, de caractéristique résiduelle nulle. Si $K_0 \subset K$ est un sous-corps aux différences maximal tel que $v(K_0^\times) = \{0\}$, alors l'application res définit une bijection entre $K_0$ et le corps résiduel de $K$.

*Démonstration.* Si $\mathrm{res}\,(K_0) \neq k_K$, prenons $\bar{a} \in k_K \setminus \mathrm{res}\,(K_0)$. Si $\bar{a}$ est $\bar{\sigma}$-transcendant sur $\mathrm{res}\,(K_0)$, alors tout relèvement $a$ de $\bar{a}$ sera $\sigma$-transcendant sur $K_0$, et nous aurons que $K_0(a)_\sigma/K_0$ est purement résiduelle, ce qui contredit la maximalité de $K_0$. Si $\bar{a}$ est $\bar{\sigma}$-algébrique sur $K_0$, comme $v(K_0^\times) = (0)$ est pur dans $\Gamma_K$, on utilise l'étape 4a(d) (cf. 8.14) pour trouver $a$ tel que $K_0(a)_\sigma/K_0$ soit non ramifiée.

**8.16. Etape 5 - a** Nous pouvous supposer que $v(A^\times)$ est pur dans $\Gamma_C$.

Tout d'abord, par l'étape 3 et par l'étape 4a(b), nous pouvons supposer que $k'_A$, le corps résiduel de $A$, est relativement algébriquement clos dans $C$, et que $A$ est Hensélien. Soient $\ell$ un nombre premier et $\alpha \in \Gamma_C$ tels que $\alpha \notin v(A^\times)$, $\ell\alpha \in v(A^\times)$. Comme $A^{alg} \cap C$ a même corps résiduel que $A$, nous savons par le Lemme 3.28 qu'il existe $a \in C$ tel que $v(a) = \alpha$ et $a^\ell \in A$. De plus, nous pouvons choisir cet $a$ tel que $\overline{\mathrm{ac}}(a) = 1$, et si la caractéristique résiduelle est $p > 0$, tel que $\overline{\mathrm{ac}}_n(a) = 1$, pour $n$ arbitrairement grand (par exemple $\geq 3$).

L'extension $A(a)/A$ est alors totalement ramifiée. Soit $a_1 = \sigma(a)a^{-1}$. Alors $\mathrm{res}\,(a_1) = 1$. Si la caractéristique de $k_K$ est nulle, l'élément $a_1$ est l'unique racine $\ell$-ième de $\sigma(a^\ell)a^{-\ell}$ d'image résiduelle égale à 1, et appartient à $A$ puisque $A$ est Hensélien. Nous avons donc $A(a) = A(a)_\sigma$. Si $b \in L$ est tel que $b^\ell = f(a^\ell)$ et $\overline{\mathrm{ac}}(b) = 1$, alors de la même façon, $B(b)_\sigma = B(b)$, et $f$ s'étend en un isomorphisme envoyant $a$ sur $b$.

Supposons maintenant que la caractéristique résiduelle soit $p > 0$. Si $\ell \neq p$, alors toutes les racine $\ell$-ièmes de l'unité ont des images résiduelles distinctes. Le même raisonnement nous donne que l'élément $a_1$ appartient à $A$, et est l'unique racine $\ell$-ième de $\sigma(a^\ell)a^{-\ell}$ d'image résiduelle égale à 1. Prenons $b \in L$ tel que $b^\ell = f(a^\ell)$ et $\overline{\mathrm{ac}}_1(b) = 1$. Alors pour $m > 1$, dans $\mathcal{O}_A/p^m\mathcal{O}_A$, l'élément $\overline{\mathrm{ac}}_m(a)$ est uniquement déterminé par les équations $T^\ell = \overline{\mathrm{ac}}_m(a^\ell)$ et $\pi_{1,m}(T) = 1$ ; donc, dans $\mathcal{O}_B/p^m\mathcal{O}_B$, l'élément $f(\overline{\mathrm{ac}}_m(a))$ est uniquement déterminé par les equations $T^\ell = f(\overline{\mathrm{ac}}_m(a^\ell))$ et $\pi_{1,m}(T) = 1$, ce qui entraîne que $f(\overline{\mathrm{ac}}_m(a)) = \overline{\mathrm{ac}}_m(b)$. Nous avons donc montré que l'isomorphisme de corps valués $A(a) \to B(b)$ qui envoie $a$ sur $b$ respect aussi les $\overline{\mathrm{ac}}_m$.

Si $\ell = p$, alors $C$ ne contient aucune racine primitive $p$-ième de l'unité (puisque $v(p)$ est le plus petit élément positif de $\Gamma_C$), ce qui entraîne que $a$ est l'unique solution de $T^p = a^p$ dans $C$. Nous avons supposé que $\overline{\mathrm{ac}}_3(a) = 1$, et donc si $a_1 = \sigma(a)a^{-1}$, nous aurons $\mathrm{res}\,_3(a_1) = 1$. Puisque $A$ est Hensélien et $a_1^p \in A$, nous avons $a_1 \in A$. Pour $m > 3$, dans $\mathcal{O}_A/p^m\mathcal{O}_A$, l'élément $\overline{\mathrm{ac}}_m(a)$ est uniquement déterminé par les équations $T^p = \overline{\mathrm{ac}}_m(a^p)$ et $\pi_{3,m}(T) = 1$ ; alors, dans $\mathcal{O}_B/p^m\mathcal{O}_B$, l'élément $f(\overline{\mathrm{ac}}_m(a))$ est uniquement déterminé par les équations $T^p = f(\overline{\mathrm{ac}}_m(a^p))$ et $\pi_{3,m}(T) = 1$, ce qui entraîne que $f(\overline{\mathrm{ac}}_m(a)) = \overline{\mathrm{ac}}_m(b)$, et termine la preuve.

Nous étendons $f$ de proche en proche, jusquà ce que $v(A^\times)$ soit pur dans $\Gamma_C$.

**8.17. Fin de l'étape 4**. Nous pouvons donc supposer que le corps résiduel de $A$ est $k_C$ : en utilisant l'étape 8.16, nous pouvons supposer que $v(A^\times)$ est pur dans $\Gamma_C$, ce qui nous permet d'appliquer les résultats de 8.14 et de trouver $A'$ ayant même groupe de valeurs que $A$, et ayant pour corps résiduel $k_C$.

**8.18. Fin de l'étape 5**. Nous pouvons supposer que $v(A^\times) = \Gamma_C$.

Nous sommes maintenant dans la situation suivante : le corps résiduel de $A$ est $k_C$, et nous voulons agrandir le groupe de valeurs de $A$. Soit $\alpha \in \Gamma_C$, $\alpha \notin v(A^\times)$. S'il existe $\ell \neq 0$ tel que $\ell\alpha \in v(A^\times)$, nous utilisons l'étape 5-a (8.16) pour étendre $f$. Supposons maintenant qu'il n'existe pas de tel $\ell$, et que $v(A^\times)$ soit pur dans $\Gamma_C$. Prenons $a \in C$ tel que $v(a) = \alpha$, $\sigma(a) = a$, et $\overline{\mathrm{ac}}(a) = 1$. Alors l'extension $A(a)_\sigma/A$ est totalement ramifiée. Soit $b \in L$ tel que $v(b) = f(\alpha)$, $\sigma(b) = b$, $\overline{\mathrm{ac}}(b) = 1$. Alors, posant $f(a) = b$ nous donne un isomorphisme $A(a) \to B(b)$ de corps valués qui respecte $\overline{\mathrm{ac}}$. Si la caractéristique résiduelle est positive, il faut respecter aussi les $\overline{\mathrm{ac}}_m$, et pour cela, il suffit de multiplier $b$ par un élément $c$ de valuation 0, satisfaisant $\mathrm{res}\,_m(c)\overline{\mathrm{ac}}_m(b) = f(\overline{\mathrm{ac}}_m(a))$ pour tout $m$.

## 8.5 Prolongement à une extension immédiate, quelques considérations

Nous sommes maintenant dans la situation où $C$ est une extension immédiate de $A$. En utilisant l'étape 3, nous pouvons supposer que $A^{alg} \cap C = A$ (puisque $A^{alg} \cap C = A^h$). Soit $a \in C \setminus A$. Nous pouvons alors trouver une suite pseudo-convergente $(a_\alpha)_{\alpha<\kappa}$ d'éléments de $A$, qui pseudo-converge vers $a$, et n'a pas de pseudo-limite dans $A$. Nous savons que cette suite est de type transcendant sur $A$. Cependant, très probablement, il existe $n$ tel que la suite $(\sigma^n(a_\alpha))$ (dont une pseudo-limite est $\sigma^n(a)$)) ne soit plus de type transcendant sur $A(a, \sigma(a), \ldots, \sigma^n(a))$.

La stratégie est la suivante : trouver $n$ minimum tel qu'il existe une suite pseudo-convergente $(a_\alpha)_{\alpha<\kappa}$, sans limite dans $A$, telle que $(a_\alpha) \Rightarrow a$, et telle qu'il existe $g(X) \in A[X]_\sigma$ d'ordre $n$ et tel que $g(a_\alpha) \Rightarrow 0$. On prend ensuite $g$ de degré minimum en $X_n$. Nous voulons de plus que si $h(X) = H(X_0, \ldots, X_n)$ est "moins compliqué" que $g(X)$, alors $(h(a_\alpha)) \Rightarrow h(a)$, et pour $\alpha \gg 0$, nous ayions $v(h(a_\alpha)) = v(h(a))$, et en faisant un changement de variable, nous nous trouvons en position d'appliquer la condition de $\sigma$-Hensel à $g(X)$.

Nous prendrons alors une pseudo-limite $a'$ de $(a_\alpha)$ qui satisfait $g(X) = 0$, puis de l'autre côté une pseudo-limite $b$ de $(f(a_\alpha))$ satisfaisant $g^f(X) = 0$. Nous voulons montrer que en posant $f(a) = b$, nous définissons bien un isomorphisme de corps valués.

Que veut dire "moins compliqué" : tout simplement d'ordre inférieur à $n$, ou bien d'ordre $n$ et de degré en $X_n$ inférieur à celui de $g(X)$. Nos conditions entraînent alors que $f$ définit un isomorphisme de corps valués entre $A(a, \sigma(a), \ldots, \sigma^n(a))$ et $B(b, \sigma(b), \ldots, \sigma^n(b))$.

Nous allons commencer par un cas facile

**8.19. Etape 6 - a**. Nous pouvons supposer que $A$ a suffisamment de constantes (axiome 3 dans 8.5).

Par l'étape 3, nous allons supposer que $A$ est Hensélien. Soit $a \in A$, et considérons $a_1 = a\sigma(a)^{-1}$. Si $c \in C$ est de valuation 0 et satisfaisant $\sigma(X) = a_1 X$, alors nous aurons $v(ca) = v(a)$ et $\sigma(ca) = ca$. Si un tel $c$ existe dans $A$, nous n'avons rien à faire. Sinon, nous savons qu'un tel $c$ existe dans $C$, et que l'extension $A(c)_\sigma = A(c)$ est une extension immédiate de $A$. Si $(c_\alpha)_{\alpha<\kappa}$ est une suite pseudo-convergente d'éléments de $A$, sans pseudo-limite dans $A$ et telle que $(c_\alpha) \Rightarrow c$, alors la suite $(c_\alpha)$ est de type transcendant (car $A$ est Hensélien et n'a pas d'extension immédiate algébrique propre), et determine entièrement le corps valué $A(c)$ (à isomorphisme près). Nous choisissons donc $d \in L$ tel que

$$v(d - f(c_\alpha)) = f(v(c - c_\alpha)) \ \forall \alpha < \kappa \qquad \text{et} \qquad \sigma(d) = f(a_1)d.$$

Alors, posant $f(c) = d$, nous aurons un isomorphisme étendant $f$ et ayant $c$ dans son domaine. Pourquoi pouvons nous trouver un tel $d$ ? Comme $v(c) = 0$, nous avons (pour $\alpha \gg 0$) $v(c_\alpha - c) > 0$, et donc $v(\sigma(c_\alpha) - a_1 c_\alpha) > 0$. Par $\sigma$-Hensel, passant à une sous-suite de $(a_\alpha)$, nous pouvons trouver $d \in L$, tel que $v(d - f(c_\alpha)) \geq f(v(c - c_\alpha))$ et $\sigma(d) = f(a_1)d$. Par $\kappa$-saturation de $L$, il existe donc $d \in L$ tel que $\sigma(d) = f(a_1)d$ et $v(d - f(c_\alpha)) \geq f(v(c - c_\alpha))$ pour tout $\alpha$. Alors on a $v(d - f(c_\alpha)) \geq f(v(c - c_\alpha))$ pour tout $\alpha$, et $(f(c_\alpha)) \Rightarrow d$. C'est à dire, posant $f(c) = d$, $f$ est un isomorphisme de corps valués qui commute avec $\sigma$. Cela montre le résultat.

## 8.6 Plus sur les suites pseudo-convergentes

Je renvoie aux paragraphes 3.33 et 3.34 pour les définitions. Je vais donner un peu plus de détails sur les preuves.

**Notation/Convention** J'abbrévierai désormais pseudo-convergent par *p.c.*. Etant donnée une suite p.c. $(a_\alpha)$, j'ecrirai $(a_\alpha) \Rightarrow^{\text{ev}} a$ pour dire que pour $\alpha > \alpha_0$, nous avons $v(a - a_\alpha) = v(a_{\alpha+1} - a_\alpha)$, pour un certain $\alpha_0$.

**8.20. Lemme**. Soient $\Gamma$ un groupe ordonné abélien, $\delta_1, \ldots, \delta_k \in \Gamma$, $m_1, \ldots, m_k$ des entiers positifs, et $(\gamma_\alpha)_{\alpha<\kappa}$ une suite strictement croissante d'éléments de $\Gamma$. Alors il existe $\alpha_0$, tel que pour tout $\alpha, > \alpha_0$ et $i \neq j$, on ait

$$m_i\gamma_\alpha + \delta_i < m_j\gamma_\alpha + \delta_j \iff m_i\gamma_\beta + \delta_i < m_j\gamma_\beta + \delta_j.$$

*Démonstration.* On peut supposer $k = 2$, et sans perte de généralité, que $m_1 < m_2$. Nous regardons

$$\frac{\delta_1 - \delta_2}{m_2 - m_1} \ ? \ \gamma_\alpha,$$

où ? est un de $>$, $<$, et nous voulons montrer que pour $\alpha \gg 0$, ? ne dépend plus de $\alpha$. S'il existe $\alpha_0$ tel que $\frac{\delta_1-\delta_2}{m_2-m_1} \leq \gamma_{\alpha_0}$, alors, comme $\gamma_\alpha$ est strictement croissante, pour tout $\alpha > \alpha_0$, nous aurons $\frac{\delta_1-\delta_2}{m_2-m_1} < \gamma_\alpha$. Si par contre il n'y a pas de tel $\alpha_0$, cela veut dire que pour tout $\alpha$, nous avons $\frac{\delta_1-\delta_2}{m_2-m_1} > \gamma_\alpha$.

**8.21. Remarque**. Soit $(a_\alpha)$ une suite p.c, et supposons que $(a_\alpha) \not\Rightarrow^{\text{ev}} 0$. Alors pour $\alpha \gg 0$, $v(a_\alpha)$ devient constante, et $v(a_\alpha) < v(a_{\alpha+1} - a_\alpha)$.

*Démonstration.* S'il existe un $\alpha$ satisfaisant $v(a_\alpha) < v(a_{\alpha+1} - a_\alpha)$, alors, comme $v(a_{\alpha+1} - a_\alpha) = v(a_\beta - a_\alpha)$ pour tout $\beta > \alpha$, on obtient que pour tout $\beta > \alpha$, on a $v(a_\beta) = v(a_\alpha)$. S'il n'existe pas de tel $\alpha$, alors nous avons, pour tout $\alpha$, $v(a_\alpha) \geq v(a_{\alpha+1} - a_\alpha)$. En particulier, $v(a_{\alpha+1}) \geq v(a_{\alpha+2} - a_{\alpha+1}) > v(a_{\alpha+1} - a_\alpha)$. Cela entraîne que $v(a_\alpha) = v(a_{\alpha+1} - a_\alpha)$ (car $a_\alpha = -(a_{\alpha+1} - a_\alpha) + a_{\alpha+1}$). La suite $v(a_\alpha)$ est donc strictement croissante, ce qui contredit $(a_\alpha) \not\Rightarrow^{\text{ev}} 0$.

**8.22. Lemme**. Soient $K$ un corps valué, et $(a_\alpha)_{\alpha<\kappa}$ une suite p.c. sans pseudo-limite dans $K$.

(1) Si $f(T) \in K[T]$ alors pour $\alpha > \alpha_0$, la suite $(f(a_\alpha))$ devient p.c.

(2) Deux cas sont possibles pour la suite $v(f(a_\alpha))$ : ou bien pour $\alpha \gg 0$, $v(f(a_\alpha))$ se stabilise ; ou bien $(f(a_\alpha)) \Rightarrow^{\text{ev}} 0$.

*Démonstration.* On montre (1) et (2) en même temps par induction sur le degré de $f(T)$. Si ce degré est 0, il n'y a rien à montrer. Supposons le résultat montré pour les polynômes de degré inférieur à celui de $f(T)$, et supposons d'abord que si $\deg(g) < \deg(f)$, alors $v(g(a_\alpha))$ se stabilise.

En utilisant le développement de Taylor de $f(T)$, nous écrivons

$$f(a_{\alpha+1}) - f(a_\alpha) = \sum_{\ell \geq 1} D_\ell(f)(a_\alpha)(a_{\alpha+1} - a_\alpha)^\ell.$$

Par hypothèse d'induction, comme les polynômes $D_\ell(f)(T)$ sont de degré inférieur à celui de $f(T)$ pour $\ell \geq 1$, nous savons que pour $\alpha \gg 0$, les valeurs de $v(D_\ell(f)(a_\alpha))$ se stabilisent, en $\delta_\ell$ disons. Le lemme 8.20 nous dit que nous pouvons trouver un indice $i$ tel que, pour $\alpha \gg 0$, si $j \neq i$, alors

$$v(D_i(f)(a_\alpha)(a_{\alpha+1} - a_\alpha)^i) < v(D_j(f)(a_\alpha)(a_{\alpha+1} - a_\alpha)^j).$$

Pour $\alpha \gg 0$, nous avons donc, pour tout $\alpha \gg 0$,

$$v(f(a_{\alpha+1}) - f(a_\alpha)) = \delta_i + iv(a_{\alpha+1} - a_\alpha).$$

Cela montre que la suite $(f(a_\alpha))$ est finalement p.c., et montre (1).

Passant à une sous-suite, nous supposons que $(f(a_\alpha))$ est p.c. ; s'il existe $\alpha_0$ tel que $v(f(a_{\alpha_0+1}) - f(a_{\alpha_0})) > v(f(a_{\alpha_0}))$, alors on obtient $v(f(a_{\alpha_0})) = v(f(a_{\alpha_0+1})) = v(f(a_\alpha))$ pour tout $\alpha > \alpha_0$, ce qui montre (2). S'il n'existe pas de tel $\alpha_0$, alors nous avons pour tout $\alpha$, $v(f(a_\alpha)) \geq v(f(a_{\alpha+1}) - f(a_\alpha))$, ce qui entraîne (comme $(f(a_\alpha))$ est p.c.) que $v(f(a_{\alpha+1}) > v(f(a_\alpha)) = v(f(a_{\alpha+1}) - f(a_\alpha)) = v(D_i(f)(a_\alpha)) + iv(a_{\alpha+1} - a_\alpha)$, et montre (2).

Finalement, supposons qu'il existe un polynôme $g(T)$ de degré inférieur à celui de $f$ et tel que $g(a_\alpha) \Rightarrow^{\text{ev}} 0$. Prenons un tel $g$ de degré minimal. Ecrivons $f(T) = h(T)g(T)+r(T)$, où $\deg(r) < \deg(g)$. On montre alors facilement (2) : s'il existe $\alpha_0$ tel que $v(hg(a_{\alpha_0})) \geq v(r(a_{\alpha_0}))$, alors $v(f(a_\alpha)) = v(r(a_\alpha))$ pour $\alpha > \alpha_0$ ; s'il n'existe pas de tel $\alpha$, alors $v(f(a_\alpha)) = v(h(a_\alpha))+v(g(a_\alpha))$.

La démonstration de (1) est un peu détournée, et utilise en fait le théorème 8.24(2) (une inspection de la preuve montre qu'elle n'utilise que le cas déjà montré). Soit donc $a$ dans une extension de $K$, satisfaisant $g(T) = 0$ et $(a_\alpha) \Rightarrow a$. On applique Taylor à $f(a_\alpha) - f(a)$, et on obtient $i$ tel que, pour $\alpha \gg 0$, on a $v(f(a_\alpha) - f(a)) = v(D_i(f)(a)) + iv(a_\alpha - a)$ ; on a donc $(f(a) - f(a_\alpha)) \Rightarrow^{\text{ev}} 0$, ce qui montre que pour $\alpha \gg 0$, la suite $f(a_\alpha)$ est p.c.

**8.23. Remarque** En fait, la preuve de (2) donne : il existe $\delta$ et un entier $m$ tel que $v(f(a_\alpha)) = \delta + mv(a_{\alpha+1} - a_\alpha)$ pour tout $\alpha \gg 0$.

**8.24. Définitions** S'il existe $f(T) \in K[T]$ non nul tel que $(f(a_\alpha)) \Rightarrow^{\text{ev}} 0$, on dit que $(a_\alpha)$ est de *type algébrique*. S'il n'existe pas de tel $f(T)$, on dit que $(a_\alpha)$ est de *type transcendant*

**Théorème**. Soient $K$ un corps valué, $(a_\alpha)$ une suite p.c. d'éléments de $K$ sans pseudo-limite dans $K$.

(1) Si $(a_\alpha)$ est de type transcendant sur $K$, alors il existe $a$ (dans une extension de $K$) tel que $(a_\alpha) \Rightarrow a$, l'extension $K(a)/K$ est immédiate et est entièrement déterminée par $(a_\alpha) \Rightarrow a$. C'est à dire, si $(a_\alpha) \Rightarrow b$, alors les corps valués $K(a)$ et $K(b)$ sont $K$-isomorphes, par un isomorphisme envoyant $a$ sur $b$.

(2) Suposons maintenant que $(a_\alpha)$ soit de type algébrique sur $K$, et que $f(T) \in K[T]$ soit de degré minimal tel que $(f(a_\alpha)) \Rightarrow^{\text{ev}} 0$. Alors il existe $a$ tel que $(a_\alpha) \Rightarrow a$, et $f(a) = 0$. De plus, ces conditions déterminent uniquement l'extension $K(a)/K$, et cette extension est immédiate.

*Démonstration.* (1) Soit $g(T) \in K[T]$. Par 8.22, nous pouvons supposer que $v(D_\ell(g)(a_\alpha)) = \delta_\ell$ ne dépend pas de $\alpha$, pour $\ell = 0, \ldots, \deg(g)$. Alors $g(a) - g(a_\alpha) = \sum_{\ell \geq 1} D_\ell(g)(a_\alpha)(a - a_\alpha)^\ell$. Par le lemme 8.20, il existe un indice $i$ tel que $v(g(a) - g(a_\alpha)) = iv(a - a_\alpha) + \delta_i$ pour tout $\alpha \gg 0$ ; par le résultat précédent 8.22, nous avons $v(g(a_{\alpha+1}) - g(a_\alpha)) = iv(a_{\alpha+1} - a_\alpha) + \delta_i$, et comme $v(g_\alpha)$ ne dépend pas de $\alpha$, nous sommes obligés d'avoir $v(g(a)) = v(g(a_\alpha))$. Cela montre l'unicité de la structure de corps valué sur $K(a)$. Comme $v(K(a)^\times) = v(K^\times)$, $K(a)/K$ n'est pas ramifiée. S'il existait $r \in K(a)$ tel que $v(r) = 0$, et pour tout $b \in \mathcal{O}_K$, $v(r - b) = 0$, alors, écrivant $r = f(a)/g(a)$, où $f(T), g(T) \in K[T]$, nous obtenons que pour tout $b \in K$, $v(f(a) - bg(a)) = v(f(a)) = v(g(a))$. Cela contredit le fait que $(f(a_\alpha) - rg(a_\alpha)) \Rightarrow^{\text{ev}} f(a) - rg(a)$. Donc $K(a)/K$ est immédiate.

(2) On prend une racine $a$ de $f(T) = 0$, et nous définissons sur $a$ une valuation étendant celle de $K$. Pour cela, il suffit de considérer les polynômes $g(T)$ de degré inférieur à celui de $f(T)$, et de définir $v(g(a))$. On prend pour $v(g(a))$ la valeur sur laquelle $v(g(a_\alpha))$ se stabilise (ici on utilise la minimalité du degré de $f(T)$). On vérifie que c'est bien une valuation. On raisonne comme dans (1) pour montrer que $K(a)/K$ est immédiate.

Soit maintenant $b$ avec $f(b) = 0$ et $(a_\alpha) \Rightarrow b$. Pour tout $g(T) \in K[T]$ de degré inférieur à celui de $f(T)$, raisonnant comme dans (1), $v(g(b))$ doit être la valeur sur laquelle $v(g(a_\alpha))$ se stabilise, et donc être égal à $v(g(a))$. L'isomorphisme $K(a) \to K(b)$ qui envoie $a$ sur $b$ est donc un isomorphisme de corps valués.

## 8.7 La preuve du résultat de B-M-S dans le cas immédiat

Je ne donnerai pas la preuve complète, énoncerai seulement les résultats principaux qui amènent au résultat final. Pour simplifier l'énoncé des résultats, dans les paragraphes de cette section, $K$ sera toujours un corps qui satisfait tous les axiomes de $T_0$, à l'exception de l'axiome (7) ($\sigma$-Hensel). En particulier, des propriétés de clôture du corps résiduel, et le fait que $v(K^\times) = v(\text{Fix}(\sigma)(K)^\times)$. Ces hypothèses peuvent souvent être affaiblies, pour plus de détails, voir l'article de Bélair, Macintyre, Scanlon.

**8.25. Définition**. Soient $(a_\alpha)$, $(b_\beta)$ deux suites p.c. dans $K$. Elles sont *équivalentes*, noté $(a_\alpha) \sim (b_\beta)$, si dans toute extension de $K$, elles ont les même pseudo-limites. Rappelons que la largeur d'une suite p.c. $(a_\alpha)$ est la coupure déterminée par la suite $\gamma_\alpha := v(a_{\alpha+1} - a_\alpha)$, c'est-à-dire, $\{\gamma \in \Gamma_K \mid \gamma > \gamma_\alpha \text{ pour tout } \alpha\}$. Voici quelques formulations équivalentes de de $(a_\alpha) \sim (b_\beta)$ :

(1) $(a_\alpha)$ et $(b_\beta)$ ont la même largeur, et ont une pseudo-limite commune.

(2) Pour tout $\alpha$ il existe $\beta_0$ tel que si $\beta > \beta_0$ alors $v(b_\beta - a_{\alpha+1}) > v(a_{\alpha+1} - a_\alpha)$, et pour tout $\beta$, il existe $\alpha_0$ tel que si $\alpha > \alpha_0$ alors $v(a_\alpha - b_{\beta+1}) > v(b_{\beta+1} - b_\beta)$.

(3) Supposons que $(a_\alpha)$ et $(b_\beta)$ n'ont pas de pseudo-limite dans $K$. Alors elles sont une pseudo-limite commune (dans une extension de $K$).

**8.26. Définitions**. Soit $(a_\alpha)$ une suite p.c. dans $K$, sans pseudo-limite dans $K$. On dit que $(a_\alpha)$ est de type $\sigma$-*algébrique* s'il existe une suite $(b_\beta)$ équivalente à $(a_\alpha)$, et $g(X) \in K[X]_\sigma$ tels que $(g(b_\beta)) \Rightarrow 0$, et pour tout $h(X) \in \mathcal{H}(g)$, $(h(a_\alpha))$ est p.c.

Ici, $\mathcal{H}(g)$ est un ensemble fini de polynômes aux différences, qui, si $g(X) = G(X_0, \ldots, X_n)$, contient les polynômes $D_\ell(G)(X)$ pour $|\ell| \geq 1$ (notés $D_\ell(g)(X)$), ainsi que certains autres polynômes aux différences quand la caractéristique résiduelle est positive, et qui permettent de calculer des coefficients angulaires d'ordre supérieur.

**8.27. Théorème 1** (La caractéristique résiduelle est $p > 0$). Soient $(a_\alpha)$ une suite p.c. dans $K$, $f_1(T), \ldots, f_m(T) \in K[T]$. Alors il existe $(b_\beta) \sim (a_\alpha)$ tel que les suites $(f_i(b_\beta))$ sont p.c. pour $i = 1, \ldots, m$. De plus, si $(a_\alpha) \Rightarrow a$, où $a$ est dans une extension, on peut les choisir telles que $(f_i(b_\beta)) \Rightarrow f_i(a)$ pour $i = 1, \ldots, m$.

**8.28. Théorème 2** Soient $(a_\alpha)$ une suite p.c. de $K$, sans pseudo-limite dans $K$, et $(a_\alpha) \Rightarrow a$. On suppose que $(g(a_\alpha)) \Rightarrow^{\text{ev}} 0$, que si $h(X) \in \mathcal{H}(g)$ n'est pas constante, alors pour $\alpha \gg 0$, $(h(a_\alpha))$ est p.c., mais $(h(a_\alpha)) \not\Rightarrow^{\text{ev}} 0$. Alors il existe $(a'_\alpha) \sim (\alpha)$ telle que $g(a'_\alpha) \Rightarrow^{\text{ev}} 0$, et si $h(X) \in \mathcal{H}(g)$ n'est pas constante, $(h(a'_\alpha)) \Rightarrow h(a)$.

**8.29.** La complexité d'un polynôme aux différences $g(X) \in K[X]_\sigma$ est la paire $(n, d)$, où $n$ est l'ordre de $g(X)$, et $d$ le degré de $g(X)$ considéré comme un polynôme en $X_n$. Nous prenons l'ordre lexicographique sur ces paires: $(n, d) < (n', d')$ si $n < n'$, ou bien $n = n'$ et $d < d'$.

**Théorème 3**. Soient $(a_\alpha)$ une suite p.c. dans $K$, sans pseudo-limite dans $K$, $(a_\alpha) \Rightarrow a$, avec $K(a)_\sigma/K$ imédiate. On suppose que $(a_\alpha)$ est de type $\sigma$-algébrique, et que $g(X)$ est un polynôme aux différences de complexité minimale qui témoigne de cette $\sigma$-algébricité. Alors il existe $(a'_\alpha) \sim (a_\alpha)$, telle que $g(a'_\alpha) \Rightarrow 0$, si $h(X) \in \mathcal{H}(g)$ n'est pas constante, alors $(h(a'_\alpha)) \Rightarrow h(a)$, $(h(a'_\alpha)) \not\Rightarrow 0$, et telle que pour $\alpha \geq 0$, on puisse appliquer l'axiome (7') (la version forte de $\sigma$-Hensel) à $g(X)$ en $a'_\alpha$. De plus, ou bien $g(a) = 0$, ou bien on peut aussi appliquer $\sigma$-Hensel fort à $g(X)$ en $a$.

**8.30. Théorème 4** Soit $(a_\alpha)$ une suite p.c. dans $K$, sans pseudo-limite dans $K$, et qui est de type $\sigma$-transcendant. Alors il existe une extension $K(a)_\sigma/K$, avec $(a_\alpha) \Rightarrow a$. De plus, ces conditions déterminent uniquement l'extension $K(a)_\sigma/K$, et $K(a)_\sigma/K$ est immédiate, $a$ est $\sigma$-transcendant sur $K$.

**8.31. Théorème 5**. Soient $(a_\alpha)$ une suite p.c. dans $K$, sans pseudo-limite dans $K$, de type $\sigma$-algébrique, et $g(X) \in K[X]_\sigma$ de complexité minimale qui témoigne de cette $\sigma$-algébricité. Alors il existe $a$ tel que $g(a) = 0$ et $(a_\alpha) \Rightarrow a$. De plus, ces conditions déterminent uniquement l'extension $K(a)_\sigma/K$, et $K(a)_\sigma/K$ est immédiate.

**8.32. Théorème 6**.

(a) $K$ a une extension immédiate propre si et seulement si $K$ a une extension immédiate propre qui est un corps aux différences.

(b) $K$ a une extension immédiate propre qui est $\sigma$-algébrique, si et seulement si $K$ contient une suite p.c. $(a_\alpha)$ sans pseudo-limite dans $K$, et qui est de type $\sigma$-algébrique.

(c) On suppose $K(a)_\sigma/K$ immédiate, et $K_2$ un modèle de $T_0$ contenant $K$ et tel que toute suite p.c. de $K_2$ de longueur $\leq |\Gamma_K|$ a une pseudo-limite dans $K_2$. Alors $K(a)_\sigma$ se $K$-plonge dans $K_2$.

(d) On suppose $K(a)_\sigma/K$ immédiate et $\sigma$-algébrique, et $K_2$ un modèle de $T_0$ contenant $K$ et tel que toute suite p.c. de $K_2$ de longueur $\leq |\Gamma_K|$ et qui est de type $\sigma$-algébrique a une pseudo-limite dans $K_2$. Alors $K(a)_\sigma$ se $K$-plonge dans $K_2$.

**8.33. Théorème 7**.

(1) $K$ a une extension immédiate maximale, et qui est unique à $K$-isomorphisme près.

(2) $K$ a une extension immédiate $\sigma$-algébrique maximale, et qui est unique à $K$-isomorphisme près.

**8.34. Corollaire : la fin de la preuve du théorème 8.8**. Soient $C$, $A$, $K$, $L$ et $f$ comme dans à la fin de la section 8.4. Soit $\hat{C}$ l'extension immédiate maximale de $C$ à l'intérieur de $K$. Alors $\hat{C}$ se $K$-plonge dans $L$.

*Démonstration.* Comme $L$ est $\kappa$-saturé, avec $\kappa \geq \aleph_1$, et $A$ est dénombrable, $C/A$ est immédiate, on sait que $K$ contient une copie de l'extension immédiate maximale de $A$ (qui est aussi celle de $C$) ; de même, $L$ contient une copie de l'extension immédiate maximale $\hat{B}$ de $B$. Alors il existe un isomorphisme de corps valués aux différences $f : \hat{C} \to \hat{B}$, qui prolonge $f|_A$. Comme $\hat{C}/A$ est immédiate, ce prolongement de $f$ est compatible avec $f|_{\Gamma_C \cup k_C}$.

## 8.8 Quelques remarques finales et conséquences de la preuve

Ce résultat a de multiples conséquences, la plus immédiate étant celle d'un résultat *à la Ax-Kochen-Ershov* :

**8.35. Théorème** Soient $K$ et $L$ des corps valués aux différences de caractéristique 0, satisfaisant les axiomes (2) – (4), (6) – (8) de 8.5, ainsi que, si la caractéristique résiduelle est $p > 0$, alors $v(p)$ est le plus petit élément positif du groupe de valeurs. On se place ou bien dans le langage $\mathcal{L}_{\text{div}} \cup \{\sigma\}$, ou bien dans le langage à trois sortes $\mathcal{L}'_{\text{c.val}} \cup \mathcal{L}'_{\text{gp}} \cup \mathcal{L}'_{\text{c.rés}}$ avec les applications $v$ et res , mais sans les applications coefficients angulaires. Alors

(1) $K \equiv L \iff k_K \equiv k_L \qquad \text{et} \qquad \Gamma_K \equiv \Gamma_L$.

(2) Supposons $K \subset L$. Alors $K \prec L \iff k_K \prec k_L \qquad \text{et} \qquad \Gamma_K \prec \Gamma_L$.

*Démonstration.* (1) Passant à des extensions élémentaires, nous pouvons supposer que $K$ et $L$ sont $\aleph_1$-saturés. Alors leurs sous-corps $\text{Fix}(\sigma)(K)$ et $\text{Fix}(\sigma)(L)$ seront aussi $\aleph_1$-saturés[4]. Par le Lemme 4.17, il existe donc une section $s : \Gamma_K \to \text{Fix}(\sigma)(K)$ de la valuation $v$. Si la

[4]Une notation que j'aurais dû introduire avant : si $K$ est un corps aux différences, alors $\text{Fix}(\sigma)(K)$ dénote $\{a \in K \mid \sigma(a) = a\}$.

caractéristique de $k_K$ est positive, on peut aussi supposer que $s(1) = p$. Cela nous permet de définir des applications $\overline{\text{ac}}$, $\overline{\text{ac}}_n$ sur $K$. On raisonne de la même façon pour $L$.

Par Théorème 8.8, il suffit maintenant de montrer que les sous-structures de $(K, \Gamma_K, k_K)$ et $(L, \Gamma_L, k_L)$ engendrées par les constantes sont isomorphes. Celle de $(K, \Gamma_K, k_K)$ est égale à $(\mathbb{Z}, \Gamma_K^0, k_K^0)$ où $\Gamma_K^0$ est la sous-$\mathcal{L}'_{\text{gp}}$-structure de $\Gamma_K$ engendrée par les constantes (et par $v(p)$ si la caractéristique de $k_K$ est $p > 0$), et $k_K^0$ est la sous-$\mathcal{L}'_{\text{c.rés}}$-structure de $k_K$ engendrée par les constantes. De la même façon, celle de $(L, \Gamma_L, k_L)$ est $(\mathbb{Z}, \Gamma_L^0, k_L^0)$. Notre hypothèse entraine que $\Gamma_K^0 \simeq \Gamma_K^0$ et $k_K^0 \simeq k_L^0$, ce qui nous donne le résultat, car ces isomorphismes sont bien sûr compatibles avec $id_{\mathbb{Z}}$.

(2) On prend maintenant une extension élémentaire $\aleph_1$-saturée de la paire $(K, L)$, définissons une section $s$ en la définissant d'abord de $\Gamma_K$ à valeurs dans $\text{Fix}(\sigma)(K)$, puis en l'étendant à tout $\Gamma_L$. Cela nous permet de définir des applications coefficients angulaires sur $L$ qui étendent celles de $K$. On conclut en appliquant 8.8.

**8.36. Remarque 1**. Soit $\mathbb{Q}_p^{nr}$ l'extension maximale algébrique non ramifiée de $\mathbb{Q}_p$. Alors son corps résiduel est $\mathbb{F}_p^{alg}$, et nous avons vu en 5.15 que si on munit le corps valué $\mathbb{Q}_p^{nr}$ d'un prédicat $S$ pour les représentants de Teichmüller, alors on a $(\mathbb{Q}_p^{nr}, S) \prec (W(\mathbb{F}_p^{alg}), S)$ (en fait nous avions montré seulement l'équivalence élémentaire, mais ceci est vrai aussi). Voici un exemple facile montrant que si $\sigma$ dénote l'automorphisme de $W(\mathbb{F}_p^{alg})$ ou de $\mathbb{Q}_p^{nr}$ qui relève le Frobénius $x \mapsto x^p$, alors $(\mathbb{Q}_p^{nr}, \sigma) \not\equiv (W(\mathbb{F}_p^{alg}), \sigma)$. En effet, considérons la formule $\exists x\ \sigma(x) = x + p$. Nous savons que $W(\mathbb{F}_p^{alg})$ est $\sigma$-Hensélien (par 8.10) ; de plus, 1 est une solution résiduelle de cette équation, et donc $W(\mathbb{F}_p^{alg})$ contient une solution $a$ de cette équation satisfaisant $v(a-1) > 0$. Comme la caractéristique est nulle, les éléments $\sigma^i(a) = a + pi$ sont tous distincts.

Soit $b \in \mathbb{Q}_p^{nr}$, et soient $b = b_1, \ldots, b_n$ ses conjugués au-dessus de $\text{Fix}(\sigma)(\mathbb{Q}_p^{nr})$. Alors $\sigma$ induit une permutation de $\{b_1, \ldots, b_n\}$, et ainsi nous avons $\sigma^m(b) = b$ pour un $0 < m \leq n$. Nous ne pouvons donc avoir $\sigma(b) = b + p$ puisque cela entrainerait $mp = 0$.

**8.37. Remarque 2**. Soit $\mathcal{K} = (K, \Gamma_K, k_K)$ un modèle de $T$, et $\mathcal{A} = (A, \Gamma_A, k_A)$ une sous-structure de $\mathcal{K}$. L'analogue du Lemme 7.13(a) est alors faux dans ce contexte particulier : par exemple, si la caractéristique résiduelle est $p > 0$, l'équation $\sigma(x) = x^p$ définit dans $K$ un ensemble $S$ de représentants du corps résiduel, qui est donc contenu dans la clôture définissable de $k_K$ (je ne suis pas sûre de ce qui se passe en acaractéristique résiduelle nulle). Cependant nous avons toujours:

(1) $acl(\mathcal{A}) \cap \Gamma_K = acl_{\text{Th}(\Gamma_K)}(\Gamma_A)$, et

(2) $acl(\mathcal{A}) \cap k_K = acl_{\text{Th}(k_K)}(k_A)$.

**8.38. Définition**. On travaille dans un modèle $M$ suffisamment saturé (d'une théorie $T$). Soit $S \subset M^n$ un ensemble définissable sans paramètres (ou bien une intersection infinie de tels ensembles, i.e., un ensemble $\infty$-définissable sur $\emptyset$). On dit que $S$ est *stablement plongé* si et seulement si, pour tout $m$ et tout sous-ensemble définissable (avec paramètres) $D$ de $M^{nm}$, il existe $D'$, définissable avec des paramètres de $S$, tels que $S \cap D = S \cap D'$.

Concrètement, si $S$ est définissable, cela veut dire la chose suivante : considérons $S$ dans le langage obtenu en ajoutant un prédicat $m$-aire $R_\varphi$ pour toute formule $\varphi$ sans paramètres à $nm$ variables, ce prédicat étant interprété par $S \models R_\varphi(b) \iff M \models \varphi(b)$ pour tout $b \in S^m$. Alors la structure de $S$ dans ce nouveau langage est exactement la structure induite sur $S$ par l'inclusion $S \subset M^n$.

**8.39. Commentaires**.

(1) La restriction que $S$ soit défini sur $\emptyset$ peut être contournée en ajoutant des symboles de constantes au langage.

(2) Si $T$ est stable, alors tout sous-ensemble $\infty$-définissable sur $\emptyset$ est stablement plongé.

(3) Si $S$ est stablement plongé et $a$ est un uplet d'éléments de $M$, alors $tp(a/S)$ sera *définissable*, c'est-à-dire, pour toute formule $\varphi(x, y)$ il existe une formule $d_\varphi(y)$ telle que pour tout $b \in S$, on a
$$M \models \varphi(a, b) \iff M \models d_\varphi(b).$$

(4) Il existe plusieurs formulations équivalentes de la définition, une que nous utiliserons est la suivante : $S$ est stablement plongé si pour tout uplet fini $a$ de $M$, il existe un "petit" sous-ensemble $S_0$ de $S$ tel que $tp(a/S_0) \vdash tp(a/S)$. (Petit veut dire de cardinalité inférieure à celle de l'ensemble des formules sur $\emptyset$ du langage). Un des corollaires de la preuve du Théorème 8.8 est alors que

**8.40. Théorème**. Soit $\mathcal{K} = (K, \Gamma_K, k_K)$ un modèle de $T$. Alors $k_K$ et $\Gamma_K$ sont stablement plongés.

*Démonstration.* Cela suit (de la démonstration) du Théorème 8.8. En effet, soit $(a, \alpha, \bar{a})$ un uplet de $\mathcal{K}$, et soient $A$ le corps aux différences engendré par $a$, $\Gamma_A$ son groupe de valeurs et $k_A$ son corps résiduel. Si $\beta, \gamma$ sont des uplets de $\Gamma_K$ qui satisfont les mêmes $\mathcal{L}'_{\mathrm{gp}}(\Gamma_A, \alpha)$-formules, alors l'application $f$ qui fixe $(A, \alpha, \bar{a})$ et envoie $\beta$ sur $\gamma$ est élémentaire. Cela montre que $tp(\beta/\Gamma_A, \alpha) \vdash tp(\beta/a, \alpha, \bar{a})$, et par symétrie, que $tp(a, \alpha, \bar{a}/\Gamma_A, \alpha) \vdash tp(a, \alpha, \bar{a}/\Gamma_K)$. La preuve est similaire pour $k_K$.

# 9 Trucs jetés

**Hypothèse supplémentaire dans le cas (ii),** $e > 1$. Nous ajoutons au langage du corps valué un symbole de constante $c_1$, qui sera interprété dans $K$ par un élément $\pi_K$ tel que $v(\pi_K) = 1$ et $\pi_K$ est algébrique sur $\mathbb{Q}$, et dans $L$ par un élément $\pi_L$ tel que $w(\pi_L) = 1$ et $\pi_L$ est algébrique sur $\mathbb{Q}$ (de tels éléments existent, cf Remarque 3.29). Il faudra bien sûr, pour avoir un espoir d'envoyer $\pi_K$ sur $\pi_L$, que leurs polynômes minimals sur $\mathbb{Q}$ soient les mêmes, mais ce n'est pas suffisant. Nous savons que le corps résiduel de $K$ (et de $L$) est $\mathbb{F}_q$ pour une puissance $q$ de $p$. Le groupe multiplicatif de $\mathbb{F}_q$ est cyclique, engendré par un élement d'ordre $q-1$, qui est donc une racine simple de l'équation $T^{q-1} - 1 = 0$. Par Hensélianité, le corps $K$ contient donc une racine primitive $(q-1)$-ème de l'unité, et de même pour $L$. Nous ajoutons donc au langage du corps valué une deuxi'eme constante $c_2$, qui sera interprétée dans $K$ et dans $L$ par une racine primitive $(q-1)$-ème de l'unité, notée $\zeta$.

Notons que maintenant la sous-structure de $K$ engendrée par $\emptyset$ est l'anneau $\mathbb{Z}[\pi_K, \zeta]$, qui a corps résiduel $\mathbb{F}_q$ et groupe de valeurs engendré par 1. Nous avons donc éliminé notre problème, au moins pour la prolongation de $f$.

Si nous voulons que notre théorie $T_e$ soit complète (dans ce nouveau langage), nous devons cependant rajouter des axiomes qui décrivent l'anneau $\mathbb{Z}[\pi_K, \zeta]$. Nous lui rajoutons donc un axiome disant que $c_2$ est une racine primitive $(q-1)$-ème de l'unité, et un autre disant que $P(c_1, c_2) = 0$, où $P(X, Y) \in \mathbb{Z}[X, Y]$ est un polynôme irréductible qui s'annule en $(\pi_K, \zeta)$. Notez que ce sont des énoncés sans quantificateurs.

**9.1. Extensions algébriques**. Soient $(K, v)$ un corps valué, et $L$ une extension de Galois de $K$, que nous supposerons de degré fini sur $K$, avec $\mathcal{G}al(L/K) = G$.

La valuation $v$ aura en général plusieurs extensions distinctes à $L$, et elles seront toutes conjuguées par des éléments de $G$ : si $w : L \to \Gamma$ est un valuation étendant $v$, et $\sigma \in G$, alors $w \circ \sigma$ est aussi une valuation de $L$ étendant $v$. Pour l'existence

Pour (1) $\Rightarrow$ (2), on se place dans une clôture algébrique de $K$, et on écrit $f(T) = \prod_{i=1}^{r}(T - a_i)^{n_i}$ où les $a_i$ sont les racines de $f(T)$, et sont deux à deux distinctes. On se ramène facilement au cas où $g$ et $h$ sont unitaires. Puisque $g$ et $h$ sont relativement premiers, on peut supposer que pour $i < s$, $\operatorname{res} a_i$ est une racine de $g(T)$, et pour $i \geq s$, $\operatorname{res} a_i$ est une racine de $h(T)$. Il nous faut donc montrer que $\prod_{i<s}(T - a_i)^{n_i}$ a ses coefficients dans $\mathcal{O}_K$.

**9.2. Systèmes topologiques**. Soient $\mathcal{L}$ un langage, et $M$ une $\mathcal{L}$-structure. Un *système topologique sur* $M$ est la donnée, pour chaque $m \geq 1$, d'une topologie $\mathcal{T}_m$ sur $M^m$ satisfaisant les conditions suivantes :

(1) Si $t_1(x), \ldots, t_m(x)$ sont des $\mathcal{L}$-termes, $x$ un $n$-uplet de variables, alors l'application $M^n \to M^m$, $a \mapsto (t_1(a), \ldots, t_m(a))$ est continue.

(2) Tout singleton de $M$ est fermé.

(3) Pour tout symbole $n$-aire de relation $R$ de $\mathcal{L}$, pour tout $k \leq n$ et $1 \leq i_1 < i_2 < \ldots i_k \leq m$, si $R_{\bar{\imath}}$ dénote la relation $k$-aire obtenue à partir de $R$ en remplaçant les variables $x_j$ avec

$j \neq i_\ell$ par 0, alors l'ensemble $R_{\bar{\imath}} \cap (M \setminus \{0\})^k$ et son complémentaire $(M \setminus \{0\})^k \setminus R_{\bar{\imath}}$ sont ouverts dans $M^k$. [Nous ne considérons pas $=$ comme une relation de $\mathcal{L}$]

Notons que par (i) et (ii), si $t(x)$ est un $\mathcal{L}$-terme, alors $\{a \in M^n \mid t(a) = 0\}$ est fermé.

Parmi les ensembles ouverts, nous aurons aussi les ensembles de bases $\{a \in M^n \mid t(a) \neq 0\}$ pour $t(x)$ un $\mathcal{L}$-terme, et les ensembles de la forme $\{a \in M^n \mid t(a) \in R_{\bar{\imath}} \cap (M \setminus \{0\})^k\}$ et $\{a \in M^n \mid t(a) \in R_{\bar{\imath}} \cap (M \setminus \{0\})^k\}$, où $R_{\bar{\imath}}$ est comme dans (iii), et $t(x)$ est un $k$-uplet de $\mathcal{L}$-termes. Les intersections finies d'ensembles de cette forme seront appelés des *ensembles ouverts spéciaux* (de $M^n$).

**9.3. Théorème** Soit $\mathcal{L}$ un langage étendant le langage des anneaux, mais sans nouveau symbole de fonction d'arité positive (les constantes sont donc permises, ainsi que les relations). Soit $M$ une $\mathcal{L}$-structure qui est un anneau commutatif intègre, et dont la théorie élimine les quantificateurs. Supposons que de plus $M$ puisse être muni d'un système topologique, pour lequel tout sous-ensemble spécial ouvert de $M$ est infini.

Alors $M$ est algébriquement borné.

Pour la démonstration, voir l'article de L. van den Dries, *Dimension of definable sets, algebraic boundedness and Henselian fields*, Annals of Pure and Applied Logic 45 (1989), 189 – 209.

**9.4. Lemme**. Soit $K$ un corps, $f(T) \in K[T]$ un polynôme irréductible sur $K$, $\alpha$ une racine de $f(T) = 0$, et $L = K(\alpha)$. Alors $L$ est définissable dans $K$ (avec comme paramètres les coefficients de $f(T)$).

*Démonstration.* Ecrivons $f(T) = \sum_{i=0}^{n} a_i T^i$, avec $a_n = 1$ (on peut supposer que $f$ est unitaire) ; alors le $K$-espace vectoriel $L$ a pour base $\{1, \alpha, \ldots, \alpha^{n-1}\}$, et nous avons une bijection $L \to K^n$, qui à un élément $b$ de $L$ associe ses coordonnées par rapport à la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Nous allons montrer que les opérations $+^*$ et $\cdot^*$ induites sur $K^n$ sont définissables. Tout d'abord, $+^*$ est tout simplement l'addition usuelle de $K^n$ ; notons que $0^* = (0, 0, \ldots, 0)$ et $1^* = (1, 0, \ldots, 0)$. De plus le prédicat unaire correspondant au sous corps $K$ de $L$ est aussi définissable : un $n$-uplet $(x_1, \ldots, x_n)$ représente un élément de $K$ si et seulement si $x_2 = \cdots = x_n = 0$. La multiplication par $\alpha$ définit une transformation linéaire de $K^n$, dont la matrice par rapport à la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ est donnée par

$$M_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

puisque $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$. Alors $M_\alpha^2$ sera la matrice correspondant à la multiplication par $\alpha^2$, etc. Nous aurons donc, (avec $M_\alpha^0$ la matrice identité), pour $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$,

$$(x_1,\dots,x_n)\cdot^*(y_1,\dots,y_n)=\sum_{i=1}^{n}x_iM_\alpha^{i-1}\begin{pmatrix}y_1\\y_2\\\vdots\\y_n\end{pmatrix}.$$

**Corollaire**. Soit $(K,v)$ un corps valué Hensélien, et $f(T)$, $L$ comme ci-dessus. Alors le corps valué $(L,v)$ est définissable dans $K$.

*Démonstration.* Cela découle du lemme ci-dessus et du fait que l'extension de $v$ à $L$ est unique. Plus précisément, si $\beta\in L$ a pour polynôme minimal unitaire $g(T)$ sur $K$, alors $\beta$ et tous ses conjugués ont la même valuation ; comme le produit de $\beta$ et de ses conjugués est égal à $g(0)$, on obtient $v(\beta)=v(g(0))/\deg(g)$. En particulier $v(\beta)\geq 0 \iff v(g(0))\geq 0$, et $v(\beta)>0 \iff v(g(0))>0$.

Comme nous pouvons parler du sous-corps $K$ de $L$, nous pouvons définir les coefficients du polynôme minimal sur $K$ d'un élément de $L$.

**9.5. Remarques**. (1) Si $L$ est Galois sur $K$, on peut aussi interpréter $\mathcal{G}al(L/K)$ et son action sur $L$. On peut, de la même façon, interpréter plusieurs extensions algébriques finies de $K$ dans $K$. Cela nous permet d'interpréter dans $K$ des extensions algébriques qui ne sont pas nécessairement engendrées au-dessus de $K$ par un seul élément (c'est utile quand la caractéristique est positive).

(2) Notons que la définition de $L$ dans $K$ est uniforme en $(a_0,\dots,a_{n-1})$, et que le seul endroit où ces paramètres sont utilisés, est dans la définition de la multiplication. C'est-à-dire, la multiplication $\cdot^*$ est définie par un $n$-uplet de termes de la forme $t(a,x,y)$. De plus, si $b_0,\dots,b_{n-1}\in K$ sont tels que $g(T)=T^n+\sum_{i=0}^{n-1}b_iT^i$ est irréductible sur $K$, et si $M$ est engendré au-dessus de $K$ par une racine $\beta$ de $g(T)=0$, alors le n-uplet $t(b,x,y)$ définit une opération $\cdot^*$ sur $K^n$ qui le rend isomorphe à $M$.

Nous pourrons donc, dans $K$, dire des choses du genre : pour toute extension $L$ de $K$ de degré $n$, il existe une extension $M$ de degré $m$ de $K$ contenant $L$ et telle que $(M,L,K)$ satisfait une certaine propriété du premier ordre du langage des anneaux augmenté de deux prédicats unaires pour les sous-corps $K$ et $L$.