École Normale Supérieure
Département de Mathématiques et Applications

Exposé de première année

Responsables : Martin Hils & Silvain Rideau

Théorie des modèles de $\mathbb{Q}_p$
Rationalité des séries de Poincaré

Jean-François MARTIN
& Davide STEFANI

Paris, le 18 juin 2013

Table des matières

Introduction

Historiquement, les premières application de la théorie des modèles étaient dues à l'élimination des quantificateurs dans certains modèles simples. Par exemple, le théorème d'Ax a été déduit de l'élimination des quantificateurs dans les corps algébriquement clos.

Suivant cette démarche, les modélistes ont tenté de démontrer l'élimination des quantificateurs dans de nombreux modèles. L'étude des nombres p-adiques, débutée par Ax et Cochen, s'est révélée particulièrement fructueuse une fois l'élimination des quantificateurs démontrée par Macintyre en 1976, débouchant en particulier sur la résolution de la conjecture d'Artin dans le cas p-adique. Nous nous intéresserons une autre application : la rationalité des séries de Poincaré P et $\tilde{P}$.

Historiquement, la rationalité de $\tilde{P}$ a été démontrée par Igusa et Meuser en utilisant le théorème d'Hironaka sur la résolution des singularités, celle de P, après avoir été conjecturée par Serre et Oesterlé, par Denef.

C'est cette dernière approche que nous suivrons dans ce rapport.

Nous tenons à remercier Martin Hils et Silvain Rideau pour leur encadrement enrichissant et motivant.

Résumé

Afin de démontrer l'élimination des quantificateurs dans $\mathbb{Q}_p$, nous utiliserons une stratégie de "va-et-vient" (théorème 4.1.9) qui nécessitera une bonne compréhension des extensions de corps valué. Nous étudierons donc dans un premier temps l'algèbre des corps valués, nous concentrant sur l'étude de leurs extensions et de leur théorie de Galos, avec une attention particulière envers les corps Henséliens.

Nous en déduiront alors que, sur le langage $\mathcal{L}_{\text{Mac}}$ de Macintyre, la théorie pCF des corps valués henséliens de corps résiduel isomorphe à $\mathbb{F}_p$ dont le groupe de valeurs est un $\mathbb{Z}$-groupe de plus petit élément $v(p)$ admet l'élimination des quantificateurs et est donc la théorie de $\mathbb{Q}_p$.

Cette élimination des quantificateurs permet alors une bonne compréhension des ensembles définissables dans $\mathbb{Q}_p^n$. Nous montrerons en particulier le théorème de décomposition cellulaire 6.4.3 permettant de partitionner finiment les ensembles définissables en de sous-ensembles sympathiques.

Cette bonne compréhension des ensembles définissables rend alors l'intégration sur ces derniers aisée, ce dont nous déduirons le théorème de rationalité abstrait 6.3.3 affirmant que certaines fonctions définies par une intégrale sur des ensembles définissables de $\mathbb{Q}_p^n$ sont essentiellement des fonctions rationnelles.

Finalement, les séries de Poincaré P et $\tilde{P}$, définies comme séries de comptages associées à des variétés de $\mathbb{Q}_p$, seront essentiellement de la forme précédente et nous prouverons donc qu'elles sont des fonctions rationnelles.

Chapitre 1

Rappels sur les valuations

1.1 Groupes ordonnés

Un *groupe ordonné* est une structure $(G, +, -, <, 0)$ dans le langage $\mathcal{L}_{GO} = \{+, -, <, 0\}$ qui respecte les axiomes qui disent que G est un groupe et $<$ est un ordre total sur G qui respecte l'opération, c'est à dire pour tout $g < h$ et u dans G, $g + u < h + u$ et $u + g < u + h$. Le groupe sera dit archimédien si $\forall x, y > 0,\ \exists n \in \mathbb{N} : nx > y$. Il ne faut pas oublier que ce n'est pas le cas général.

Définition 1.1.1. Le groupe des entiers $\mathbb{Z}$ est évidemment un groupe ordonné. Soit $\mathrm{Th}(\mathbb{Z})$ sa théorie dans le langage $\mathcal{L}_{GO,1} = \mathcal{L}_{GO} \cup \{1\}$. On dit que une $\mathcal{L}_{GO,1}$-structure G est un $\mathbb{Z}$-groupe si $G \models \mathrm{Th}(\mathbb{Z})$. C'est un résultat classique le fait que la théorie $\mathrm{Th}(\mathbb{Z})$ est axiomatisé par la théorie des groupes abéliens ordonnés sans torsion, à laquelle on rajoute les axiomes :

$$\forall x\ x > 0 \to x \geqslant 1$$

et le schéma d'axiomes

$$\exists^{=n} x\ \forall y \left(\bigwedge_{i \neq j} x_i - x_j \neq ny \right) \quad \forall n \in \mathbb{N}^{>0}.$$

Remarque 1.1.2. Si on ajoute au langage $\mathcal{L}_{GO}$ la constante 1 et les prédicats 1-aires $\{\overline{\mathrm{P}}_n |\ n \in \mathbb{N}\}$, et on ajoute à la théorie des $\mathbb{Z}$-groupes les axiomes

$$\forall x (\overline{\mathrm{P}}_n(x) \longleftrightarrow \exists\, y\ ny = x)$$

la théorie ainsi obtenue admet l'élimination des quantificateurs.

1.2 Extension d'anneaux

Soit R un anneau intègre, $R \subset K$ corps, $a \in K$ est dit *entier* sur R si il existe un polynôme unitaire $\mathrm{p}(x) \in R[x]$ tel que $\mathrm{p}(a) = 0$. Si tout $a \in K$

entier sur R est dans R, alors on dit que R est *intégralement clos* dans K. Si $R \subset S$ et tout élément de S est entier sur R on dit que $R \hookrightarrow S$ est une *extension entière*.

Remarque 1.2.1. Sont équivalentes :
- a entier sur R ;
- $R[a]$ est un R-module de type fini ;
- il existe $B \supset R[a]$ anneau tel que B est un R-module de type fini.

Si A est un anneau intègre, on note $K(A)$ le corps des fractions de A.

1.3 Valuations

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 ordonné, satisfaisant pour tout $a, b \in R$ et $\gamma \in \Gamma$:

1. $v(a) = \infty \longleftrightarrow a = 0$
2. $v(a + b) \geqslant \min\{v(a), v(b)\}$
3. $v(ab) = v(a) + v(b)$
4. $\gamma < \infty$ et $\gamma + \infty = \infty$

Remarque 1.3.1. Soit (K, v) un corps valué.

1. $v(1) = v(-1) = 0$, $v(ab^{-1}) = v(a) - v(b)$
2. $v(a) < v(b) \Rightarrow v(a + b) = v(a)$
3. si $v(\sum_{i=1}^{n} a_i) > \min\{v(a_i)\} \Rightarrow \exists\, i \neq j$ tels que $a_i = a_j$

Soit $\mathcal{O}_v := \{a \in K |\ v(a) \geqslant 0\}$, $\mathcal{M}_v := \{a \in K |\ v(a) > 0\}$, $\mathcal{O}_v$ est appelé *anneau de valuation*, dont $\mathcal{M}$ est l'unique idéal maximal. Clairement, $v(a) \leqslant v(b) \Rightarrow v(ba^{-1}) \geqslant 0 \Rightarrow ba^{-1} \in \mathcal{O}_v$, et $\mathcal{O}_v$ est intégralement clos dans K car si $a^n + b_1 a^{n-1} + \cdots + b_n = 0$ avec $b_i \in \mathcal{O}_v$, alors $v(a) < 0 \Rightarrow v(a^n) < v(b_i a^{n-i}) \Rightarrow v(0) = v(a^n)$ ce qui est absurde.

Définition 1.3.2. Le corps $\mathcal{O}_v/\mathcal{M}_v$ est appelé *corps résiduel*, noté κ_v et la projection $\mathcal{O}_v \xrightarrow{\text{res}} \mathcal{O}_v/\mathcal{M}_v$ est appelée *application résiduelle*.

Remarque 1.3.3. Dans la suite sera important de pouvoir, à partir de $\mathcal{O}_v$, retrouver le corps K et la valuation v. En effet :
- K est le corps des fractions de $\mathcal{O}_v$;
- $\mathcal{M}_v$ est l'ensemble des éléments non inversibles de $\mathcal{O}_v$, et le seul idéal maximal de $\mathcal{O}_v$;
- $\kappa_v = \mathcal{O}_v/\mathcal{M}_v, \text{res} : \mathcal{O}_v \longrightarrow \mathcal{O}_v/\mathcal{M}_v$;
- Γ est naturellement isomorphe à $K^*/\mathcal{O}_v^*$ car $K^* \xrightarrow{v} \Gamma$ est surjective, avec noyeau $\mathcal{O}_v^*$. L'ordre sur Γ est défini par $v(a) \leqslant v(b) \longleftrightarrow ba^{-1} \in \mathcal{O}_v$

1.4 Anneaux de valuation

Si R est un anneau commutatif intègre, K son corps des fractions, on dit que R est un *anneau de valuation* si $\forall a \in K \quad a \notin R \Rightarrow a^{-1} \in R$. Avec la construction ci-dessus, si R est un anneau de valuation, alors il est l'anneau de valuation d'une unique valuation sur K, de groupe de valeurs K^*/R^*.

Définition 1.4.1. Soit K corps, et $v : K \to \Gamma_v \cup \{\infty\}$, $w : K \to \Gamma_w \cup \{\infty\}$ valuations sur K. On dit que v et w sont équivalents si il existe un isomorphisme de groupes ordonnés $\phi : \Gamma_v \to \Gamma_w$ tel que $w = \phi \circ v$.

Chapitre 2

Nombres p-adiques

2.1 Valuations sur $\mathbb{Q}$

Si v est une valuation non triviale sur $\mathbb{Q}$, par 1. et 3. dans 1.3.1 on a que $v(n) = v(1 + \cdots + 1) \geqslant v(1) = 0$ donc $\mathbb{Z} \subset \mathcal{O}_v$. Soit $\mathcal{I} = \mathbb{Z} \cap \mathcal{M}_v$. $\mathcal{I}$ est maximal et v non triviale, donc $\mathcal{I} = p\mathbb{Z}$ avec $p \geqslant 2$ premier. Alors, le groupe des valeurs est isomorphe à $\mathbb{Z}$, où $1 = v(p)$, et $v(p^n a) = n$ si $a \wedge p = 1$. Si $q \in \mathbb{Q}$, il existe n, a, b tels que $p \wedge a = p \wedge b = 1$, $q = \frac{a}{b}p^n$, donc $v(q) = n$. On appelle v *valuation p-adique* sur $\mathbb{Q}$, de groupe de valeurs $\mathbb{Z}$ et corps résiduel $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On note v_p la valuation p-adique sur $\mathbb{Q}$.

2.2 Topologie, $\mathbb{Z}_p$, $\mathbb{Q}_p$

Soit (K, v) corps valué, Γ groupe de valeurs. On considère l'ensemble

$$\tau := \{\mathrm{B}(a, \gamma) |\ a \in K, \gamma \in \Gamma\} \text{ où } \mathrm{B}(a, \gamma) = \{x \in K |\ v(a - x) > \gamma\}.$$

Alors τ est base d'une topologie sur K, car si $c \in \mathrm{B}(a_1, \gamma_1) \cap \mathrm{B}(a_2, \gamma_2)$ et $\gamma_1 > \gamma_2$, alors $\mathrm{B}(c, \gamma_1) \subset \mathrm{B}(a_1, \gamma_1) \cap \mathrm{B}(a_2, \gamma_2)$ (en effet $v(x - a_i) = v(x - c + c - a_i) \geqslant \min\{v(x - c), v(c - a_i)\}$).

Remarque 2.2.1. Quand Γ est archimédien on peut supposer $\Gamma \subset \mathbb{R}$, donc $a \mapsto e^{-v(a)}$ est une norme qui induit la topologie ci-dessus sur le corps K.

Définition 2.2.2. Le corps des rationnels p-adiques $\mathbb{Q}_p$ est la complétion de $\mathbb{Q}$ avec la norme $|q| = e^{-v_p(q)}$. Il est facile de voir que le suites de Cauchy dans $\mathbb{Q}$ pour la topologie p-adique sont les $(x_n)_n$ telles que pour tout N il existe m avec $v(x_{n+1} - x_n) > N\ \forall n > M$. Alors la limite x de $(x_n)_n$ a valuation $v_p(x) = \lim_{x \to +\infty} v_p(x_n)$.

On note $\mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p}$ l'anneau des *entiers p-adiques*.

Remarque 2.2.3. v_p est bien définie sur $\mathbb{Q}_p$ car si $v_p(x_{n+1} - x_n) \xrightarrow{n} +\infty$ alors $\exists N\,;\, \forall n \geqslant N$, $v_p(x_n) = v_p(x_N)$. De plus on veut $v_p(x - x_n) \xrightarrow{n} +\infty$, ce qui n'est possible que si on a ultimement $v_p(x) = v_p(x_n)$.

Concrètement on peut penser $\mathbb{Z}_p$ comme l'ensemble des suites (a_n) d'entiers tels que $0 \leqslant a_n < p^n$ et $a_{n+1} \equiv a_n \pmod{p^n}$, avec les opérations définies par

$$(a_n) + (b_n) = (c_n) \longleftrightarrow \forall n \quad a_n + b_n \equiv c_n \pmod{p^n}$$

$$(a_n)(b_n) = (c_n) \longleftrightarrow \forall n \quad a_n b_n \equiv c_n \pmod{p^n},$$

où l'on identifie $\mathbb{Z}$ avec les suites ultimement constantes par

$$x \mapsto (x \pmod{p^n})_n$$

et où la valuation v_p est donnée par $v_p((a_n)_n) = \sup\{n |\ a_n = 0\}$.

En effet, la valuation y est positive, $\mathbb{Q}$ est dense dans le corps des fractions $\tilde{\mathbb{Q}}_p$ de cet anneau (muni de la valuation naturelle) et toute suite de Cauchy de $\mathbb{Q}$ y est convergente, ce qui est bien suffisant pour affirmer $\tilde{\mathbb{Q}}_p = \mathbb{Q}_p$.

Effectivement, si $\frac{(a_n)}{(b_n)} \in \tilde{\mathbb{Q}}_p$, et $(a_n^N)_n$ est défini par

$$a_n^N := \begin{cases} a_n & \text{si } n \leqslant N \\ a_N & \text{sinon} \end{cases}$$

alors

$$\frac{(a_n^N)}{(b_n^N)} \in \mathbb{Q} \text{ et } v_p\left(\frac{(a_n)}{(b_n)} - \frac{(a_n^N)}{(b_n^N)}\right) \overset{N\to\infty}{\longrightarrow} \infty.$$

d'où la densité de $\mathbb{Q}$.

De plus, si (x_k) est une suite de Cauchy de $\mathbb{Q}$, sa valuation étant ultimement constante, on peut après multiplication par le puissance de p idoine la considérer comme appartenant à $\mathbb{Z}$. Comme $v_p(x_{k+1} - x_k) \xrightarrow{k} +\infty$, pour tout n (x_k) sera ultimement constante modulo p^n, valant $a_n \in [\![0; p^n - 1]\!]$. Alors, la suite des (x_k) convergera bien vers l'élément (a_n) de $\tilde{\mathbb{Q}}_p$.

Chapitre 3

Extensions algébriques et corps Henséliens

3.1 Un résultat d'algèbre

Le but de cette section est de démontrer le théorème suivant :

Théorème 3.1.1. *Soit (K, v) corps valué et L une extension galoisienne algébrique de K. Alors v s'étend à une valuation w de L, et si w' est une autre valuation de L étendant v, alors $\exists\, \sigma \in \mathrm{Aut}(L/K) : w' = w \circ \sigma$.*

On utilisera sans démonstration les propriétés simples de la localisation, et le lemme de Nakayama.

Lemme 3.1.2. *Si $R \subset S$ est une extension entière, $\mathfrak{P}$ un idéal premier de R, alors il existe un idéal premier $\mathfrak{Q} \subset S$ tel que $\mathfrak{Q} \cap R = \mathfrak{P}$. On dit que $\mathfrak{Q}$ est* au-dessus *de $\mathfrak{P}$. De plus, $\mathfrak{P}$ est maximal si et seulement si $\mathfrak{Q}$ l'est.*

Démonstration. On peut se réduire au cas où R est un anneau local : il y a une correspondance entre idéaux premiers de $R_{\mathfrak{P}}$ et idéaux de R qui intersectent $\mathfrak{P}$ en (0), de plus $R_{\mathfrak{P}} \hookrightarrow S_{\mathfrak{P}}$ est encore une extension entière, et les idéaux premiers de $S_{\mathfrak{P}}$ au-dessus de $\mathfrak{P}R_{\mathfrak{P}}$ correspondent à idéaux premiers de S au-dessus de $\mathfrak{P}$. On suppose donc R local ; il suffit de montrer que $\mathfrak{P}S \neq S$, car dans ce cas $\mathfrak{P}S$ est contenu dans un idéal maximal de S, et si $\mathfrak{Q}$ est un tel idéal, $\mathfrak{P} \subset \mathfrak{Q} \cap R$, et $\mathfrak{Q} \cap R$ est un idéal de R, qui ne contient pas 1, donc est égal à $\mathfrak{P}$.
Si par l'absurde $\mathfrak{P}S = S$, on a

$$1 = \sum_{i=1}^{n} a_i s_i \quad a_i \in \mathfrak{P},\ s_i \in S.$$

Alors $R[s_1, \ldots, s_n]$ est un R-module fini (car s_i est entier sur R) avec $\mathfrak{P}R[s_1, \ldots, s_n] = R[s_1, \ldots, s_n]$, donc par le lemme de Nakayama $R[s_1, \ldots, s_n] = 0$, contradiction.

Supposons maintenant que $\mathfrak{P}$ est maximal dans R. Alors $R/\mathfrak{P}$ est un corps, $R/\mathfrak{P} \hookrightarrow S/\mathfrak{Q}$ est une extension entière, donc $S/\mathfrak{Q}$ est un corps aussi, et $\mathfrak{Q}$ est maximal (si $b \in S/\mathfrak{Q}$ alors $R/\mathfrak{P}[b]$ est un corps, donc $b^{-1} \in R/\mathfrak{P}[b] \subset S/\mathfrak{Q}$).

Inversement si $\mathfrak{Q}$ est maximal, $S/\mathfrak{Q}$ est un corps, et $R/\mathfrak{P} \hookrightarrow S/\mathfrak{Q}$ est une extension entière. Si $R/\mathfrak{P}$ n'est pas un corps, il existe un idéal maximal $\mathfrak{M}$ dans $R/\mathfrak{P}$, donc il existe un idéal premier $\mathfrak{M}' \subset S/\mathfrak{Q}$ au-dessus de $\mathfrak{M}$, contradiction. □

Théorème 3.1.3. *Soir R un anneau de valuation, K son corps des fractions, $K \hookrightarrow L$ une extension de Galois finie, $S \subset L$ la clotûre intégrale de R dans L. Si $\mathfrak{P}$ est l'idéal maximal de R, et $\mathfrak{Q}, \mathfrak{Q}'$ des idéaux de S au-dessus de $\mathfrak{P}$, alors*

1. *$S_{\mathfrak{Q}}$ est un anneau de valuation, $L = K(S_{\mathfrak{Q}})$ et la valuation induite sur L étend v.*
2. *il existe $\sigma \in G = \mathrm{Gal}(L/K)$ tel que $\sigma(\mathfrak{Q}) = \mathfrak{Q}'$, et les valuation correspondants à $\mathfrak{Q}$ et $\mathfrak{Q}'$ ne sont pas équivalentes.*

Inversement si w est une valuation sur L que étende v, il existe $\mathfrak{Q} \subset S$ idéal tel que $\mathcal{O}_w = S_{\mathfrak{Q}}$.

Démonstration. 1. Soit $y \in L$, et soit $P_y(x) = x^n + a_0 x^{n-1} + \cdots + a_n \in K[x]$ le polynôme minimal de y sur K. On a $y \in S$ si et seulement si $P_y(x) \in R[x]$. Supposons ça ne soit pas le cas, alors $v(a_n) = \min\{v(a_i) |\ i \leqslant n\}$, et $P_{y^{-1}} = a_n^{-1} X^n P_y(X^{-1})$ est dans $R[x]$, et donc $y^{-1} \in S$. L'idéal maximal de $S_{\mathfrak{Q}}$ est $\mathfrak{Q}S_{\mathfrak{Q}}$, et $\mathfrak{Q}S_{\mathfrak{Q}} \cap R = \mathfrak{P}$, donc la valuation induite par $S_{\mathfrak{Q}}$ sur L étend celle induite par R sur K.

2. Supposons $\sigma(\mathfrak{Q}) \neq \mathfrak{Q}' \ \ \forall \sigma \in G$ c'est à dire $\sigma\mathfrak{Q} \neq \tau\mathfrak{Q}' \ \forall \sigma, \tau \in G$. D'après le théorème du reste Chinois, ($\mathfrak{Q}, \mathfrak{Q}'$ maximaux $\Rightarrow \sigma\mathfrak{Q} + \tau\mathfrak{Q}' = S$) on obtient un $x \in S$ tel que

$$x \equiv 1 \pmod{\sigma\mathfrak{Q}} \ \forall \sigma \in G$$

$$x \equiv 0 \pmod{\sigma\mathfrak{Q}'} \ \forall \sigma \in G$$

Le produit

$$y = \prod_{\sigma \in G} \sigma x$$

est fixé par l'action du Galois, donc $y \in \mathfrak{Q}' \cap R = \mathfrak{P}$ (car R est intégralement clos dans K). $x \notin \sigma\mathfrak{Q}$ pour tout $\sigma \in G$, donc $\sigma x \notin \mathfrak{Q}$ pour tout $\sigma \in G$, mais $\mathfrak{Q}$ est premier, donc $x \notin \mathfrak{Q}$, contradiction.

Or, si w est une valuation sur L étendant v, $S \subset \mathcal{O}_w$. En effet soit $a \in S$, et $a^n + b_1 a^{n-1} + \cdots + b_n = 0$ avec $b_i \in R$; alors si $w(a) < 0$, $w(a^n) < w(a^{n-i} b_i)$ pour tout $i > 0$, donc $\infty = w(0) = w(a^n + b_1 a^{n-1} + \cdots + b_n) = w(a^n)$ ce qui implique $a = 0$. $\mathcal{M}_w \cap S = \mathfrak{Q}$ est un idéal maximal de S donc l'anneau

$S_{\mathfrak{Q}}$ est exactement l'anneau de valuation de w, d'après la première partie du théorème. De plus, deux valuations équivalentes sur L ont même anneaux de valuation, donc évidemment les valuations induites par deux différents idéaux au-dessus de $\mathfrak{P}$ ne sont pas équivalents. □

On obtient comme corollaire le théorème 3.1.1 :

Démonstration. Soit R l'anneau de valuation de v, $\mathfrak{P}$ l'idéal maximal de R. Si S est la clotûre intégrale de R dans L et $\mathfrak{Q}$ est un idéal de S au-dessus de $\mathfrak{P}$, alors $S_{\mathfrak{Q}}$ est un anneau de valuation dont la valuation étend v.
Si maintenant w, w' sont des valuations étendant v à L, $\mathfrak{M}_w, \mathfrak{M}_{w'}$ sont des idéaux de S au-dessus de $\mathfrak{P}$, et pour le théorème 3.1.3 il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma\mathfrak{M}_w = \mathfrak{M}_{w'}$, de plus σ laissant invariant S, $\sigma(\mathcal{O}_w) = \sigma(S_{\mathfrak{M}_w}) = S_{\sigma(\mathfrak{M}_w)} = S_{\mathfrak{M}_{w'}} = \mathcal{O}_{w'}$, donc $w \circ \sigma = w'$

□

Dans la suite on va étudier certaines propriétés des extensions des corps valués.

3.2 Notation

Si $K \subset L$ corps, v une valuation sur K et w une valuation sur L qui étend v, on note $(K, v) \subset (L, w)$. On note les corps résiduels et les groupes de valeurs, respectivement $\kappa_K, \kappa_L, \Gamma_K, \Gamma_L$. Si $(K, v) \subset (L, w)$, $\Gamma_K \subset \Gamma_L$ et $\kappa_K \subset \kappa_L$, car le noyeau de l'application $\mathcal{O}_v \longrightarrow \mathcal{O}_w/\mathcal{M}_w$ est $\mathcal{M}_w \cap \mathcal{O}_v = \mathcal{M}_v$, donc

$$\mathcal{O}_v/\mathcal{M}_v \longrightarrow \mathcal{O}_w/\mathcal{M}_w$$

est injective.
En général les inclusion seront strictes, on note $f = f(L/K, w) := [\kappa_L : \kappa_K]$ le *degré d'inertie* de w sur K, et $e = e(L/K, w) := [w(L^*) : \Gamma_K]$ l'*indice de ramification* de v dans (L, w). On se demande, dans le cas où $K \subset L$ est une extension finie de corps valué, quand est-ce que on peut la décomposer en une tour d'extensions simples qui vérifient chacune une des conditions suivantes :

- $f = [L : K]$ auquel cas on dit que l'extension est *totalement résiduelle*, et on a $\kappa_K \subsetneq \kappa_L$ et $\Gamma_K = \Gamma_L$;
- $e = [L : K]$, auquel cas on dit que l'extension est *totalement ramifié*, et on a $\kappa_K = \kappa_L$ et $\Gamma_K \subsetneq \Gamma_L$;
- $\kappa_K = \kappa_L$ et $\Gamma_K = \Gamma_L$ auquel cas on dit que l'extension est *immédiate*.

Proposition 3.2.1. *Soient $(K, v) \subset (L, w)$ corps valués. Soient $a_1, \ldots, a_r \in \mathcal{O}_w$ tels que $\mathrm{res}\, a_1, \ldots, \mathrm{res}\, a_r$ soient linéairement indépendants sur κ_K, et*

$b_1, \ldots, b_s \in L^*$ tels que $w(b_1) + \Gamma_K, \ldots, w(b_s) + \Gamma_K$ soient deux-à-deux disjoints. Alors les éléments $a_i b_j \quad 1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s$ sont linéairement indépendants, et, si les $c_{ij} \in K$ sont non tous nuls,

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

Démonstration. Il suffit de montrer la deuxième assertion. Soit I l'ensemble des paires (i,j) telles que $v(c_{ij}) + w(b_j) = \delta := \min_{i,j}\{v(c_{ij}) + w(b_j)\}$. Alors dans I apparaît exactement un indice parmi les j, en effet si $j \neq j',\ v(c_{ij}) + w(b_j) = v(c_{i'j'}) + w(b_{j'})$ alors $w(b_j) - w(b_{j'}) \in \Gamma_K$, contradiction. Donc $I = \{(i, j_0) |\ w(b_{j_0}) + v(c_{ij_0}) = \delta\}$. Montrons que

$$w\left(\sum_i c_{ij_0} a_i b_{j_0}\right) = \delta.$$

En effet, si $c_{i_0 j_0} \neq 0$, et $d_i := c_{ij_0} c_{i_0 j_0}^{-1}$ on a

$$w\left(\sum_i c_{ij_0} a_i b_{j_0}\right) = w(c_{i_0 j_0} b_{j_0}) + w\left(\sum_i d_i a_i\right)$$

avec $v(d_i) = 0$, donc $d_i \in \mathcal{O}_v$ et la combinaison linéaire

$$\operatorname{res}(\sum d_i a_i) = \sum \operatorname{res} d_i \operatorname{res} a_i \neq 0$$

car $\operatorname{res}(d_{i_0}) = \operatorname{res} 1 = 1$ et les $\operatorname{res} a_i$ sont linéairement indépendants. Donc, comme $\forall x \in \mathcal{O}_w \quad w(x) \geqslant 0$ et $w(x) > 0 \longleftrightarrow \operatorname{res} x = 0$, on obtient que $w\left(\sum_i c_{ij_0} a_i b_{j_0}\right) = w(c_{i_0 j_0} b_{j_0}) = v(c_{i_0 j_0} b_{j_0}) = \delta$. En conclusion, comme

$$w\left(\sum_{(i,j)\notin I} c_{ij} a_i b_j\right) \geqslant \min_{(i,j)\notin I}\{v(c_{ij}) + w(b_j)\} > \delta = w\left(\sum_{(i,j)\in I} c_{ij} a_i b_j\right),$$

en utilisant 2. dans 1.3.1 on obtient le résultat. □

3.3 Groupes de décomposition et d'inertie

Soit $(K, v) \subset (L, w)$, avec $K \hookrightarrow L$ extension de Galois de degré n, $G = \operatorname{Gal}(L/K)$. On définit le groupe de décomposition de w dans L comme :

$$G_{dec,w} := \{\sigma \in G |\ \sigma(\mathcal{M}_w) = \mathcal{M}_w\} < G.$$

Vu que $\mathcal{O}_w$ est obtenu en localisant $\mathcal{O}$ en $\mathcal{O} \cap \mathcal{M}_w$, on peut définir de façon équivalente

$$G_{dec,w} = \{\sigma \in G |\ \sigma(\mathcal{O} \cap \mathcal{M}_w) = \mathcal{O} \cap \mathcal{M}_w\}.$$

On a facilement que si $w' = w \circ \sigma$, alors

$$G_{dec,w'} = \{\tau \in G |\, \tau(\mathcal{M}_{w'}) = \mathcal{M}_{w'}\} = \{\tau |\, \tau\sigma^{-1}(\mathcal{M}_w) = \sigma^{-1}\mathcal{M}_w\} = \sigma^{-1}G_{dec,w}\sigma$$

et que les extensions distinctes de v correspondent aux classes latérales de $G_{dec,w}$, c'est à dire si $[G : G_{dec}] = g$ et $\tau_1, \ldots, \tau_g$ sont des éléments de G tels que $G_{dec}\tau_i \cap G_{dec}\tau_j = \varnothing \quad \forall\ i \neq j$, alors les extensions de v sont $\{w \circ \tau_i |\ i = 1, \ldots, g\}$.

On définit L^{dec} comme étant le corps fixé par G_{dec}, alors pour la correspondance de Galois on a que

$$G_{dec} = \mathrm{Gal}(L/L^{dec}).$$

L'extension L^{dec} ainsi construite est la plus petite sous-extension $K \subset L^{dec} \subset L$ telle que la restriction de la valuation w à L^{dec} admette une unique extension à L. En effet d'après le théorème 3.1.1 les extension de $w|_{L^{dec}}$ sont du type $w \circ \sigma$, où $\sigma \in \mathrm{Aut}(L/L^{dec})$, mais par définition $\mathrm{Aut}(L/L^{dec}) = G_{dec} = \{\sigma |\ w \circ \sigma = w\}$ donc il existe une unique extension.

On admet le résultat suivant :

Théorème 3.3.1. *$K \hookrightarrow L^{dec}$ est une extension immédiate.*

3.4 Corps Hensélien

Définition 3.4.1. Soit (K, v) corps valué. (K, v) est dit *Hensélien* si pour tout polynôme $f(x) \in \mathcal{O}_v[x]$, pour tout $a \in \mathcal{O}_v$, si $\mathrm{res}\, f(a) = 0$, $\mathrm{res}\, f'(a) \neq 0$ alors il existe $b \in \mathcal{O}_v$ tel que $f(b) = 0$ et $\mathrm{res}\, b = \mathrm{res}\, a$.

Remarque 3.4.2. En ce cas b est l'unique élément de $\mathcal{O}_v$ satisfaisant $f(x) = 0$ et $v(x - a) > 0$. En effet si $c \neq b$ est un autre tel élément, on a $(x - b)(x - c) | f(x)$, donc $\mathrm{res}(x - b)\,\mathrm{res}(x - c) = (x - \mathrm{res}\, a)^2 |\, \mathrm{res}\, f(x)$, donc $\mathrm{res}\, f'(a) = 0$, absurde.

Théorème 3.4.3. *Soit (K, v) un corps valué. Sont équivalents :*

1. *(K, v) est Hensélien ;*
2. *Si L extension algébrique de K, alors v a une unique extension à L ;*
3. *Si $f(x) \in \mathcal{O}_v[x]$ est telle 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 $f(b) = 0$.*

Le fait que les extensions algébriques d'un corps Hensélien prolongent de façon unique la valuation sera utilisé dans la démonstration de l'élimination des quantificateurs dans le corps des p-adiques.

Démonstration. On a que pour toutes valuations sur L^{sep} il existe une unique extension à L. En effet l'existence est vrai en général et est un résultat

classique (voir [6] chap. 3.1), et l'unicité suive du fait que si $a \in L \backslash L^{sep}$, et $x^n - a^n$ est le polynôme minimal de a sur L^{sep}, alors $v(a) = \frac{1}{n} v(a^n)$. D'après le théorème d'existence d'extensions cité ci-dessus on voit que la condition :

"pour toute L extension algébrique de K, alors v a une unique extension à L"

est équivalente à la condition

"pour toute L extension de Galois de K, alors v a une unique extension à L".

On suppose donc L normale et séparable sur K, et soit w une extension de v à L, G_{dec} son groupe de décomposition et L^{dec} corps fixé par G_{dec}.

1) $\Rightarrow$ 2) Soit $id = \tau_1, \ldots, \tau_g$ un ensemble de représentant des classes latérales de G_{dec}, et $\mathcal{O}$ la clotûre intégrale de $\mathcal{O}_v$ dans L^{dec}. Vu que $\tau_i(\mathcal{M}_w \cap \mathcal{O}) + \tau_j(\mathcal{M}_w \cap \mathcal{O}) = \mathcal{O}$ on peut appliquer le théorème du reste chinois et obtenir un $a \in \mathcal{O}$ tel que :
   - $a \notin \mathcal{M}_w$
   - $a \in \tau_i \mathcal{M}_w$ si $i \geqslant 2$

   En particulier $a \in \sigma \mathcal{M}_w \quad \forall \sigma \notin G_{dec}$. Si $f(x) \in \mathcal{O}_v[x]$ est le polynôme minimal de a, $f(x) = \prod_{i=1}^{n} (x - a_i)$ et $a = a_1$, alors les autres racines sont de la forme $a_j = \sigma a$ avec $\sigma \notin G_{dec}$, donc $\operatorname{res} f(x) = \prod_{i=1}^{n} (x - \operatorname{res} a_i) = x^{n-1}(x - \operatorname{res} a)$ donc $\operatorname{res} a$ est une racine simple de $\operatorname{res} f(x)$, ce que implique qu'il existe $b \in \mathcal{O}_v$ tel que $f(b) = 0$, contradiction.

2) $\Rightarrow$ 1) Soit $f(x) \in \mathcal{O}[x]$, $a \in \mathcal{O}_v$ tels que $v(f(a)) > 0$, $v(f'(a)) > 0$. On peut supposer f irréductible. On montre que $\deg f = 1$, ce qui entraine qu'il existe un b tel que $f(b) = 0$ et $\operatorname{res} b = \operatorname{res} a$.
   Si $b_1, \ldots, b_n$ sont des racines de f, pour tout i, j, $w(b_i) = w(b_j)$ par unicité de w (car $\mathrm{Gal}(L/K)$ agit transitivement sur $\{b_1, \ldots, b_n\}$). Soit $\gamma := w(b_i)$. Soit

$$f(x) = c \prod_{i=1}^{n} (x - b_i) = c \left(\sum_{k=0}^{n} a_k x^{n-k} \right)$$

   Si $\gamma < 0$, $v(a_n) < v(a_i)$ car $v(a_n) = n\gamma < i\gamma \leqslant v(a_i)$ pour tout $i < n$, donc $\operatorname{res} f(x) = \operatorname{res}(c a_n)$ sur $\mathcal{O}_v$, mais $\operatorname{res} f(x)$ n'est pas constant, contradiction. Si $\gamma > 0$ on a $\operatorname{res} f(x) = \operatorname{res}(c) x^n$ donc $n = 1$ et f a une racine dans $\mathcal{O}_v$.
   Supposons alors que $\gamma = 0$. On peut donc supposer $c = 1$. $\operatorname{res} f(x) = \prod_i (x - \operatorname{res} b_i)$. Vu que f est irréductible, $\operatorname{res} f(x)$ est une puissance du polynôme minimal d'une de ses racines. En effet $\mathrm{Aut}(\kappa_L/\kappa_K)$ agit transitivement sur $\{\operatorname{res} b_1, \ldots, \operatorname{res} b_n\}$, car si $\sigma \in \mathrm{Gal}(L/K)$ telle que $\sigma(b_i) = b_j$, alors l'application $\overline{\sigma} : \kappa_L \longrightarrow \kappa_L$ telle que $\overline{\sigma}(\operatorname{res} a) = \operatorname{res} \sigma(a)$ est dans $\mathrm{Aut}(\kappa_L/\kappa_K)$ et $\overline{\sigma}(\operatorname{res} b_i) = \operatorname{res} b_j$. Donc en particulier tous les $\operatorname{res} b_i$ sont racines du même polynôme irréductible g, et $\operatorname{res} f = g^k$. Vu que $\operatorname{res} f$ a une racine simple, $k = 1$ et $\deg f = 1$.

3) $\Rightarrow$ 1) Soit $\operatorname{res} f(a) = 0$, $\operatorname{res} f'(a) \neq 0$. Alors si $g(x) = f(a+x)$, $v(g(0)) > 2v(g'(0))$, et il existe $b \in \mathcal{O}_v$ tel que $v(b) = v(g(0)) = v(f(a))$ et $f(a+b) = g(b) = 0$. En particulier $v(b) > 0$ donc $\operatorname{res}(a+b) = \operatorname{res} a$.
1) $\Rightarrow$ 3) Soit $c = -f(0)/f'(0)$, et $g(x) := f(cx)/f(0)$. Alors $g(x) \in \mathcal{O}_v[x]$, $g(0) \in \mathcal{M}_v$ et $g'(0) + 1 \in \mathcal{M}_v$.

□

Corollaire 3.4.4. *Si (K, v) corps valué, w une extension 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 unique plus petit corps Hensélien contenant K, qui est en particulier le sous-corps de K^{sep} fixé par $G_{dec,w}$. Il est unique à K-isomorphisme près, et on le note K^h.*
3. *K^h est une extension immédiate de K.*

Démonstration. 1. D'après le point 2. de 3.4.3.

2. Soit $K^h := K^{G_{dec,w}}$. Il suffit de montrer que, pour toute extension finie de Galois L de K, $w|_{K^h \cap L}$ admet une unique extension à L. Mais c'est clair car si $\overline{\sigma} \in G_{dec,\, w|_{K^h \cap L}}$, il existe un $\sigma \in G_{dec,w}$ tel que $\overline{\sigma} = \sigma|_{K^h \cap L}$, donc le corps fixé par $G_{dec,\, w|_{K^h \cap L}}$ est exactement $K^h \cap L$ et on obtient le résultat. En particulier si $K^h \subset L$ est algébrique, w admet une unique extension, donc K^h est Hensélien. Inversement un corps Hensélien contenant K doit contenir le corps fixé par $G_{dec,w}$, donc K^h est le minimal. D'après le théorème 3.1.1 si w' est une autre extension de v à K^{sep}, il existe $\sigma \in \operatorname{Gal}(L/K)$ tel que $G_{dec,w'} = \sigma G_{dec,w} \sigma^{-1}$, donc $K^{G_{dec,w'}} = K^{\sigma G_{dec,w} \sigma^{-1}} = \sigma K^{G_{dec,w}}$ et donc K^h est unique à K-isomorphisme près.
3. Si $K \hookrightarrow L$ est une extension finie, $K^h \cap L = L^{dec}$ est une extension immédiate de K par le théorème 3.3.1, donc $K \hookrightarrow K^h$ est immédiate aussi.

□

On conclut cette section avec un important résultat dont on ne donne pas la démonstration :

Théorème 3.4.5. *Soit (K, v) un corps valué Hensélien, L une extension algébrique de K de degré n, et w l'unique extension de v à L. Alors $n = e(L/K) f(L/K) \chi^d$ où $d \geqslant 0$ entier et χ est la caractéristique de κ_K si elle est positive, et 1 sinon.*

Remarque 3.4.6. Une conséquence importante du théorème 3.4.5 est que en caractéristique résiduelle nulle, un corps valué Hensélien n'a pas des extensions immédiates propres.

On va introduire des nouveaux outils pour démontrer le même résultat dans le cas où la caractéristique résiduelle est $p > 0$ et le groupe de valeurs a un plus petit élément π tel que $v(p)$ soit un multiple entier de π.

3.5 Suites pseudo-convergentes, pseudo-limites

Soit (K, v) un corps valué de groupe de valeurs Γ.

Définition 3.5.1. Une suite $\{a_\alpha\}_{\alpha<\lambda}$ d'éléments de K indexée sur un ordinal λ limite, est dite *pseudo-convergente* si il existe un $\alpha_0 < \lambda$ tel que

$$v(a_\sigma - a_\tau) > v(a_\tau - a_\beta) \text{ pour tout } \sigma > \tau > \beta \geqslant \alpha_0.$$

Dans la suite on va supposer $\alpha_0 = 0$ pour simplifier, tous les résultats se généralisent facilement au cas $\alpha_0 > 0$.

Proposition 3.5.2. *Soit $\{a_\alpha\}_{\alpha<\lambda}$ suite pseudo-convergente. Alors :*

1. *soit $v(a_\alpha) > v(a_\beta)$ pour tout $\alpha > \beta$*
2. *soit il existe un $\gamma_0 < \lambda$ tel que $v(a_\alpha) = v(a_{\gamma_0})$ pour tout $\alpha > \gamma_0$.*

Démonstration. Supposons 1. ne soit pas vérifié , et soit $v(a_\alpha) \geqslant v(a_{\gamma_0})$ pour $\alpha < \gamma_0$. Alors pour tout $\sigma > \gamma_0$ $v(a_\sigma) = v(a_{\gamma_0})$, sinon $v(a_\sigma - a_{\gamma_0}) = \min\{v(a_\sigma),\ v(a_{\gamma_0})\} \leqslant v(a_{\gamma_0})$ et $v(a_{\gamma_0} - a_\alpha) \geqslant v(a_{\gamma_0})$, ce qui contredit $v(a_\sigma - a_{\gamma_0}) > v(a_{\gamma_0} - a_\alpha)$.

□

Remarque 3.5.3. On note que si $\{a_\alpha\}$ est une suite pseudo-convergente, $v(a_\sigma - a_\alpha) = v(a_{\alpha+1} - a_\alpha)$ pour tout $\sigma > \alpha$. En effet $v(a_\sigma - a_\alpha) = v(a_\sigma - a_{\alpha+1} + a_{\alpha+1} - a_\alpha) = v(a_{\alpha+1} - a_\alpha)$.

Définition 3.5.4. Un élément x de K est dit *pseudo-limite* de $\{a_\alpha\}_{\alpha>\lambda}$ si pour tout $\beta < \alpha$ $v(x - a_\beta) = v(a_{\beta+1} - a_\beta)$. On note $a_\alpha \Rightarrow x$.

On va étudier les extensions immédiates des corps valués.

Théorème 3.5.5. *Soit $(K, v) \subset (L, w)$ une extension immédiate. Alors tout élément de $L \backslash K$ est une pseudo-limite d'une suite pseudo-convergente dans K sans pseudo-limites dans K.*

Démonstration. Soit $a \in L \backslash K$, $I = \{w(a-b) |\ b \in K\}$. Alors I n'est pas borné, car si $b \in K$, il existe $c \in K$ tel que $w(a-b) = w(c)$, donc comme l'extension est immédiate et $w(\frac{a-b}{c}) = 0$, il existe $d \in K$ tel que $\operatorname{res} d = \operatorname{res} \frac{a-b}{c}$, c'est à dire $w(\frac{a-b}{c} - d) > 0$, donc $w(a - b - dc) > w(c) = w(a - b)$.
On choisit $\{c_\alpha\}_{\alpha<\lambda}$ tel que $\{w(a - c_\alpha)\}_{\alpha<\lambda}$ soit croissante et cofinale en I. Alors $w(c_{\alpha+1} - c_\alpha) = w((a - c_\alpha) - (a - c_{\alpha+1})) = w(a - c_\alpha)$ donc $\{c_\alpha\}_{\alpha<\lambda}$ est pseudo-convergente. De plus $\{c_\alpha\}_{\alpha<\lambda}$ n'a pas des pseudo-limites dans K (sinon si $a_0 \in K$ l'est, $w(a - a_0) = w((a - c_\alpha) - (a_0 - c_\alpha)) \geqslant w(c_{\alpha+1} - c_\alpha)$ pour tout α, mais $w(a - a_0) \in I$, absurde).

□

On veut obtenir des résultats dans l'autre direction : étant donnée une suite pseudo-convergente dans K qui n'a pas de limites dans K, on se demande s'il existe une extension immédiate de K où il y a des pseudo-limites. La réponse est toujours affirmative.

3.6 Formule de Taylor

Si K est un corps, $f(x) \in K[x]$, on appelle *formule de Taylor* de $f(x)$

$$f(x+y) = \sum_{i=0}^{\deg(f)} \mathrm{D}_i(f(x))y^i$$

où D_i est l'application K-linéaire de $K[x]$ dans $K[x]$ telle que $\mathrm{D}_i(x^n)$ est le coefficient de y^i dans $(x+y)^n$. La formule ci-dessus généralise la formule de Taylor standard aux corps de caractéristique quelconque.

Remarque 3.6.1. Si $f \in K[x]$, et $\{a_\alpha\}$ est une suite pseudo-convergente en K, alors $\{f(a_\alpha)\}$ est pseudo-convergente aussi. En effet $\{v(x-a_\alpha) = v(a_{\alpha+1}-a_\alpha) |\ \alpha < \lambda\}$ est finiment réalisé dans K, donc par compacité il existe $L \geq K$ où $\{a_\alpha\}_{\alpha<\lambda}$ a une pseudo-limite a. On a que

$$f(a) - f(a_\alpha) = \sum_{i=1}^{\deg(f)} \mathrm{D}_i\, f(a)(a-a_\alpha)^i.$$

On montre facilement qu'il existe un $\alpha_0 < \lambda$ et un i_0 avec $1 \leqslant i_0 \leqslant \deg f$ tels que pour tout $\alpha > \alpha_0$, $i \neq i_0$,

$$v(\mathrm{D}_{i_0}\, f(a)) + i_0 v(a-a_\alpha) < v(\mathrm{D}_i\, f(a)) + iv(a-a_\alpha)$$

donc en particulier pour $\alpha > \alpha_0$

$$v(f(a) - f(a_\alpha)) = v(\mathrm{D}_{i_0}\, f(a)) + i_0 v(a-a_\alpha),$$

en particulier $v(f(a)-f(a_\alpha))$ est ultimement croissante, et donc $v(f(a) - f(a_\alpha)) = v(f(a_{\alpha+1}) - f(a_\alpha))$, ce que implique que $\{f(a_\alpha)\}_{\alpha<\lambda}$ pseudo-converge (avec la définition donnée au-dessus).

Remarque 3.6.2. En particulier on obtient que si $a_\alpha \Rightarrow a$ alors $f(a_\alpha) \Rightarrow f(a)$.

Définition 3.6.3. On déduit que pur toute suite pseudo-convergente $\{a_\alpha\}$ et pour tout $f(x) \in K[x]$, il y a deux cas possibles :

1. il existe $\alpha_0 < \lambda$ tel que pour tout $\sigma > \alpha_0$ $v(f(a_\sigma)) = v(f(a_{\alpha_0}))$
2. pour tout $\sigma > \alpha$ $v(f(a_\sigma)) > v(f(a_\alpha))$.

On dit que $\{a_\alpha\}_{\alpha<\lambda}$ est de type *transcendant* si pour tout $f \in K[x]$ la condition 1. est vérifié, et de type *algébrique* si il existe $f \in K[x]$ pour lequel la condition 2. est vérifié.

Théorème 3.6.4. *Si $\{a_\alpha\}_{\alpha<\lambda}$ est une suite pseudo-convergente de type transcendant dans K sans pseudo-limites dans K, il existe une extension immédiate transcendante $(K,v) \subset (K(z),v)$, où la valuation est définie sur les polynômes $f \in K[x]$ par*

$$v(f(z)) = \lim_{\alpha\to\lambda} v(f(a_\alpha)).$$

De plus z est une pseudo-limite de $\{a_\alpha\}$.
Inversement si $(K,v) \subset (K(u),w)$ est une extension immédiate telle que $a_\alpha \Rightarrow u$, alors

$$\begin{array}{ccc} K(u) & \longrightarrow & K(z) \\ u & \longmapsto & z \end{array}$$

est un isomorphisme de corps valués.

Démonstration. L'application v est bien définie car $\{a_\alpha\}_{\alpha<\lambda}$ est de type transcendent, c'est de plus une valuation : pour σ suffisamment grand,

$$v(f(z)g(z)) = v(f(a_\sigma)g(a_\sigma)) = v(f(a_\sigma)) + v(g(a_\sigma)) = v(f(z)) + v(g(z))$$

et de même

$$v(f(z)+g(z)) \geqslant \min\{v(f(z)),\ v(g(z))\}.$$

L'extension $(K,v) \subset (K(z),v)$ est immédiate : en effet le groupe de valeurs est le même, et pour σ suffisamment grand

$$v(f(z)-f(a_{\alpha+1})) = v(f(a_\sigma)-f(a_{\alpha+1})) > v(f(a_{\alpha+1})-f(a_\alpha)) \geqslant 0$$

donc $\mathrm{res}(f(z)-f(a_{\alpha+1})) = 0$ ce qui implique $\mathrm{res}(f(z)) = \mathrm{res}(f(a_{\alpha+1}))$ et le corps résiduel est le même. Par définition $v(z-a_\alpha) = v(a_\sigma - a_\alpha)$ pour σ grand, donc z est une pseudo-limite de $\{a_\alpha\}_{\alpha<\lambda}$.
Soit u comme ci-dessus, on sait que $f(a_\alpha) \Rightarrow f(u)$, vu que $w(f(a_\alpha))$ est ultimement constant, nécessairement $w(f(u)) = v(f(a_\alpha))$ pour α suffisamment grand, et en particulier $w(f(u)) = v(f(z))$. □

Théorème 3.6.5. *Si $\{a_\alpha\}_{\alpha<\lambda}$ est une suite pseudo-convergente de type algébrique en K, sans pseudo-limite dans K, et si $q(x)$ est un polynôme de degré minimal qui satisfait la condition 2. dans 3.6.3, il existe une extension algébrique immédiate $(K,v) \subset (K(z),v)$ telle que z est racine de q, et pour tout $f(x)$ avec $\deg f < \deg q$, $v(f(z)) = \lim_{\alpha\to\lambda} v(f(a_\alpha))$. De plus, z est une pseudo-limite de $\{a_\alpha\}_{\alpha<\lambda}$.*
Inversement, si u est une racine de $q(x)$, $(K,v) \subset (K(u),w)$ avec $a_\alpha \Rightarrow u$, alors

$$\begin{array}{ccc} K(u) & \longrightarrow & K(z) \\ u & \longmapsto & z \end{array}$$

est un isomorphisme de corps valué.

Démonstration. Notons que $q(x)$ est de degré > 1, sinon $q(x) = x - a$, et on aurait $a_\alpha \Rightarrow a$. De plus, $q(x)$ est irréductible, sinon si $q(x) = q_1(x)q_2(x)$ soit q_1 soit q_2 satisfait 2. dans 3.6.3, ce qui contredit la minimalité de $\deg q$. Toute la preuve du théorème est similaire à celle du théorème 3.6.4, sauf la démonstration du fait que v est une valuation : si $f,\ g \in K[x]$, $\deg f < \deg q$, $\deg g < \deg q$, on a $f(x)g(x) = q(x)s(x) + r(x)$, avec $\deg r < \deg q$, donc $f(a_\alpha)g(a_\alpha) - r(a_\alpha) = q(a_\alpha)s(a_\alpha)$. Or, ultimement la valuation de $q(a_\alpha)s(a_\alpha)$ croît strictement, et celle de $f(a_\alpha)g(a_\alpha)$, et de $r(a_\alpha)$ est ultimement constante. Donc pour avoir égalité il est nécessaire que $v(f(a_\alpha)g(a_\alpha)) = v(r(a_\alpha))$ ultimement, c'est à dire $v(f(z)g(z)) = v(r(z))$. □

On obtient un important résultat sur les extensions des corps valué Henséliens :

Théorème 3.6.6. *Soit (K, v) un corps valué Hensélien de caractéristique nulle, de caractéristique résiduelle $p > 0$ et de groupe de valeurs isomorphe à $\mathbb{Z}$. Alors K n'a pas d'extension algébrique immédiate propre.*

Démonstration. D'après le théorème 3.6.5, il suffit de montrer que toute suite pseudo-convergente de type algébrique a une pseudo-limite dans K. Soit $\{a_\alpha\}_{\alpha<\lambda}$ une telle suite, a une pseudo-limite dans une extension $L = K(a)$, et soit $f(x)$ le polynôme minimal de a sur K (d'après le théorème 3.6.5 on peut supposer a algébrique sur K). On a que $f(a_\alpha) \Rightarrow f(a)$ et $f'(a_\alpha) \Rightarrow f'(a) \neq 0$. Vu que Γ_K est isomorphe à $\mathbb{Z}$, $\{v(f(a_\alpha))\}$ est cofinale dans Γ_K, et $v(f'(a_\alpha)) = v(f'(a))$ ultimement. On a en particulier ultimement $2v(f'(a_\alpha)) < v(f(a_\alpha))$, et par le théorème 3.4.3, existe un zéro de f dans K, c'est à dire $a \in K$.

□

En utilisant le théorème 3.4.5 et 3.6.5 on peu démontrer le résultat suivant, qu'on admettra dans la suite :

Théorème 3.6.7. *Soit (K, v) un corps valué Hensélien de caractéristique nulle, de caractéristique résiduelle $p > 0$ et tel que le groupe de valeurs Γ ait un plus petit élément 1 avec $v(p) = e1$, pour e entier strictement positif. Alors K n'a pas d'extension algébrique immédiate propre.*

On conclut le chapitre en démontrant que le corps $\mathbb{Q}_p$ est Hensélien.

Théorème 3.6.8. *Soit (K, v) un corps valué de groupe de valeurs archimédien, complet avec la topologie induite par v. Alors K est Hensélien.*

Démonstration. Soit $p(x) \in \mathcal{O}_v[x]$ tel que $v(p(a)) > 0$ et $v(p'(a)) = 0$. On construit une suite de Cauchy $(a_n)_n$ telle qu'elle converge vers une solution de $f(x) = 0$. Soit $a_0 = a$, $a_1 = a_0 - p(a)/p'(a)$, $\gamma := v(f(a))$. En utilisant la formule de Taylor,

$$p(a_1) = p(a_0)+p'(a_0)(a_1-a_0)+\sum_{i=0}^{\deg p} \mathrm{D}_i(p)(a_0)(a_1 - a_0)^i = \sum_{i=0}^{\deg p} \mathrm{D}_i(p)(a_0)(a_1 - a_0)^i$$

on obtient que $v(p(a_1)) \geqslant 2v(a_0 - a_1) = 2\gamma$. Comme $\operatorname{res} a = \operatorname{res} a_1$, on a aussi $\operatorname{res} p'(a_1) \neq 0$. On définit ainsi $a_{n+1} = a_n - f(a_n)/f'(a_n)$, et on vérifie $v(f(a_{n+1})) \geqslant 2v(a_{n+1} - a_n) \geqslant 2^{n+1}\gamma$. La suite (a_n) est de Cauchy, et si $b \in \mathcal{O}_v$ est une limite de telle suite, vu que $p(a_n)$ pseudo-converge vers $p(b)$, et $v(p(a_n)) \geqslant 2^n\gamma$ est cofinale en Γ, on obtient $v(p(b)) = \infty$, ce qui est équivalent à $p(b) = 0$. □

Chapitre 4

Théorie des modèles et corps valués

Le but de cette section est de démontrer que étant donnée une théorie T, T admet l'élimination des quantificateurs si et seulement si pour tous modèles $\mathcal{N}$, $\mathcal{M}$ $\aleph_1$-saturés, et pour tout isomorphisme partiel $\sigma : A \to B$, avec $A \subset N$, $B \subset M$ dénombrables, et pour tout $a \in N \backslash A$, il existe $\overline{\sigma} : A \cup \{a\} \to M$ un isomorphisme partiel qui prolonge σ.

4.1 Types

Définition 4.1.1. On dit qu'une théorie T dans un langage $\mathcal{L}$ élimine les quantificateurs (EQ) si pour toute $\phi = \phi(\overline{x}) \in \mathcal{F}ml^{\mathcal{L}}$ il existe une formule sans quantificateurs $\psi = \psi(\overline{x})$ telle que

$$T \vdash \forall \overline{x}(\phi(\overline{x}) \longleftrightarrow \psi(\overline{x}))$$

On dit que ϕ est équivalente à ψ dans T, et on note $\phi \sim_T \psi$.

Remarque 4.1.2. Pour démontrer qu'une théorie T a l'EQ, il suffit de démontrer que toute formule du type $\exists\, y\phi(\overline{x}, y)$, avec ϕ sans quantificateurs, est équivalente dans T à une formule sans quantificateurs. En effet, si $\phi_1 \sim_T \psi_1$, $\phi_2 \sim_T \psi_2$, alors $\exists\, y\phi_1 \sim_T \exists\, y\psi_1$ et $\phi_1 \wedge \phi_2 \sim_T \psi_1 \wedge \psi_2$, $\neg\phi_1 \sim_T \neg\psi_1$, donc par induction sur l'hauteur de ϕ on obtient que toute formule est équivalente dans T à une formule sans quantificateurs.

Définition 4.1.3. Soit $\mathcal{M}$ une $\mathcal{L}$-structure, $A \subset M$. On dit qu'un ensemble de $\mathcal{L}_A$-formules, $\Sigma(\overline{x}) = \Sigma(x_1, \ldots, x_n)$ est un n-type sur A si pour tout sous-ensemble fini de $\Sigma(x_1, \ldots, x_n)$, $\{\phi_1(\overline{x}), \ldots, \phi_k(\overline{x})\}$, il existe $\overline{a} \in M^n$ tel que $\mathcal{M} \models \phi_1(\overline{a}) \wedge \cdots \wedge \phi_k(\overline{a})$.
On dit que $\Sigma(\overline{x})$ est *complète* si c'est un sous-ensemble maximale de $\mathcal{F}ml^{\mathcal{L}_A}$ avec cette propriété. On note $S_n(A)$ l'ensemble des n-types complets sur A.

On dit que $\mathcal{M}$ réalise $\Sigma(\overline{x})$ s'il existe $\overline{a} \in M^n$ tel que pour toute $\phi \in \Sigma(\overline{x})$ $\mathcal{M} \models \phi(\overline{a})$. Si $\overline{a} \in M^n$ et $A \subset M$ on définit

$$\mathrm{tp}(\overline{a}/A) := \{\phi(\overline{x}) |\ \mathcal{M} \models \phi(\overline{a})\}$$

et on l'appelle *type de $\overline{a}$ sur A*. Evidemment $\mathrm{tp}(\overline{a}/A) \in S_n(A)$.

- En général il existe des types qui ne sont pas réalisés, par exemple dans $(\mathbb{Q}, <)$, le 1-type $\Sigma(x) = \{x < q |\ q > 0\} \cup \{x > 0\}$ est finiment réalisé, mais pas réalisé.
- Si $\mathcal{M}$ est une $\mathcal{L}$-structure, $A \subset M$ et $\overline{a}, \overline{b} \in M^n$ tels que $\mathrm{tp}(\overline{a}/A) = \mathrm{tp}(\overline{b}/A)$, alors l'application $\sigma : A \cup \{\overline{a}\} \to A \cup \{\overline{b}\}$ telle que $\sigma|_A = \mathrm{id}_A$ et $\sigma(a_i) = b_i$ est un isomorphisme partiel élémentaire, i.e. pour toute formule $\phi \in \mathcal{F}ml^{\mathcal{L}}$, $x_1, \ldots, x_n \in A \cup \{\overline{a}\}$, $\mathcal{M} \models \phi(x_1, \ldots, x_k) \longleftrightarrow \mathcal{M} \models \phi(\sigma(x_1), \ldots, \sigma(x_k))$.

Proposition 4.1.4. *Soit $\mathcal{M}$ une $\mathcal{L}$-structure, p un n-type complet sur $A \subset M$, alors il existe $\mathcal{N} \succeq \mathcal{M}$ qui réalise p.*

Démonstration. On ajoute n constantes au langage, $c_1, \ldots, c_n$, et on considère la théorie $T' = \mathrm{D}^{el}(\mathcal{M}) \cup \{\phi(c_1, \ldots, c_n) |\ \phi(\overline{x}) \in p\}$, où $\mathrm{D}^{el}(\mathcal{M})$ est le diagramme élémentaire de $\mathcal{M}$. Alors par définition T' est finiment consistante, donc consistante, et si $\mathcal{N} \models T'$, $M \preceq \mathcal{N}$, et les interprétations de $c_1, \ldots, c_n$ dans la restriction de $\mathcal{N}$ au langage $\mathcal{L}$ réalisent p.

□

Soit ϕ une formule en $\mathcal{L}_A$, soit $<\phi>= \{p \in S_n(A) |\ \phi \in p\}$. L'ensemble $\{<\phi> \mid \phi\ \mathcal{L}_A$-formule$\}$ est une base d'ouverts d'une topologie sur $S_n(A)$. En effet $<x = x>= S_n(A)$, $<\neg\phi>= S_n(A) \setminus <\phi>$ et $<\phi> \cap <\psi>=<\phi \wedge \psi>$. Il est alors clair que les $<\phi>$ sont aussi une base de fermés dans cette topologie.

$S_n(A)$ est compact avec cette topologie. En effet si $\bigcap_i <\phi_i>= \varnothing$, l'ensemble de formules $\{\phi_i\}_i$ est incohérente, donc finiment incohérent, donc il existent $i_1, \ldots, i_n$ tels que $\phi_{i_1}, \ldots, \phi_{i_n}$ sont incohérent, et

$$\varnothing =<\bigwedge_{j=1}^{n} \phi_{i_j}>= \bigcap_{j=1}^{n} <\phi_{i_j}>.$$

On a démontré que pour tout famille de fermés d'intersection vide, il existe une sous-famille finie d'intersection vide, donc $S_n(A)$ est compact.

Définition 4.1.5. Soit κ cardinal infini. On dit que une $\mathcal{L}$-structure $\mathcal{M}$ est κ-saturé si pour tout $A \subset M$ avec $|A| < \kappa$, $p \in S_1(A)$, $\mathcal{M}$ réalise p.

Théorème 4.1.6. *Soit $\mathcal{M}$ est κ-saturé, $\lambda < \kappa$, $A \subset M$ avec $|A| < \kappa$ et $\overline{x}$ un uplet de variables de longueur λ. Alors pour tout $\Sigma(\overline{x})$ ensemble de $\mathcal{L}(A)$-formules en $\overline{x}$ qui est finiment satisfaisable dans $\mathcal{M}$, $\Sigma(\overline{x})$ est réalisé dans $\mathcal{M}$.*

Démonstration. On peut supposer $\Sigma(\overline{x})$ maximal. On considère les ensembles de formules

$$\Sigma_\beta := \{(\exists\, x_\gamma)_{\gamma \geqslant \beta} \phi(\overline{x}) |\ \phi(\overline{x}) \in \Sigma(\overline{x})\}$$

où les variables libres sont indexé sur β. Si $(m_\alpha)_{\alpha<\gamma}$ réalise Σ_γ, alors il existe $m_\gamma \in M$ tel que $(m_\alpha)_{\alpha<\gamma+1}$ réalise $\Sigma_{\gamma+1}$. En effet $\{\phi(\overline{m}, x_\gamma) |\ \exists\, x_\gamma \phi(\overline{x}) \in \Sigma_\gamma\}$ est finiment réalisé dans M, donc réalisé. Avec cette remarque, une facile induction sur $\beta < \lambda$ montre que il existe une suite $(m_\alpha)_{\alpha<\lambda}$ telle que $(m_\alpha)_{\alpha<\beta}$ réalise Σ_β d'où la conclusion.

□

Proposition 4.1.7. *$\mathcal{M}$ $\mathcal{L}$-structure, κ cardinal infini. Alors il existe $\mathcal{N} \geq \mathcal{M}$ κ-saturé.*

Démonstration. On construit, à l'aide de la proposition 4.1.4, une chaine élémentaire $(\mathcal{M}_\alpha)_{\alpha<\kappa^+}$ telle que :

- $\mathcal{M}_0 = \mathcal{M}$
- $\mathcal{M}_{\alpha+1} \geq \mathcal{M}_\alpha$ et pour tout $A \subset \mathcal{M}_\alpha$ avec $|A| < \kappa$, $\mathcal{M}_{\alpha+1}$ réalise tout les types dans $S_1(A)$
- $\mathcal{M}_\lambda = \bigcup_{\alpha<\lambda} \mathcal{M}_\alpha$ pour λ limite.

Alors $\mathcal{M}_{\kappa^+} \geq \mathcal{M}$, et si $A \subset M_{\kappa^+}$, avec $|A| < \kappa$, il existe $\alpha < \kappa^+$ tel que $A \subset M_\alpha$ (car $\mathrm{cof}(\kappa^+) = \kappa^+$). Par construction $\mathcal{M}_{\alpha+1}$ réalise $S_1(A)$, et donc $\mathcal{M}_{\kappa^+}$ aussi. □

Remarque 4.1.8. Soit $\mathcal{M}$ une $\mathcal{L}$-structure κ-saturé. Soient $A \subset M$, $B \subset M$, avec $|A| < \kappa$, $|B| < \kappa$, $\sigma : A \to B$ un isomorphisme partiel élémentaire. On peut montrer sans effort que pour tout $a \in M \backslash A$ il existe un morphisme partiel élémentaire $\overline{\sigma}$ qui prolonge σ et dont le domaine contient a. On dit que $\mathcal{M}$ est *κ-homogène.*

Théorème 4.1.9. *Soit T une théorie dans un langage $\mathcal{L}$ dénombrable. Sont équivalents :*

1. *T a l'EQ ;*
2. *Pour tout $\mathcal{M} \models T$, $\mathcal{N} \models T$ modèles $\aleph_1$-saturés, si $A \subset M$, $B \subset N$ sont des sous-structures dénombrables telles que $\sigma : A \to B$ est un isomorphisme, alors pour tout $a \in M \backslash A$ on peut prolonger σ à un isomorphisme partiel dont le domaine contient a.*

Démonstration.

1) $\Rightarrow$ 2) On peut supposer $A = B$ sous-structure commune de $\mathcal{M}$ et $\mathcal{N}$. Soit $p = \mathrm{tp}(a/A)$. Soit $\phi = \phi(\overline{b}, x) \in p$ avec $\overline{b} \in A^n$, $\phi \in \mathcal{F}ml^{\mathcal{L}}$, alors $\mathcal{M} \models \exists\, x \phi(\overline{b}, x)$. Mais T a l'EQ, donc $\exists\, x \phi(\overline{b}, x)$ est équivalente dans T à une formule sans quantificateurs $\psi = \psi(\overline{y})$, donc

$$\mathcal{M} \models \exists\, x \phi(\overline{b}, x) \overset{\mathcal{M} \models T}{\Longleftrightarrow} \mathcal{M} \models \psi(\overline{b}) \overset{\psi \text{ s.q.}}{\Longleftrightarrow} \mathcal{N} \models \psi(\overline{b}) \overset{\mathcal{N} \models T}{\Longleftrightarrow} \mathcal{N} \models \exists\, x \phi(\overline{b}, x).$$

Donc p est finiment réalisé dans $\mathcal{N}$, et par $\aleph_1$-saturation est réalisé en $b \in \mathcal{N}$ ($|A| \leqslant \aleph_0$). Il est clair que $A \cup \{a\} \longrightarrow A \cup \{b\}$ est un isomorphisme partiel.

2) $\Rightarrow$ 1) On démontre que chaque formule de la forme $\exists\, y\phi(\overline{x}, y)$, avec ϕ sans quantificateurs est équivalente dans T à une formule sans quantificateurs. C'est suffisant d'après la remarque 4.1.2. Par l'absurde, supposons que $\rho(\overline{x}) := \exists\, y\phi(\overline{x}, y)$ ne soit pas équivalente dans T à une formule sans quantificateurs. L'ensemble

$$T' = T \cup \{\psi(\overline{a}) \longleftrightarrow \psi(\overline{b}) |\ \psi \text{ sans quantificateurs}\} \cup \{\rho(\overline{a}) \longleftrightarrow \neg\rho(\overline{b})\}$$

est finiment consistante, sinon il existe $\psi_1, \ldots, \psi_k$ sans quantificateurs tels que

$$T' \vdash \left(\bigwedge_{i=1}^{k} \psi_i(\overline{a}) \longleftrightarrow \psi_i(\overline{b})\right) \longrightarrow \big(\rho(\overline{a}) \longleftrightarrow \rho(\overline{b})\big)\,.$$

Supposons $k = 1$. On obtient

$$T \vdash \forall \overline{x}, \overline{y}((\psi(\overline{x}) \longleftrightarrow \psi(\overline{y})) \longrightarrow (\rho(\overline{x}) \longleftrightarrow \rho(\overline{y}))$$

qui implique

$$T \vdash (\forall \overline{x}(\psi(\overline{x}) \longleftrightarrow \rho(\overline{x})) \vee (\forall \overline{x}(\neg\psi(\overline{x}) \longleftrightarrow \rho(\overline{x}))))$$

ce qui contredit l'hypothèse, car ψ et $\neg\psi$ sont sans quantificateurs. Le cas $k > 1$ est similaire.
Soit $\mathcal{M} \models T'$ un modèle $\aleph_1$-saturé, et $\overline{a}^{\mathcal{M}}, \overline{b}^{\mathcal{M}}$ les interprétations respectives de $\overline{a}$ et de $\overline{b}$ dans $\mathcal{M}$. Si A est la sous-structure engendrée par $\overline{a}^{\mathcal{M}}$ et B celle engendré par $\overline{b}^{\mathcal{M}}$, l'application $\sigma : A \to B$ qui envoie $\overline{a}^{\mathcal{M}}$ sur $\overline{b}^{\mathcal{M}}$ est un isomorphisme entre A et B. Si maintenant $c \in M$ est tel que $\mathcal{M} \models \phi(\overline{a}^{\mathcal{M}}, c)$, par hypothèse il existe $\overline{\sigma}$ un isomorphisme partiel étendant σ qui contient c dans son domaine, donc $\mathcal{M} \models \phi(\overline{b}^{\mathcal{M}}, \sigma(c))$ et par construction $\mathcal{M} \models \neg\exists\, y\phi(\overline{b}^{\mathcal{M}}, y)$, contradiction.

□

Chapitre 5

EQ dans les corps p-adiquement clos

5.1 Le langage $\mathcal{L}_{\mathrm{Mac}}$

On considère le langage $\mathcal{L}_{\mathrm{Mac}} = \{+, -, \cdot, 0, 1, \mathrm{div}, \mathrm{P}_n \mid n \in \mathbb{N}\}$ où div est une relation binaire, et P_n un prédicat unaire. Dans un corps valué le symbole div est interprété par

$$a \,\mathrm{div}\, b \longleftrightarrow v(a) \leqslant v(b) \longleftrightarrow ba^{-1} \in \mathcal{O}_v.$$

Le symbole P_n sera interprété par $\mathrm{P}_n(x) \longleftrightarrow \exists\, y\ y^n = x$.

On note pCF la théorie des corps p-adiquement closes dans le langage $\mathcal{L}_{\mathrm{Mac}}$, où :

- pCF contient la théorie des corps valués Henséliens
- le corps résiduel est $\mathbb{F}_p$
- le groupe de valeurs Γ est un $\mathbb{Z}$-groupe ordonné, i.e. un groupe abélien ordonné sans torsion tel que $\forall n \in \mathbb{N}\ [\Gamma : n\Gamma] = n$ et avec un plus petit élément positif
- $v(p)$ est le plus petit élément positive du groupe de valeurs
- pCF contient le schéma d'axiomes

$$\{\forall x(\mathrm{P}_n(x) \longleftrightarrow x \neq 0 \wedge \exists\, y\ y^n = x) \mid n \in \mathbb{N}\}.$$

On peut axiomatiser pCF dans le langage $\mathcal{L}_{\mathrm{Mac}}$: en effet si K est une $\mathcal{L}_{\mathrm{Mac}}$-structure tel que K est un corps valué, et div interprété comme ci-dessus, $\mathcal{O}_v$ est définissable dans K par la formule $\phi(x) = 1 \,\mathrm{div}\, x$. D'après la remarque 1.3.3, $\mathcal{M}_v, \kappa_v, \mathrm{res}, v, \Gamma_v$ sont intérpretables dans K, donc en particulier on peut axiomatiser dans $\mathcal{L}_{\mathrm{Mac}}$:

- la théorie des corps valué ;
- $\kappa_v = \mathbb{F}_p$ par la formule

$$\exists^{=p} x_i \in \kappa_v (\bigwedge_{i \neq j} x_i \neq x_j)$$

– $\Gamma_v \models$ GAOSt (Groupes Abéliens Ordonnés Sans torsion), et on ajoute l'énoncé

$$\exists^{=n} x_i \in \Gamma_v \forall y \in \Gamma_v (\bigwedge_{i \neq j} x_i - x_j \neq ny)$$

– $v(p)$ est le plus petit élément de Γ_v se dit par $\neg p \operatorname{div} 1$ et

$$\forall x((1 \operatorname{div} x \wedge \neg x \operatorname{div} 1) \longrightarrow p \operatorname{div} x)$$

– finalement on ajoute pour chaque $n \in \mathbb{N}$, si $f(x, \overline{y}) = x^n + x^{n-1}y_0 + \cdots + y_{n-1}$ et $f'(x, \overline{y}) = nx^{n-1} + \cdots + y_{n-2}$ l'énoncé

$$\forall x, \overline{y} \left(\operatorname{res} f(x, \overline{y}) = 0 \wedge \operatorname{res} f'(x, \overline{y}) \neq 0 \longrightarrow \exists z f(z, \overline{y}) = 0 \wedge \operatorname{res}(z) = \operatorname{res}(x) \right).$$

Dans la suite on utilisera plusieurs fois le résultat suivant :

Théorème 5.1.1. *Soient $(E, v) \subset (F, w)$ tels que $E \models pCF$ et $F \models pCF$. Alors :*

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 $n \in \mathbb{N}$, avec $n > 0$ minimal avec cette propriété. Alors il existe $b \in F$ tel que $b^n \in E$ et $w(b) = \gamma$.*

Démonstration. 1. On considère $p(t) = t^n - (1 + u)$. Alors $w(p(1)) = w(u) > 2w(n) = w(p'(1))$. D'après le théorème 3.4.3 il existe $b \in F$ tel que $b^n = 1 + u$ et $w(b - 1) = w(u) - w(n)$.

2. Supposons $n \wedge p = 1$, soient $a \in F$, $c \in E$ tels que $w(a) = \gamma$, $v(c) = n\gamma$. Vu que le corps résiduel est le même, on peut choisir c de façon que $\operatorname{res}(ac^{-n}) = 1$, i.e. $a^n = c(1 + u)$ avec $w(u) > 0 = 2w(n)$. D'après le théorème 3.4.3 $1 + u$ a une racine n-ième en F, et donc c aussi.

   Si maintenant $p|n$, il existe $m \in \mathbb{N}$ tel que $p|m$ et $w(u - m) > 2w(n)$ (on utilise le fait que Γ_F est un $\mathbb{Z}$-groupe). On a alors

$$\frac{1 + u}{1 + m} = 1 + \frac{u - m}{1 + m} = 1 + u',$$

   avec $w(u') > 2v(n)$, donc $1 + u'$ a une racine n-ième d. On obtient donc que

$$a^n = c(1 + u) = c(1 + m)(1 + u') = c(1 + m)d^n$$

   donc $v(c) = v(c) + v(1 + m) = v((\frac{a}{d})^n) = nv(\frac{a}{d})$.

□

Remarque 5.1.2. Le résultat est vrai si on suppose seulement que E et F sont Henséliens, ont même corps résiduel et groupe de valeurs avec le même plus petit éléments positif.

Théorème 5.1.3. *La théorie pCF admet l'élimination des quantificateurs.*

Démonstration. On utilise le théorème 4.1.9 : il suffit de montrer que pour tout $\mathcal{M},\mathcal{N} \models pCF$, $\mathcal{M},\mathcal{N}$ $\aleph_1$-saturés, pour tout $A \subset M$, $B \subset N$ sous-structures dénombrables et $\sigma : A \to B$ isomorphisme, et tout $a \in M\backslash A$, il existe un isomorphisme partiel $\overline{\sigma}$ qui étende σ et dont le domaine contient a.

Notons d'abord que σ s'étend à un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme entre les corps des fractions $\sigma' : K(A) \to K(B)$. En effet on a

$$\frac{a}{b} \operatorname{div} \frac{c}{d} \longleftrightarrow ad \operatorname{div} bc,$$

et

$$\mathrm{P}_n(ab^{-1}) \longleftrightarrow \mathrm{P}_n(ab^{n-1}),$$

donc on peut supposer que A et B sont des corps. On considère une sous-structure élémentaire $\mathcal{C} \preceq \mathcal{M}$ dénombrable telle que $A \cup \{a\} \subset C$, et on va prolonger σ à cette sous-structure en deux étapes :

1. On étend σ à un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme entre A^h et B^h
2. On étend σ à tout $\mathcal{C}$.

1. Vu que C est Hensélien, $A^h \subset C$, et de la même façon $B^h \subset N$. Par unicité de l'Hensélianisée, σ s'étend à un isomorphisme de corps valué $\overline{\sigma} : A^h \to B^h$. Il faut vérifier que $A^h \models \mathrm{P}_n(x) \longleftrightarrow B^h \models \mathrm{P}_n(\sigma(x))$: soit $x \in A^h$, alors $A^h \models \exists\, y\ y^n = x$ si et seulement si

$$\forall b \in B(x, v(x) + 2v(n)) \cap A \quad A^h \models \exists\, y\ y^n = b.$$

   En effet $b \in B(x, v(x) + 2v(n)) \cap A$ si et seulement si $v(b - x) > v(x) + 2v(n) \longrightarrow v(bx^{-1} - 1) > 2v(n)$, en utilisant le lemme 5.1.1, on a que bx^{-1} a une racine n-ième dans A^h, donc b aussi. Il suffit maintenant de remarquer que l'intersection est non-vide, ce qui suive du fait que $I = \{v(x-a) |\ a \in A\}$ est non-borné en Γ_A, que $v(x) \in I$ et que $v(n)$ est un multiple entier de 1.

   En particulier $\overline{\sigma}$ respecte les P_n i.e. est un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme. Par praticité on note ce isomorphisme σ au lieu de $\overline{\sigma}$.

2. D'abord on étend $\sigma : \Gamma_A \to \Gamma_B$ à un plongement $\sigma' : \Gamma_C \to \Gamma_N$ qui respecte les $\overline{\mathrm{P}}_n$, i.e. si $\alpha \in n\Gamma_C$ alors $\sigma'(\alpha) \in n\Gamma_N$. Pour faire ça, on énumère $\Gamma_C\backslash\Gamma_A = \{\gamma_\alpha\}_{\alpha<\lambda}$, et inductivement on construit $\sigma_\alpha : \Gamma_\alpha \to \Gamma_N$ un plongement tel que $\gamma_\alpha \in \Gamma_\alpha$, $\sigma_\alpha|_{\Gamma_\beta} = \sigma_\beta$ pour tout $\beta < \alpha$. Il suffit de poser : $\sigma_0 = \sigma$, $\sigma_\beta = \bigcup_{\alpha<\beta} \sigma_\alpha$ si β limite, et

$$\Gamma_{\alpha+1} = \begin{cases} \Gamma_\alpha & \text{si } \gamma_{\alpha+1} \in \Gamma_\alpha \\ < \Gamma_\alpha, \gamma_{\alpha+1} > & \text{si } \gamma_{\alpha+1} \notin \Gamma_\alpha \end{cases}$$

et dans le deuxième cas, $\sigma_{\alpha+1}$ s'étende à $\Gamma_{\alpha+1}$ en envoyant $\gamma_{\alpha+1}$ en $\beta_{\alpha+1}$ où $\beta_{\alpha+1} \in \Gamma_N$ tel que $\mathrm{tp}(\beta_{\alpha+1}/\Gamma_\alpha) = \mathrm{tp}(\gamma_{\alpha+1}/\Gamma_\alpha)$ (on identifie ici Γ_α et $\sigma'(\Gamma_\alpha)$), qui existe par $\aleph_1$-saturation de $\mathcal{N}$. On a que $\sigma' := \sigma_\lambda : \Gamma_C \to \Gamma_N$ est le plongement qui prolonge σ désiré. Notons que en admettant le résultat 1.1.2, et que les $\overline{\mathrm{P}}_n$ définis en 1.1.2 sont définissables en $\mathcal{L}_{\mathrm{Mac}}$, on a tout suite que le plongement $\Gamma_A \to \Gamma_B$ s'étend à Γ_C.
On va prolonger $\sigma : A^h \to B^h$ à C de façon à qu'elle coincide avec σ' sur le groupe des valeurs. On peut écrire C comme union d'une chaîne croissante de sous-corps $(C_n)_{N\in\mathbb{N}}$ tels que :
– $C_0 = (A^h)^{alg} \cap C$;
– $C_n^{alg} \cap C = C_n$;
– $\mathrm{tr.deg}(C_{n+1}/C_n) = 1$.

Lemme 5.1.4. *Soit $E \subset C$ tel que $E^{alg} \cap C = E$. Alors pour tout g isomorphisme de E dans un sous-corps de N tel que g induit σ' sur Γ_E, g respecte les prédicats P_n.*

Démonstration. Si $\mathcal{E} \models \mathrm{P}_n(a)$ alors $\mathcal{N} \models \mathrm{P}_n(g(a))$, car g est un isomorphisme. Inversement, supposons $\mathcal{N} \models \mathrm{P}_n(g(a))$. D'après le lemme 5.1.1, Γ_M/Γ_E est sans-torsion, car $\mathcal{C} \preceq \mathcal{M}$ et donc $E^{alg} \cap M = E$. E est donc Hensélien, car si f polynôme, $a \in E$ et $b \in M$ sont comme dans la définition 3.4.1, alors b est algébrique sur E, et donc est dans E. Comme σ' respecte les $\overline{\mathrm{P}}_n$, $\Gamma_N/\Gamma_{g(E)}$ aussi sera sans torsion. Or, $g(E)$ est Hensélien, donc par le théorème 3.6.7 $g(E)$ n'a pas d'extension algébrique immédiate propre. De plus $\kappa_{g(E)} = \kappa_N = \mathbb{F}_p$, donc $N/g(E)$ est purement ramifiée. Si par l'absurde $\mathcal{N} \models b^n{=}g(a)$ et $g(E) \models \neg\exists\, x\ x^n{=}g(a)$, on a que $v(b) \notin \Gamma_{g(E)}$, $nv(b) \in \Gamma_{g(E)}$, ce qui contredit $\Gamma_N/\Gamma_{g(E)}$ sans torsion. □

Extension de σ à C_0 : Supposons $E \subset C_0$ finiment engendré sur A^h. Alors E/A^h est totalement ramifié (car A^h Hensélien, E/A^h algébrique et $\kappa_E = \kappa_C = \kappa_{A^h}$). Soit

$$\Gamma_E/\Gamma_{A^h} = < \gamma_1 + \Gamma_{A^h} > \oplus \cdots \oplus < \gamma_m + \Gamma_{A^h} >$$

avec $\gamma_i + \Gamma_{A^h}$ d'ordre n_i. Par le lemme 5.1.1, E étant Hensélien, ils existent $\{a_i\}$ tels que

$$v(a_i) = \gamma_i \ ,\ a^{n_i} \in A^h \text{ et } [A^h(a_1, \ldots, a_i) : A^h(a_1, \ldots, a_{i-1})] = n_i.$$

Comme $[\Gamma_{A^h(a_1,\ldots,a_m)} : \Gamma_{A^h}] = [E : A^h]$, on a $A^h(a_1, \ldots, a_m) = E$. En plus pour tout i, $\mathcal{N} \models \mathrm{P}_{n_i}(\sigma(a_i^{n_i}))$. Il existent alors $b_1, \ldots, b_m$ dans N tels que $b_i^{n_i} = \sigma(a_i^{n_i})$. Alors

$$\begin{array}{ccc} \sigma_1 : A^h(a_1, \ldots, a_m) & \longrightarrow & B^h(b_1, \ldots, b_m) \\ a_i & \longmapsto & b_i \end{array}$$

est un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme. En effet σ_1 est un isomorphisme de corps valués : si $m = 1$ on a facilement

$$v(\sum_{j=1}^{n_i} \alpha_j a_1^j) = \min_j\{v(\alpha_j) + jv(a_1)\} \quad \forall \alpha_j \in A^h$$

et

$$v(\sigma_1(\sum_{j=1}^{n_i} \alpha_j a_1^j)) = \min_j\{v(\sigma(\alpha_j)) + jv(b_1)\}.$$

Enfin σ_1 induit σ' sur le groupe de valeurs, donc par le lemme 5.1.4 σ_1 est un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme. Une induction facile montre que ça vaut pour tout m.

On a montré que pour tout $k \in \mathbb{N}$, $x_1, \ldots, x_k \in C_0$ il existe un plongement de $A^h(x_1, \ldots, x_k)$ dans N. Cela entraine qu'il existe un plongement de C_0 dans N : d'après le théorème 4.1.6, di $\overline{x}$ est un uplet de variables indexé sur $|C_0\, \mathrm{A}^h\,|$, l'ensemble $\Sigma(\overline{x})$ des $\mathcal{L}_{A^h}$-formule sans quantificateurs satisfaites par C_0 est finiment réalisé dans M, donc réalisé ; ça entraine qu'il existe un plongement de C_0 dans N.

Extension à C_{n+1} : On a deux cas :

(a) $\Gamma_{C_{n+1}} \neq \Gamma_{C_n}$

(b) $\Gamma_{C_{n+1}} = \Gamma_{C_n}$

(a) On démontre à nouveau que pour tout $k \in \mathbb{N}$, $x_1, \ldots, x_k \in C_{n+1}$, il existe un plongement $f : E = C_n(x_1, \ldots, x_k) \longrightarrow N$ qui induit σ' sur le groupes de valeurs. $\Gamma_E/\Gamma_{C_n} \simeq \mathbb{Z}$ car Γ_E/Γ_{C_n} est sans torsion, et $\mathrm{tr.deg}(C_{n+1}/C_n) = 1$. Donc $\Gamma_E = \Gamma_{C_n} \oplus < v(a) >$ pour un $a \in E$; soit $b \in N$ tel que $v(b) = \sigma'(v(a))$. D'après le théorème 5.1.1 et la proposition 3.2.1

$$\begin{array}{ccc} C_n(a) & \longrightarrow & \sigma(C_n)(b) \\ a & \longmapsto & b \end{array}$$

est un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme, et vu que $E \subset C_n(a)^h$, on peut étendre σ à E tout entier. On peut donc étendre σ à toutes les corps finiment engendré sur C_n et en raisonnant comme dans le cas de C_0 on étend σ à C_{n+1} entière.

(b) On considère le type $\{v(x - \sigma(c)) = \sigma(v(a - c))|\ c \in C_n\} = p$ qui est finiment réalisé en N, donc réalisé par $\aleph_1$-saturation. Soit b qui réalise p

$$\begin{array}{ccc} C_n(a) & \longrightarrow & \sigma(C_n)(b) \\ a & \longmapsto & b \end{array}$$

est un $\mathcal{L}_{\mathrm{Mac}}$-isomorphisme, et on peut l'étendre à $C_{n+1} = C_n(a)^h$(car $C_{n+1}/C_n(a)$ est algébrique et immédiate, et C_{n+1} Hensélien).

□

Chapitre 6

Décomposition cellulaire

6.1 Fonctions de Skolem définissables en pCF

Définition 6.1.1. Soit T une théorie dans un langage $\mathcal{L}$. On dit que T *a des fonction de Skolem définissables* si pour toute $\mathcal{L}$-formule $\phi(\overline{x}, y)$ il existe une formule $\psi(\overline{x}, y)$ telle que :

(i) $T \vdash \forall \overline{x}, y\,(\psi(\overline{x}, y) \longrightarrow \phi(\overline{x}, y))$

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

(iii) $T \vdash \forall \overline{x}\,(\exists\, y\ \phi(\overline{x}, y) \longrightarrow \exists\, y\ \psi(\overline{x}, y))$

On veut démontrer que si $K \models p\mathrm{CF}$ alors K admet des fonctions de Skolem définissables.

Théorème 6.1.2. *Si T est une $\mathcal{L}$-théorie avec l'EQ, sont équivalentes :*

- *T admet des fonctions de Skolem définissables*
- *$\forall A \models T_\forall$ il existe $A \subset B \models T$ tel que B est algébrique sur A et rigide sur A i.e. le seul $\sigma : B \to B$ A-automorphisme est l'identité.*

On démontre donc que les corps p-adiquement clos ont des fonctions de Skolem en utilisant la deuxième condition.

Théorème 6.1.3. *Pour tout $A \models pCF_\forall$ il existe $A \subset B \models pCF$ tel que B soit algébrique sur A et rigide sur A.*

Démonstration. Soit $A \models p\mathrm{CF}_\forall$. Alors il existe $\mathcal{M}$ tel que $A \subset \mathcal{M} \models p\mathrm{CF}$. On considère la clotûre algébrique de $K(A)$ dans M, $C = K(A)^{alg} \cap M$. Alors ($\mathcal{M}$ étant Hensélien) C est un corps Hensélien, et $\mathrm{P}_n(C) = \{x^n |\ x \in C\}$. Il suffit de montrer que Γ_C est un $\mathbb{Z}$-groupe pour obtenir $C \preceq \mathcal{M}$, d'après le théorème 5.1.3.

Lemme 6.1.4. *Γ_C est un $\mathbb{Z}$-groupe.*

Démonstration. Γ_C est un sous-groupe d'un $\mathbb{Z}$-groupe, donc il suffit de montrer que $[\Gamma_C : n\Gamma_C] = n$ pour tout $n \in \mathbb{N}$. Si $p \mid n$ c'est évident. Supposons

alors que $p \wedge n = 1$. Soit donc $\gamma \in \Gamma_C$, $b \in C$ tel que $v(b) = \gamma$. Vu que Γ_M est un $\mathbb{Z}$-groupe, il existe $i \in \{1, \ldots, n-1\}$, $u \in M$ tels que $v(bp^i) = nv(u)$. On peut choisir $a \in C$ tel que $v(a) = 0$ et $\mathrm{res}(abp^i u^{-n}) = 1$, i.e. $abp^i = u^n(1+x)$ avec $v(x) > 0$. D'après le théorème 5.1.1, $1 + x$ a une racine n-ième y dans M, donc $abp^i = (uy)^n$ et $\mathcal{M} \models \mathrm{P}_n(abp^i)$, ce qui implique $C \models \mathrm{P}_n(abp^i)$. Soit $c \in C$ tel que $c^n = abp^i$, alors

$$v(b) = v(c^n a^{-1} p^{-i}) = nv(c) + i \equiv i \pmod{n\Gamma_C}.$$

On a donc démontré que $[\Gamma_C : n\Gamma_C] \leqslant n$, ce que implique $[\Gamma_C : n\Gamma_C] = n$. □

On conclut que $C \preceq \mathcal{M}$.
Montrons que C est rigide sur A. Soit $\sigma : C \to C$ un A-automorphisme. Soit $D \subset C$ le corps fixé par σ, et $b \in C$. Soit $d \in D$ tel que $C \models \mathrm{P}_n(d)$, et soit b une racine n-ième de d dans C. On trouve a et i tels que $C \models \mathrm{P}_m(bap^i)$, comme dans le lemme 6.1.4. Alors

$$C \models \mathrm{P}_m\left(\frac{\sigma(bap^i)}{bap^i}\right)$$

avec $\frac{\sigma(bap^i)}{bap^i} = \frac{\sigma(b)}{b}$ car $ap^i \in K(A)$. En plus $\frac{\sigma(b)}{b}$ est une racine n-ième de l'unité car $\sigma(b^n) = \sigma(b)^n = b^n$. On obtient $\frac{\sigma(b)}{b} \in \bigcap_{m \geqslant 1} (\mathbb{Q}_p^*)^m = \{1\}$, donc $\sigma(b) = b$ et $D = C$, et C est rigide sur A. □

La preuve montre aussi que si $A \subset M \models T$, $M \cap (K(A))^{alg} = dcl(A)$.

Théorème 6.1.5. *Si $K \models pCF$, et $\theta : K^n \longrightarrow \Gamma_K$ est une fonction définissable sur un ensemble $B \subset K$, alors θ est simple, c'est à dire il existe $D_1, \ldots, D_r$ partition de K^n en ensembles définissables sur B, $f_i, g_i \in K[\overline{x}]$, $n_i \in \mathbb{Z}\backslash\{0\}$ pour $i = 1, \ldots, r$ tels que*

$$\theta(\overline{x}) = \frac{1}{n_i} v\left(\frac{f_i(\overline{x})}{g_i(\overline{x})}\right) \ \forall i \ \forall \overline{x} \in D_i.$$

Démonstration. Soient $F_1 := K(< \overline{a}, B >)^h$ et $F_2 := <\overline{a}, B>^{alg} \cap K$. Si $\overline{a} \in K^n$, $\theta(\overline{a}) \in dcl(<\overline{a}, B>)$, car θ est définissable sur B, et d'après le théorème ci-dessus, $\theta(\overline{a}) \in F_2$. D'après le théorème 5.1.1, $\forall \gamma \in \Gamma_{F_2}\ \exists\, n \in \mathbb{N}$ tel que $n\gamma \in \Gamma_{F_1}$. De plus, F_1 et $K(< \overline{a}, B >)$ ont mêmes groupes de valeurs car l'extension est immédiate. Donc si $n\theta(\overline{a}) \in \Gamma_{F_1}$, il existe $f(\overline{x}), g(\overline{x}) \in \mathbb{Z}[B, \overline{x}]$ tels que $n\theta(\overline{a}) = v\left(\frac{f(\overline{a})}{g(\overline{a})}\right)$. Soit maintenant $\phi_{\overline{a}}(\overline{x})$ la formule

$$\theta(\overline{x}) = \frac{1}{n} v\left(\frac{f(\overline{x})}{g(\overline{x})}\right),$$

alors $<\phi_{\overline{a}}>$ est un ouvert dans $S_n(B)$ contenant $\mathrm{tp}(\overline{a}/B)$, et $\{<\phi_{\overline{a}}> \mid \overline{a} \in K^n\}$ est un recouvrement ouvert de $S_n(B)$. Par compacité il existe $\overline{a}_1, \ldots, \overline{a}_r$ tels

que $S_n(B) = \bigcup_{i=1}^{r} <\phi_{\overline{a}_i}>$, et en particulier si D_i est l'ensemble défini par la formule $\phi_{\overline{a}_i}$, on a

$$\theta(\overline{x}) = \frac{1}{n_i} v\left(\frac{f_i(\overline{x})}{g_i(\overline{x})}\right) \ \forall i \ \forall \overline{x} \in D_i.$$

□

6.2 Mesure de Haar

Afin de pouvoir intégrer, il nous faut avant tout considérer une mesure. Nous admettrons le théorème suivant :

Théorème 6.2.1. *Soit G un groupe localement compact.*
Il existe une mesure borélienne quasi-régulière non-nulle sur G vérifiant :
– $\forall A \in \mathcal{B}(A), \quad \mu(A) < \infty \Leftrightarrow \exists K$ *compact* $: A \subset K$.
– $\forall g \in G, \ \forall A \in \mathcal{B}(G), \quad \mu(g + A) = \mu(A)$.
De plus, cette mesure est unique à multiplication par une constante près.

Or, $\mathbb{Q}_p$ est localement compact (puisque, en décomposant en base p, $\mathbb{Z}_p$ est compact, or toute boule de $\mathbb{Q}_p$ est isomorphe à $\mathbb{Z}_p$), donc on peut considérer la mesure de Haar μ de $\mathbb{Q}_p$ définie en spécifiant $\mu(\mathbb{Z}_p) = 1$. On munit $\mathbb{Q}_p^n$ de la mesure produit, également notée μ.

La littérature a consacré la notation $|\mathrm{d}x| = \mathrm{d}\mu(x)$ pour l'intégration.

On remarque le fait suivant, utile dans certains calculs :

Proposition 6.2.2. $\forall a \in \mathbb{Q}_p, \ \forall A \in \mathcal{B}(\mathbb{Q}_p^n), \ \mu(aA) = p^{-nv(a)}\mu(A)$.

Démonstration. Il est clair qu'il suffit de le vérifier pour $n = 1$.

De plus, en itérant, il suffit de le vérifier pour $a = p$ et a tel que $v(a) = 0$.

Soit $\nu \colon A \mapsto \mu(pA)$.

Des propriétés analogues pour μ, il découle immédiatement que ν est une mesure de Haar sur $\mathbb{Q}_p$. Par unicité, elle est donc proportionnelle à μ.

Or, $\mathbb{Z}_p$ est l'union distincte des $i + p\mathbb{Z}_p$ pour $i = 1, ..., p-1$. Mais de plus, pour tout i, $\mu(i + p\mathbb{Z}_p) = \mu(p\mathbb{Z}_p) = \nu(\mathbb{Z}_p)$, d'où $\mu(\mathbb{Z}_p) = p\nu(\mathbb{Z}_p)$.

On a donc $\mu = p\nu$ et la conclusion pour $a = p$.

Supposons maintenant $v(a) = 0$.

Soit $\nu' \colon A \mapsto \mu(aA)$. Encore une fois, ν' est proportionnelle à μ. Mais, a étant inversible dans $\mathbb{Z}_p$, $\mathbb{Z}_p = a\mathbb{Z}_p$, d'où $\mu = \nu'$ et la conclusion. □

6.3 Séries de Poincaré

Soient $f_1(x), \ldots, f_r(x) \in \mathbb{Z}_p[x]$ avec $x = (x_1, \ldots, x_m)$. Soit $n \in \mathbb{N}$ et $a \in \mathbb{Z}_p^m$, on dénote $\overline{a}$ la classe de a dans $(\mathbb{Z}_p/p^n\mathbb{Z}_p)^m$,

$$\tilde{N}_n := \#\{\overline{a} \in (\mathbb{Z}_p/p^n\mathbb{Z}_p)^m | \ v(f_i(a)) \geqslant n \text{ pour } i = 1, \ldots, r\},$$

et

$$N_n := \#\{\overline{a} \in (\mathbb{Z}_p/p^n\mathbb{Z}_p)^m |\ \exists\, b \in \mathbb{Z}_p^m\ f_i(b) = 0 \text{ pour } i = 0, \ldots, r, \text{ et } \overline{a} = \overline{b}\}.$$

On définit le deux séries de Poincaré

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

Théorème 6.3.1. *P et $\tilde{P}$ sont des fonctions rationnelles.*

La démonstration se base sur le lemme suivant :

Lemme 6.3.2. *Soit D l'ensemble définissable*

$$\{(x, w) \in \mathbb{Z}_p^{m+1} |\ \exists y \in \mathbb{Z}_p^m : v(x - y) \geqslant v(w), \forall i = 1, \ldots, m, f_i(y) = 0\}$$

et $\tilde{D}$ l'ensemble définissable

$$\{(x, w) \in \mathbb{Z}_p^{m+1} |\ v(x) \geqslant v(w), \forall i = 1, ..., m, v(f_i(y)) \geqslant v(w)\}.$$

Pour tout $s > 0$, on pose

$$I(s) = \int_D |w|^s |\mathrm{d}x||\mathrm{d}w|, \text{ et } \tilde{I}(s) = \int_{\tilde{D}} |w|^s |\mathrm{d}x||\mathrm{d}w|.$$

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

Démonstration. Dans $\mathbb{Z}_p^m$, $v(a) \geqslant v(b)$ signifiera $v(a_i) \geqslant v(b_i) \forall i \in [\![1; m]\!]$.

$$\begin{aligned}
I(s) &= \int_D |w|^s |\mathrm{d}x||\mathrm{d}w| \\
&= \sum_{n=0}^{\infty} \int_{(x,w)\in D, v(w)=n} |w|^s |\mathrm{d}x||\mathrm{d}w| \\
&= \sum_{n=0}^{\infty} p^{-ns} \int_{(x,w)\in D, v(w)=n} |\mathrm{d}x||\mathrm{d}w| \\
&= \sum_{n=0}^{\infty} p^{-ns} \int_{(x,p^n)\in D, v(w)=n} |\mathrm{d}x||\mathrm{d}w|
\end{aligned}$$

(car la propriété $(x, w) \in D$ ne dépend en w que de sa valuation)

$$\begin{aligned}
&= \sum_{n=0}^{\infty} p^{-ns} \left(\int_{\{x \,|\, (x,p^n)\in D\}} |\mathrm{d}x| \right) \left(\int_{\{w \,|\, v(w)=n\}} |\mathrm{d}w| \right) \\
&= \sum_{n=0}^{\infty} p^{-ns} \frac{N_n}{p^{mn}} \left(\int_{\{w \,|\, v(w)=n\}} |\mathrm{d}w| \right)
\end{aligned}$$

(car $\{x \mid (x, p^n) \in D\}$ est l'union disjointe des $a_i + (p^n\mathbb{Z}_p)^m$, $i = 1, \ldots, N_n$ avec les a_i des représentants de chaque élément de l'image modulo p^n des solutions dans $\mathbb{Z}_p^m$ de $\bigwedge_{i=1}^m f_i(\overline{x}) = 0$, chacun de mesure $\mu((p^n\mathbb{Z}_p)^m) = p^{-nm}$)

$$= \sum_{n=0}^{\infty} p^{-ns} \frac{N_n}{p^{mn}} \left(\frac{1}{p^n} - \frac{1}{p^{n+1}} \right)$$

(car $\{w \mid v(w) = n\} = p^n\mathbb{Z}_p - p^{n+1}\mathbb{Z}_p$, de mesure respectives $\frac{1}{p^n}$ et $\frac{1}{p^{n+1}}$)

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

De même

$$\begin{aligned}
\tilde{I}(s) &= \int_{\tilde{D}} |w|^s |\mathrm{d}x||\mathrm{d}w| \\
&= \sum_{n=0}^{\infty} p^{-ns} \left(\int_{\{x \mid (x,p^n) \in \tilde{D}\}} |\mathrm{d}x| \right) \left(\int_{\{w \mid\ v(w)=n\}} |\mathrm{d}w| \right) \\
&= \sum_{n=0}^{\infty} p^{-ns} \frac{\tilde{N}_n}{p^{mn}} \left(\frac{1}{p^n} - \frac{1}{p^{n+1}} \right) \\
&= \frac{p-1}{p} \tilde{P}(p^{-m-1}p^{-s}).
\end{aligned}$$

□

Pour la rationalité des séries $P(t)$ et $\tilde{P}(t)$ il suffira donc le résultat de rationalité abstrait suivant, que on démontrera plus tard :

Théorème 6.3.3. *Soit $S \subset \mathbb{Q}_p^m$ définissable contenu dans un compact, e un entier strictement positif et $g\colon S \to \mathbb{Q}_p$ une fonction définissable à valuation dans $e\mathbb{Z} \cup \{\infty\}$ telle que $|g|$ soit bornée.*

On pose pour tout $s > 0$

$$Z(s) = \int_S |g(x)|^{s/e} |\mathrm{d}x|.$$

Alors, Z est une fonction rationnelle en p^{-s} :

$$\exists\, Q \in \mathbb{Q}(t) \ :\ \forall s > 0,\ Z(s) = Q(p^{-s}).$$

En effet avec ce résultat, on sait qu'il existe $Q(t), \tilde{Q}(t) \in \mathbb{Q}(t)$ tels que $P(p^{-m-1-s}) = Q(p^{-s})$ et $\tilde{P}(p^{-m-1-s}) = \tilde{Q}(p^{-s})$ pour tout $s \in \mathbb{R}^{>0}$. Alors $P(t) = Q(tp^{m+1})$ et $\tilde{P}(t) = \tilde{Q}(tp^{m+1})$ sur $]0, p^{-m-1}[$, ce qui implique l'égalité en tant que séries formelles.

Remarque 6.3.4. On s'aperçoit que, plus généralement, pour toute formule $\phi(\overline{x})$ du langage des anneaux auquel on a ajouté des constantes pour chaque élément de $\mathbb{Z}_p$, en notant $N_{\phi,n}$ le cardinal de l'image modulo p^n de l'ensemble $\{a \in \mathbb{Z}_p^m |\ \mathbb{Z}_p \models \phi(a)\}$ et $\tilde{N}_{\phi,n}$ le cardinal de $\{a \in \mathbb{Z}/p^n\mathbb{Z} |\ \mathbb{Z}/p^n\mathbb{Z} \models \phi(a)\}$, les séries $\tilde{P}_\phi(t) = \sum_{n=0}^{\infty} \tilde{N}_{\phi,n} t^n$ et $P_\phi(t) = \sum_{n=0}^{\infty} N_{\phi,n} t^n$ sont des fonctions rationnelles.

6.4 Décomposition cellulaire

Pour obtenir le théorème 6.3.3 on va partitionner les domaines d'intégration en ensembles beaucoup plus simples, où l'intégration est facile.

Théorème 6.4.1. *Soit $f(x,t) \in \mathbb{Q}_p[x,t]$ avec $x = (x_1, \ldots, x_m)$, t une variable, et soit $n \in \mathbb{N}^{>0}$. Il existe une partition finie de $\mathbb{Q}_p^{m+1}$ en sous-ensembles définissables A de la forme*

$$A = \{(x,t) \in \mathbb{Q}_p^{m+1} |\ x \in C,\ v(t - c_j(x)) \prec_{l,j} v(a_{l,j}(x)),\ j \in S,\ l \in S_j\} \quad (6.1)$$

où $C \subset \mathbb{Q}_p^m$ est définissable, $\prec_{l,j} \in \{\leqslant, \geqslant, >, <\}$, S et les S_j sont finis, et $c_j(x)$, $a_{l,j}(x)$ sont des fonction définissables $\mathbb{Q}_p^m \to \mathbb{Q}_p$, et qui sont tels que, pour tout $(x,t) \in A$, on a

$$f(x,t) = u(x,t)^n h(x) \prod_{j \in S} (t - c_j(x))^{e_j}, \quad (6.2)$$

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. Soit $f(x,t) = \sum_i a_i(x) t^i$. Alors $f(x,t)$ a degré fixé sur les ensembles définissables

$$C_k = \{x \in \mathbb{Q}_p^m |\ \bigwedge_{i=k+1}^{n} a_i(x) = 0 \wedge a_k(x) \neq 0\} \quad (6.3)$$

donc il suffit de démontrer la thèse sur un ensemble du type $C \times \mathbb{Q}_p$ sur lequel $f(x,t)$ a degré fixé d en t et C est définissable. Si $d = 0$ la thèse est évident ; si $d = 1$ on a $f(x,t) = a(x)t - b(x)$, et $\frac{b(x)}{a(x)}$ est définissable sur C, et le thèse est encore évident. Soit donc $d > 1$.
D'après le théorème A.0.1, il existe un nombre fini d'extensions de $\mathbb{Q}_p$ de degré $\leqslant d$, donc on se pose en K, le corps composite de toutes ces extensions. Vu que K est algébrique sur $\mathbb{Q}_p$, d'après le théorème 3.6.7, $N = [K : \mathbb{Q}_p]$ est égal au produit du degré d'inertie f pour l'indice de ramification e. Soit Γ_K engendré par $v(\pi)$, où $ev(\pi) = v(p) = 1$, et soient $1 = a_1, a_2 \ldots, a_f$ tels que $\operatorname{res} a_1, \ldots, \operatorname{res} a_f$ forment une base de κ_K sur $\mathbb{F}_p$. Alors d'après la proposition 3.2.1, on sait que les $a_i \pi^j$ pour $i = 1, \ldots, f$ et $j = 0, \ldots, e-1$ sont

linéairement indépendants, donc engendrent K comme $\mathbb{Q}_p$-espace vectoriel. Soit

$$\alpha_k = \begin{cases} 1 & \text{si } k = 1 \\ pa_i & \text{si } k = i,\ 1 < k \leqslant f \\ a_i \pi^j & \text{si } k = jf + i,\ 1 \leqslant j < e,\ 0 \leqslant i \leqslant f \end{cases}$$

alors $\{\alpha_i\}$ est aussi une base de K sur $\mathbb{Q}_p$. En plus $0 \leqslant v(\alpha_i) \leqslant 1$. Soit Ψ l'application

$$\begin{array}{ccc} {\mathbb{Q}_p}^N & \to & K \\ (q_1, \ldots, q_N) & \mapsto & \sum_i q_i \alpha_i \end{array}$$

Si $Z \subset C \times \mathbb{Q}_p$ est l'ensemble des zéros de $f(x,t)$, $\Psi^{-1}(Z)$ est un ensemble définissable de $\mathbb{Q}_p^N$, donc d'après le théorème 6.1.2 il existe $\beta_1(x), \ldots, \beta_d(x)$ de $\mathbb{Q}_p^m$ dans $\mathbb{Q}_p$ définissables telles que $f(x,t) = a_d(x) \prod_{i=1}^d (t - \beta_i(x))$, et $b_{i,j}(x)$ définissables de $\mathbb{Q}_p$ dans $\mathbb{Q}_p$ tels que $\beta_i(x) = \sum_j b_{j,i}(x)\alpha_j$. Vu que Z est définissable et $f(x,t) = 0$ sur Z, on peut se restreindre à partitionner $C \times \mathbb{Q}_p \backslash Z$.
Soit $I \cup J = \{1, \ldots, d\}$ une partition et $i : J \to \{2, \ldots, N\}$ une application. Soit $A = A_{I,J,i}$ l'ensemble des $(a,t) \in C \times \mathbb{Q}_p \backslash Z$ tels que :

$$\begin{array}{l} \forall j \in I\ v(t - b_{1,j}(a)) < v(b_{i,j}(a)) + v(\alpha_j) \text{ si } i \geqslant 2; \\ \forall j \in J\ v(b_{i(j),j}(a)) + v(\alpha_{i(j)}) \leqslant v(b_{k,j}(a)) + v(\alpha_k) \text{ si } k \neq i(j) \\ \forall j \in J\ v(b_{i(j),j}(a)) + v(\alpha_{i(j)}) \leqslant v(t - b_{1,j}(a)) \end{array} \quad (6.4)$$

En particulier on a que

$$\begin{array}{rcl} v(t - \beta_j(a)) & = & v(t - b_{1,j}(a)) \text{ si } j \in I \\ & = & v(b_{i(j),j}(a)\alpha_{i(j)}) \text{ si } j \in J \end{array}$$

On obtient

$$f(a,t) = a_d(a) \prod_{j \in I} (t - b_{1,j}(a)) \prod_{j \in J} b_{i(j),j}(a) \prod_j C_j(a,t)$$

pour tout $(a,t) \in A$, où

$$C_j(a,t) = \begin{cases} (t - \beta_j(a))(t - b_{1,j}(a))^{-1} & \text{si } j \in I \\ (t - \beta_j(a)) b_{i(j),j}(a)^{-1} & \text{si } j \in J \end{cases}$$

Vu qu'il y a un nombre fini de I, J, i comme ci-dessus, et que A est définissable, il suffit de trouver une décomposition de $f(x,t)$ comme dans l'équation (6.2) pour A.

Soit $\lambda = 2v(n) + 1$. On considère les classes $\pmod{p^{\lambda+d}}$ des éléments :

$$\frac{b_{i,j}(a)}{t - b_{1,j}(a)} \quad j \in I,\ 2 \leqslant i \leqslant N \quad (6.5)$$

et

$$\frac{t - b_{1,j}(a)}{b_{i(j),j}(a)},\ \frac{b_{i,j}(a)}{b_{i(j),j}(a)},\quad j \in J, 1 \leqslant i \leqslant N \tag{6.6}$$

On a dans le premier cas,

$$v\left(\frac{b_{i,j}(a)}{t - b_{1,j}(a)})\right) = v(b_{i,j}(a)) - v(t - b_{1,j}(a)) > -v(\alpha_j) \geqslant -1$$

donc vu que la valuation est entière, $v(\frac{b_{i,j}(a)}{t-b_{1,j}(a)}) \geqslant 0$, et les éléments du type (6.5) sont dans l'anneau de valuation $\mathbb{Z}_p$. Le même raisonnement vaut pour les éléments du type (6.6). On partition A en sous-ensembles définissables B tels que toutes les images de (6.5) et (6.6) dans $\mathbb{Z}_p/p^{\lambda+d}\mathbb{Z}_p$ soient constantes. Alors sur B l'image $\pmod{p^{\lambda+d}}$ de $v(C_j(x,t))$ est constante, et si $C(a,t) := \prod_j C_j(a,t)$, l'image de $C(a,t)$ dans $\mathbb{Z}_p/p^{\lambda+d}\mathbb{Z}_p$ est constante aussi, disons $C(a,t) \equiv g$. Notons que $0 \leqslant v(g) \leqslant d$, car d'après la définition des C_j,

$$v(g) = v(C(a,t)) = \sum_j v(C_j(a,t)) = \sum_{j\in J} v(\alpha_{i(j)}).$$

D'après le théorème 5.1.1, vu que $v(C(a,t)/g - 1) \geqslant \lambda > 2v(n)$ on a $\mathrm{P}_n(C(a,t)/g)$.

Proposition 6.4.2. *L'ensemble B est bien de la forme (6.1), avec $h(x) = ga_d(x)\prod_{j\in J} b_{i(j),j}(x)$, et $u(x,t)$ la seule racine de $g^{-1}C(x,t)$ congrue a 1 $\pmod{p^\lambda}$.*

Démonstration. En résumant, B est l'ensemble des $(x,t) \in \mathbb{Q}_p^{m+1}$ tels que :

1. $x \in C_d$, avec C_d définissable définit par (6.3) ;
2. (x,t) satisfait les conditions données en (6.4), qui sont du type

$$v(t - c_j(x)) \prec_{l,j} v(a_{l,j}(x));$$

3. les images des fonctions en (6.5) et (6.6) dans $\mathbb{Z}_p/p^{\lambda+d}\mathbb{Z}_p$ sont constantes.

Montrons que l'on peut exprimer la condition 3. par

$$v(t - d_j(x)) \prec_{l,j} v(p_{l,j}(x))$$

avec d_j, $p_{l,j}$ définissables sur $\mathbb{Q}_p^m$. Si $n \in \mathbb{N}$, $j \in I$ on a

$$v\left(\frac{b_{i,j}(a)}{t - b_{1,j}(a)} - n\right) \geqslant \lambda + d$$

si et seulement si

$$v\left(t - b_{1,j}(a) - \frac{b_{i,j}(a)}{n}\right) \geqslant \lambda + d + v(t - b_{1,j}(a)) - v(n).$$

De plus,comme $v(n) \leqslant d$, on a

$$v\left(\frac{b_{i,j}(a)}{t - b_{1,j}(a)}\right) = v(n), \tag{6.7}$$

donc la condition voulue est la conjonction de (6.7) et

$$v\left(t - b_{1,j}(a) - \frac{b_{i,j}(a)}{n}\right) \geqslant \lambda + d + v(b_{1,j}(a)) - 2v(n)$$

qui sont bien de la forme voulue. Si $n, m \in \mathbb{N}$, $j \in J$, on a

$$v\left(\frac{t - b_{1,j}(a)}{b_{i(j),j}(a)} - n\right) \geqslant \lambda + d \Leftrightarrow v(t - b_{1,j}(a) - nb_{i(j),j}(a)) \geqslant \lambda + d + v(b_{i(j),j}(a))$$

qui est de la forme voulue, et $v\left(\frac{b_{i,j}(x)}{b_{i(j),j}(x)} - m\right) \geqslant \lambda + d$ est un ensemble définissable dans $\mathbb{Q}_p^m$.

Enfin, sur B on a

$$f(x,t) = u(x,t)^n h(x) \prod_{j \in I} (t - b_{1,j}(t)) \prod_{j \in J} (t - \beta_j(x))^0 \prod_j (t - d_j(x))^0$$

d'où la conclusion. □

□

Théorème 6.4.3. *Soient $f_i(x,t) \in \mathbb{Q}_p[x,t]$, $i = 1, \ldots, r$, t variable, et $n \in \mathbb{N}^{>0}$. Alors il existe une partition finie de $\mathbb{Q}_p^{m+1}$ en sous-ensembles A de la forme*

$$\{(x,t) \in \mathbb{Q}_p^{m+1} |\ x \in C,\ v(a_1(x)) \prec_1 v(t - c(x)) \prec_2 v(a_2(x))\} \tag{6.8}$$

où C est un ensemble définissable dans $\mathbb{Q}_p^m$, $\prec_i \in \{<, \leqslant\}$, $a_i(x)$ et $c(x)$ sont fonctions définissables : $\mathbb{Q}_p^m \to \mathbb{Q}_p$, et pour tout $(x,t) \in A$,$i = 1, \ldots, r$

$$f_i(x,t) = u_i(x,t)^n h_i(x)(t - c(x))^{n_i} \tag{6.9}$$

avec $v(u_i(x,t)) = 0$, $h_i(x)$ et $u_i(x,t)$ définissables, et $n_i \in \mathbb{N}$.

Démonstration. D'après le théorème 6.4.1, on peut partitionner $\mathbb{Q}_p^{m+1}$ en sous-ensembles définissables de la forme (6.1), et tels que la condition (6.2) soit vérifiée pour chaque $f_i(x,t)$. Il y a plusieurs $c_j(x)$ et $a_{j,l}(x)$ qui apparaissent dans ces décompositions, et on veut une seule fonction $c_j(x)$ et au plus deux fonctions $a_{j,l}(x)$. Si on démontre que l'on peut supposer que S n'a qu'un seul élément dans (6.1), on conclut facilement, car si par exemple on a des conditions $\bigwedge_i v(t - c(x)) \leqslant a_i(x)$, il suffit de partitionner $\mathbb{Q}_p^m$ en ensembles définissables $D_i = \{x \in \mathbb{Q}_p^m |\ a_i(x) = \min_j\{a_j(x)\}\}$, et dans D_i la condition ci-dessus est équivalente à $v(t - c(x)) \leqslant a_i(x)$.

Il suffit donc de montrer que si $c_1(x), c_2(x)$ sont fonctions définissables sur $\mathbb{Q}_p^m$, alors il existe une partition de $\mathbb{Q}_p^{m+1}$ en sous-ensembles de la forme (6.1) sur lesquels $t - c_i(x) = u_i(x,t)^n h_i(x)(t - c(x))^{n_i}$, avec u_i, h_i comme dans l'énoncé 6.4.3, $c(x)$ définissable. On peut enlever l'ensemble définissable $D = \{(x,t)|\ c_1(x) = c_2(x)\}$, soit $A = \mathbb{Q}_p^{m+1} \backslash D$. On écrira c_i au lieu de $c_i(x)$ dans la suite. Soit $\lambda = 2v(n) + 1$, on a

$$\frac{p^\lambda (t - c_1)}{c_2 - c_1} = \frac{p^\lambda (t - c_2)}{c_2 - c_1} + p^\lambda. \tag{6.10}$$

A est partitionné par les 4 sous-ensembles suivants (qui sont définissables et de la forme voulue) :

1. $A_1 = \left\{(x,t)|\ v\left(\frac{t-c_1}{c_2-c_1}\right) \geqslant \lambda\right\}$
   Alors $\mathrm{P}_n\left(\frac{(t-c_1)-(c_2-c_1)}{c_2-c_1}\right)$ et $t - c_2 = t - c_1 - (c_2 - c_1) = -(c_2 - c_1)u(x,t)^n$ avec $v(u(x,t)) = 0$;
2. $A_2 = \left\{(x,t)|\ v\left(\frac{t-c_1}{c_2-c_1}\right) < -\lambda\right\}$
   Alors $t - c_2 = t - c_1 - (c_2 - c_1) = (t - c_1)u(x,t)^n$, avec $v(u(x,t)) = 0$;
3. $A_3 = \left\{(x,t)|\ v\left(\frac{(t-c_2)}{(c_2-c_1)}\right) \geqslant \lambda\right\}$
   Comme dans le cas 1., on obtient que $t - c_1 = (c_2 - c_1)u(x,t)^n$, avec $v(u(x,t)) = 0$.
4. $A_{4,e} = \left\{(x,t)|\ v\left(p^\lambda \frac{t-c_2}{c_2-c_1} - e\right) \geqslant 3\lambda\right\}$ où $0 \leqslant e < p^{3\lambda}$, $e \not\equiv 0 \pmod{p^{2\lambda}}$, $e \not\equiv -p^\lambda \pmod{p^{2\lambda}}$
   D'après (6.10) on a que
   $$v\left(p^\lambda \frac{t - c_1}{c_2 - c_1} - (e + p^\lambda)\right) = v\left(p^\lambda \frac{t - c_2}{c_2 - c_1} - e\right) \geqslant 3\lambda$$
   et $v(e + p^\lambda) \leqslant 2\lambda$, donc en appliquant le théorème 5.1.1 $p^\lambda \frac{t-c_1}{c_2-c_1} = (e + p^\lambda)u_1(x,t)^n$ avec $v(u(x,t)) = 0$ définissable, donc
   $$t - c_1(x) = p^{-\lambda}(c_2(x) - c_1(x))(e + p^\lambda)u_1(x,t)^n.$$
   De même,
   $$0 \leqslant v\left(p^\lambda \frac{t - c_2}{c_2 - c_1}\right) < 2\lambda \text{ et } v\left(p^\lambda \frac{t - c_2}{c_2 - c_1} - e\right) \geqslant 3\lambda$$
   donc
   $$p^\lambda \frac{t - c_2(x)}{c_2(x) - c_1(x)} = e u_2(x,t)^n$$
   pour un $u_2(x,t)$ définissable et tel que $v(u_2(x,t)) = 0$.

Il suffit maintenant de remarquer que

$$A_1, A_2, A_3, \{A_{4,e}|\ 0 \leqslant e < 3\lambda,\ e \not\equiv 0 - p^\lambda \pmod{p^{3\lambda}}\}$$

est une partition de A, ce qui est trivial. □

Chapitre 7

Théorème de rationalité abstrait

7.1 Puissances n-ièmes dans $\mathbb{Q}_p$

On a vu à de nombreuses reprises l'importance des puissances n-ièmes dans la théorie des modèles des p-adiques. Il est donc intéressant de bien connaître l'ensemble des x tel que $P_n(x)$.

On utilisera en particulier le théorème suivant :

Corollaire 7.1.1. *$\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n}$ est fini et a un système de représentants $\subset \mathbb{Z}$.*

Démonstration. n divisant la valuation de toute puissance n-ième, il suffit de vérifier que $U = Z_p^{times}/\mathbb{Z}_p^{times^n}$ est fini et admet un système de représentants dans $\mathbb{Z}$: si $\tilde{M}$ est un tel système, $M = \{p^i m \mid i \in [\![0; n-1]\!],\ m \in \tilde{M}\}$ est un système de représentant de $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n}$. Avec $N = 2v(n)+1$, montrons que $U = \{\overline{k} \mid k \in [\![0; p^N-1]\!] : p \nmid k\}$, ce qui concluera.

Soit $x \in \mathbb{Z}_p^{times}$. Posons k le reste de x modulo p^N. Donc, par construction, $\exists a \in \mathbb{Z}_p : x = k(1+ap^N)$, d'où $\overline{x} = \overline{k}$ par le lemme 5.1.1, ce qui conclut. □

On démontre finalement un lemme technique utile dans la preuve du théorème de rationalité :

Lemme 7.1.2. $\mu(\{a|\ v(a) = 0 \wedge \mathrm{P}_n(a)\}) = \frac{p-1}{p[\mathbb{Z}_p^\times : \mathbb{Z}_p^{\times n}]} \in \mathbb{Q}$.

Démonstration. Considérons $\tilde{M}$ comme dans la démonstration précédente.

$\mathbb{Z}_p^\times$ est l'union distincte des ensembles de la forme $m(\mathbb{Z}_p^{\times n})$ pour $m \in \tilde{M}$.

Or, $\forall m \in \mathbb{Z} - p\mathbb{Z},\ \mu(m(\mathbb{Z}_p^{\times n})) = p^{-v(m)}\mu(\{a|\ v(a) = 0 \wedge \mathrm{P}_n(a)\})$, d'où $\mu(\mathbb{Z}_p^\times) = \sharp\tilde{M}\mu(\{a|\ v(a) = 0 \wedge \mathrm{P}_n(a)\})$.

Or, en écrivant $\mathbb{Z}_p\backslash\{0\}$ comme l'union disjointe des $p^i\mathbb{Z}_p^\times$,

$$1 = \mu(\mathbb{Z}_p\backslash\{0\}) = \sum_{i=0}^{\infty} \mu(p^i\mathbb{Z}_p^\times) = \sum_{i=0}^{\infty} p^{-i}\mu(\mathbb{Z}_p^\times) = \frac{p\mu(\mathbb{Z}_p^\times)}{p-1}$$

D'où la conclusion. □

7.2 Forme des ensembles définissables de $\mathbb{Q}_p^n$

Une dernière condition pour pouvoir facilement intégrer est de bien connaître les formules définissant les ensembles définissables.

Lemme 7.2.1. $\begin{cases} \mathbb{Q}_2 \models \forall x \forall y,\ x \operatorname{div} y \leftrightarrow (x = 0 \wedge y = 0) \vee \mathrm{P}_3(x^3 + 2y^3) \\ \mathbb{Q}_p \models \forall x \forall y,\ x \operatorname{div} y \leftrightarrow (x = 0 \wedge y = 0) \vee \mathrm{P}_2(x^2 + py^2) \text{ pour } p > 2 \end{cases}$
De plus, ces disjonctions sont exclusives.

Démonstration. On suppose $p > 2$, le cas $p = 2$ étant en tout point analogue.

Si $x = 0$, alors $x \operatorname{div} y \Leftrightarrow y = 0$ et $\mathrm{P}_2(x^2 + py^2)$ n'est jamais vérifié (car $\neg\, \mathrm{P}_2(p)$).

Si $x \neq 0$, alors la première condition n'est jamais vérifiée. De plus, en divisant par x^2, on peut supposer $x = 1$.

Si $v(y) < 0$, $v(py^2) = 1 + 2v(y) < 0$ d'où

$$v(1 + py^2) = v(py^2) = 1 + 2v(y) \equiv 1 \mod 2,$$

d'où $\neg\, \mathrm{P}_2(1 + py^2)$.

Par contre, si $v(y) > 0$, $X^2 - 1 - py^2$ est un relèvement dans $\mathbb{Z}_p[X]$ de $X^2 - 1 \in \mathbb{F}_p[X]$, polynôme séparable admettant une racine non nulle. Il suffit donc d'utiliser l'hensélianité de $\mathbb{Q}_p$ pour montrer $\mathrm{P}_2(1 + py^2)$.

D'où la conclusion. □

Lemme 7.2.2. *Un ensemble définissable D de $\mathbb{Q}_p^m$ est défini par une disjonction* exclusive *de formules de la forme*

$$\overline{x} \in C \wedge \bigwedge_i \mathrm{P}_{n_i}(f_i(\overline{x}, t)) \wedge \bigwedge_j g_j(\overline{x}, t) = 0$$

avec C définissable, n_i des entiers et f_i, g_j des polynômes de $\mathbb{Q}_p[X]$.

Démonstration. pCF éliminant les quantificateurs, la formule $\phi(\overline{x}, t)$ définissant D est équivalente à une combinaison booléenne de formules atomiques et de leurs négations. Ces formules atomiques sont de la forme $P_n(t_1(\overline{x}, t))$, $t_1(\overline{x}, t) \operatorname{div} t_2(\overline{x}, t)$ et $t_1(\overline{x}, t) = t_2(\overline{x}, t)$. Concrètement, les termes sont des polynômes et on peut écrire les formules égalitaires sous la forme $t_1(\overline{x}, t) = 0$.

On peut écrire cette combinaison booléenne comme disjonction de conjonctions de formules atomiques et de leurs négations, puis comme disjonction

exclusive de conjonctions de formules atomiques et de de leur négations : si $\phi \leftrightarrow \bigvee_{i\in I} \bigwedge_{j\in J_i} \phi_{ij}$, on écrit $\phi \leftrightarrow \bigvee_{\varepsilon\in\{0;1\}^I} \bigwedge_{i\in I, j\in J_i} \neg_{\varepsilon(i)}\phi_{ij}$ où $\neg_0$ est vide et $\neg_1 = \neg$.

On fait disparaître les formules du type $t_1(\overline{x}, t) \operatorname{div} t_2(\overline{x}, t)$ en utilisant le lemme 7.2.1.

Notons pour $n \in \mathbb{N}$ M_n un système de représentants de $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n}$ qui contient 1.

Alors, on fait disparaître les négations des formules égalitaires en utilisant la relation $u \neq 0 \leftrightarrow \bigvee_{m\in M_n} \mathrm{P}_n(mu)$.

Enfin, on fait disparaître les relations de la forme $\neg\, \mathrm{P}_n(t_1(\overline{x}, t))$ en utilisant la relation $\neg\, \mathrm{P}_n(u) \leftrightarrow (u = 0 \vee \bigvee_{m\in M_n\setminus\{1\}} \mathrm{P}_n(mu))$.

On remarque que, dans ces trois cas, ça reste une disjonction exclusive de conjonction puisque $\bigvee_{m\in M_n} \mathrm{P}_n(mu)$, $(u = 0 \vee \bigvee_{m\in M_n\setminus\{1\}} \mathrm{P}_n(mu))$ et les disjonctions du lemme 7.2.1 sont des disjonctions exclusives.

Ainsi, en isolant les termes ne contenant pas t, on a montré que ϕ était équivalente à une disjonction exclusive de formules de la forme

$$\overline{x} \in C \bigwedge_i \mathrm{P}_{n_i}(f_i(\overline{x}, t)) \wedge \bigwedge_j g_j(\overline{x}, t) = 0.$$

□

7.3 Théorème de rationalité abstrait

On en vient maintenant à l'application principale du théorème de décomposition cellulaire, le théorème de rationalité abstraite, dont le théorème 6.3.1 sur la rationalité des séries de Poincaré est une application relativement directe.

Théorème (6.3.3)**.** *Soit $S \subset \mathbb{Q}_p^m$ définissable contenu dans un compact, e un entier strictement positif et $g : S \to \mathbb{Q}_p$ une fonction définissable à valuation dans $e\mathbb{Z} \cup \{\infty\}$ telle que $|g|$ soit bornée.*

On pose pour tout $s > 0$

$$Z(s) = \int_S |g(x)|^{s/e} |\mathrm{d}x|.$$

Alors, Z est une fonction rationnelle en p^{-s} :

$$\exists\, Q \in \mathbb{Q}(t) \ : \ \forall s > 0,\ Z(s) = Q(p^{-s}).$$

Démonstration. Soit S, e et g vérifiant les conditions du théorème.

Nous allons éliminer les variables de l'intégrale une à une par induction, en commençant par la dernière. Les éléments de $\mathbb{Q}_p^m$ seront donc généralement notés (x, t) avec $x \in \mathbb{Q}_p^{m-1}$ et $t \in \mathbb{Q}_p$.

Afin de construire proprement l'induction, nous oublierons pour l'instant la condition $v(g(S)) \subset e\mathbb{Z} \cup \{\infty\}$ qui ne se transmet pas inductivement.

En utilisant le théorème 6.1.5, S se partitionne en un nombre fini de sous-ensembles définissables où la valuation de g est égale (à un facteur $\frac{1}{n}$ près) à celle d'une fonction rationnelle. On se place sur un de ces sous-ensembles définissables $\tilde{S}$ où l'on peut, quitte à remplacer e par $e' = ne$, supposer $g = g_1/g_2$ avec g_1 et g_2 des polynômes.

De plus, le lemme 7.2.2 nous assure que $\tilde{S}$ peut être partitionné en un nombre fini de sous-ensembles définissables T définis par une formule de la forme $(x \in C) \wedge \left(\bigwedge \tilde{f}_i(x,t) = 0\right) \wedge (\bigwedge \mathrm{P}_n(f_i(x,t)))$ avec n entier, C définissable et f_i, $\tilde{f}_i$ des polynômes. A un $a \in \mathbb{Q}_p^{m-1}$ fixé, si $\tilde{f}_i(a,\cdot) \neq 0$, l'ensemble des éléments de D commençant par a sera de mesure nulle, donc on peut simplement supposer que T est défini par $(x \in C) \wedge (\bigwedge \mathrm{P}_n(f_i(x,t)))$.

Appliquons le théorème 6.4.3 aux polynômes f_i ? g_1, g_2 avec n le produit des n_i.

On partitionne T en un nombre fini de sous-ensembles de la forme $T \cap A$ où $A = \{(x,t) \in \mathbb{Q}_p^m \mid x \in B \wedge (v(a_1(x)) \prec_1 v(t-c(x)) \prec_2 v(a_2(x)))\}$ avec B un sous-ensemble définissable de $\mathbb{Q}_p^{m-1}$, a_1, a_2 et c des fonctions définissables, $\prec_1$, $\prec_2$ des relations de $\{<, \leqslant\}$, avec $f_i(x,t) = h_i(x)u_i(x,t)^n(t-c(x))^{e_i}$ pour tout i et $g_i(x,t) = h_i'(x)u_i'(x,t)^n(t-c(x))^{e_i'}$ pour $i = 1,2$ pour des entiers e_i et e_i', des fonctions définissables h_i, h_i', u_i et u_i' avec les u_i, u_i' de valuation nulle. En particulier, on aura $|g(x,t)|^{1/e} = |g_0(x)|^{1/e'}|t-c(x)|^{\nu/e'}$ avec g_0 définissable et $\nu \in \mathbb{Z}$.

Quitte à mettre de côté l'ensemble des zéros de f_i, de mesure nulle, on suppose que les f_i ne s'annulent pas sur A. Donc sur A, $\mathrm{P}_n(f_i(x,t))$ est équivalent à $\mathrm{P}_n(h_i(x)(t-c(x))^{e_i})$.

Comme $G = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n}$ est fini, on peut partitionner $T \cap A$ en de plus petits sous-ensembles U où les fonctions h_i et $(t-c(x))$ vues comme à valeur dans G sont constantes.

A fortiori, ces fonctions seront constantes sur les sous-ensembles U en les considérant comme à valeur dans $G_i = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n_i} < G$.

On sait que

$$\mathrm{P}_{n_i}(h_i(x)(t-c(x))^{e_i}) \iff \bigvee_{\overline{k} \in G_i} \left(\mathrm{P}_{n_i}(k^{-1}(t-c(x))) \wedge \mathrm{P}_{n_i}(k^{e_i}h_i(x))\right),$$

la disjonction étant exclusive. Pour chaque i, on trouve donc une unique classe $\alpha_i = \overline{k}$ de G_i satisfaisante, correspondant aux k tels que $\mathrm{P}_{n_i}(k^{-1}(t-c(x)))$.

Or, en considérant $M \subset \mathbb{Z}$ un système de représentants entiers de G, on sait que $\bigwedge_{k \in M} \mathrm{P}_n(k^{-1}(t-c(x)))$, donc on trouve $k \in M$ tel que $\mathrm{P}_n(k^{-1}(t-c(x)))$. En particulier, pour chaque i, $\mathrm{P}_{n_i}(k^{-1}(t-c(x)))$, d'où, dans G_i, $\alpha_i = \overline{k}$, donc la condition $\bigwedge \mathrm{P}_{n_i}(k^{-1}(t-c(x)))$ s'écrit simplement $\mathrm{P}_n(k^{-1}(t-c(x)))$.

Ainsi, les ensembles U de la partition seront définis par des formules de

la forme

$$\bigwedge_i \mathrm{P}_{n_i}(k^{e_i}h_i(x)) \wedge (x,t) \in S \cap A \wedge \mathrm{P}_n(k^{-1}(t-c(x)))$$

pour un certain entier $k \in M$, i.e. :

$$U = \{(x,t) \mid x \in D, (v(a_1(x)) \prec_1 v(t-c(x)) \prec_2 v(a_2(x))), \mathrm{P}_n(k^{-1}(t-c(x)))\}$$

avec k un entier et D définissable.

On peut donc écrire, en notant $[x] = \{\ell \in \mathbb{Z} |\ v(a_1(x)) \prec_1 \ell \prec_2 v(a_2(x))\}$:

$$\begin{aligned}
\int_U |g(x,t)|^{s/e}|\mathrm{d}x||\mathrm{d}t| &= \int_D \left(|g_0(x)|^{s/e'} \int_{\{t|(x,t)\in U\}} |t-c(x)|^{s\nu/e'}|\mathrm{d}t| \right)|\mathrm{d}x| \\
&= \int_D \left(|g_0(x)|^{s/e'} \sum_{\ell\in[x]} p^{-\frac{\ell s\nu}{e'}} \int_{\substack{v(t-c(x))=\ell \\ \mathrm{P}_n(k^{-1}(t-c(x)))}} |\mathrm{d}t| \right)|\mathrm{d}x| \\
&= \int_D \left(|g_0(x)|^{s/e'} \sum_{\ell\in[x]} p^{-\frac{\ell s\nu}{e'}} p^{-\ell} \int_{\substack{v(u)=0 \\ \mathrm{P}_n(k^{-1}p^{\ell}u)}} |\mathrm{d}u| \right)|\mathrm{d}x|
\end{aligned}$$

en faisant le changement de variable $u = p^{-\ell}(t-c(x))$.

La petite intégrale est non-nulle si et seulement si $\ell \equiv v(k) \mod n$, auquel cas elle vaut $\lambda := \mu(\{a|\ v(a) = 0 \wedge \mathrm{P}_n(a)\}) \in \mathbb{Q}$ (lemme 7.1.2).

On en déduit, en notant $I(\ell) = \{x \in D|\ v(a_1(x)) \prec_1 \ell \prec_2 v(a_2(x))\}$:

$$\begin{aligned}
\int_U |g(x,t)|^{s/e}|\mathrm{d}x||\mathrm{d}t| &= \lambda \int_D \left(|g_0(x)|^{s/e'} \sum_{\substack{\ell\in[x] \\ \ell\equiv v(k) \mod n}} p^{-\frac{\ell s\nu}{e'}} p^{-\ell} \right)|\mathrm{d}x| \\
&= \lambda \sum_{\ell\equiv v(k) \mod n} \left(p^{-\frac{\ell s\nu}{e'}-\ell} \int_{I(\ell)} |g_0(x)|^{s/e'}|\mathrm{d}x| \right).
\end{aligned}$$

On itère ce processus, en se concentrant sur l'ensemble définissable $I(\ell)$ et la fonction définissable g_0 à qui on applique également le lemme 7.2.2, le théorème 6.4.3 et le raisonnement précédent pour éliminer la variable x_{m-1} de l'intégrale et ainsi de suite jusqu'à obtenir une intégrale sur le vide.

Finalement, en sommant sur toutes les partitions de toutes les étapes de cette itération, on obtient que l'intégrale d'origine $Z(s) = \int_S |g(x)|^{\frac{s}{e}} |\mathrm{d}x|$ s'écrit comme $\mathbb{Q}$-combinaison linéaire de séries convergentes de la forme

$$\sum_{\substack{(\ell_1,\dots,\ell_m)\in\Lambda \\ l_i\equiv\nu_i \mod n_i}} p^{(-q_1\ell_1-\cdots-q_m\ell_m)s-\ell_1-\cdots-\ell_m}$$

pour des rationnels q_i, des entiers ν_i, des entiers naturels n_i et Λ l'espace des solutions d'un système d'inégalités linéaires à coefficients entiers. (La convergence vient du caractère borné de g et de la finitude de $\mu(S)$.)

En écrivant les ℓ_i comme $\nu_i + \lambda_i n_i$ et en notant d le dénominateur commun des q_i de tous les termes de Z, le lemme B.0.9 appliqué à chacune des séries nous assure que Z est une fonction rationnelle en $p^{-s/d}$:

$$\exists Q \in \mathbb{Q}(t) \ : \ \forall s > 0, \ Z(s) = Q(p^{-s/d}).$$

Or, en sommant dans la définition de Z selon les différentes valeurs de $v(g(x))$, on a immédiatement $Z(s) = \sum_{k\in\mathbb{Z}} p^{-\frac{ks}{e}} \mu(g^{-1}(v^{-1}(k)))$.

$|g|$ étant supposée bornée, il n'y a qu'un nombre fini de coefficients non nuls. De plus, comme $v(g(S)) \subset e\mathbb{Z} \cup \{\infty\}$, les termes correspondant aux k non multiples de e sont nuls. Donc Z est une série de Laurent en p^{-s} :

$$\exists P \in \mathbb{R}((t)) \ : \ \forall s > 0, \ Z(s) = P(p^{-s}).$$

Notons $R = Q(t^{1/d}) \in \mathbb{Q}(t^{1/d})$. Alors, en considérant P et R comme des éléments de $\mathbb{R}((t^{1/d}))$, on a :

$$\forall s > 0, \ P(p^{-s}) = Z(s) = R(p^{-s}).$$

Donc $P = R \in Q(t^{1/d}) \cap \mathbb{R}((t)) = \mathbb{Q}(t)$, d'où la conclusion.

□

Annexe A

Extensions finies de $\mathbb{Q}_p$

Dans cette partie, on se fixe une clôture algébrique $\overline{\mathbb{Q}_p}$ fixée de $\mathbb{Q}_p$. D'après le point 2. du théorème 3.4.3, v_p s'étend canoniquement à $\overline{\mathbb{Q}_p}$.

On cherche à démontrer le théorème suivant :

Théorème A.0.1. *$\mathbb{Q}_p$ a un nombre fini d'extensions de degré fini fixé.*

Nous étudierons d'abord la partie résiduelle, fixe, de ces extensions avant de traiter topologiquement leur partie ramifiée.

Pour f un entier, nous noterons $\overline{\zeta_f}$ un élément générateur de $\mathbb{F}_{p^f}$, $\overline{P_f}$ son polynôme minimal sur $\mathbb{F}_p$, P_f un relèvement unitaire de $\overline{P_f}$ sur $\mathbb{Z}_p[X]$, ζ_f la racine de P sur $\overline{\mathbb{Q}_p}$ avec $\operatorname{res}\zeta_f = \overline{\zeta_f}$ (en utilisant l'hensélianité et $K_f^{\text{un}} = \mathbb{Q}_p[\zeta_f]$.

On remarque immédiatement que P_f est irréductible : si il est produit de deux polynômes unitaires non triviaux a et b, alors on sait $a, b \in \mathbb{Z}_p[X]$ (sinon, avec i et j minimaux pour a_i et b_j de valuation minimale, on a $v((P_f)_{i+j}) = v(a_i) + v(b_j) < 0$), d'où $\overline{P_f} = \operatorname{res}(a)\operatorname{res}(b)$ et la contradiction.

Lemme A.0.2. *K_f^{un} est une extension totalement résiduelle de degré f de $\mathbb{Q}_p$.*

Démonstration. Comme $\overline{P_f}$ est irréductible et $\overline{\zeta_f}$ générateur,

$$\deg(P_f) = \deg(\overline{P_f}) = [\mathbb{F}_p[\overline{\zeta_f}] : \mathbb{F}_p] = [\mathbb{F}_{p^f} : \mathbb{F}_p] = f,$$

d'où, P_f étant irréductible, $[K_f^{\text{un}} : \mathbb{Q}_p] = f$.

Or, $\operatorname{res}(\zeta_f)$ étant de polynôme minimal $\overline{P_f}$ et engendrant donc $\mathbb{F}_{p^f}$, $\kappa_{K_f^{\text{un}}} = \mathbb{F}_{p^f}$ et K_f^{un} est de degré d'inertie f. Il est donc totalement résiduel. □

Lemme A.0.3. *Toute extension de $\mathbb{Q}_p$ de degré d et de degré d'inerte f est une extension totalement ramifiée de K_f^{un}.*

Démonstration. Soit K une telle extension. $\kappa_K = \mathbb{F}_{p^f}$. K étant hensélien et P_f s'annulant en $\overline{\zeta_f}$, P admet une racine de résidu $\overline{\zeta_f}$. En utilisant dans $\overline{\mathbb{Q}_p}$ l'unicité dans le lemme de Hensel, cette racine est ζ_f. Donc d'après l'existence dans le lemme précédent, K est une extension totalement ramifiée de $\mathbb{Q}_p[\zeta_f] = K_f^{\text{un}}$. □

Remarque A.0.4. Le théorème 3.6.7 montre alors que K_f^{un} est en fait l'unique extension totalement résiduelle de degré f de $\mathbb{Q}_p$.

Il suffira donc de montrer que pour toute extension finie totalement résiduelle K de $\mathbb{Q}_p$ et tout entier e fixé, il y a un nombre fini d'extensions totalement ramifiées de degré e de K.

L'outil principal sera le lemme de Krasner.

Lemme A.0.5. *Soit (K, v) un corps valué hensélien, α et β deux éléments de sa clôture algébrique avec α séparable sur $K(\beta)$ tels que*

$$\forall \sigma \in \mathrm{Gal}(K[\alpha]/K)\backslash\{id\}, \quad v(\beta - \alpha) > v(\sigma\alpha - \alpha).$$

Alors $K(\alpha) \subset K(\beta)$.

Démonstration. Soit $\tau \in \mathrm{Gal}(L/K[\beta])$ avec L la clôture normale de $K[\alpha, \beta]/K[\beta]$.

D'après le point 2. du théorème 3.4.3, on sait que $v \circ \tau = v$, d'où

$$\forall \sigma \in \mathrm{Gal}(K[\alpha]/K)\backslash\{id\}, \ v(\beta - \tau\alpha) = v(\beta - \alpha) > v(\sigma\alpha - \alpha).$$

En sommant, on en déduit $v(\tau\alpha - \alpha) > v(\sigma\alpha - \alpha) \ \ \forall \sigma \in \mathrm{Gal}(K[\alpha]/K)$.

D'où $\tau(\alpha) = \alpha$ et la conclusion. □

Deux polynômes engendrant des racines proches engendreront donc les mêmes extensions. Il s'impose alors de vérifier que les racines dépendent continûment des polynômes.

Dans un corps normé, on définit la norme d'un polynôme comme le maximum de la norme de ses coefficients.

Lemme A.0.6. *Soit $(K, |\cdot|)$ algébriquement clos et $P \in K[X]$ de degré d.*

Pour tout $\epsilon > 0$ il existe $\delta > 0$ tel que si $Q \in K[X]$ de degré d vérifie $|P - Q| < \delta$, alors chaque racine de Q est à distance $< \varepsilon$ d'une racine de P et réciproquement.

Démonstration. Soit $P = p_0 + \cdots + p_d X^d = p_d \cdot (X - x_1) \cdots (X - x_d)$ et $\varepsilon > 0$. On pose :

$$A := \sum_{i=0}^{d-1} \left(1 + 2\frac{|p_i|}{|p_d|}\right).$$

$$B := \max\left(1, \sum_{i=0}^{d-1} \frac{|p_i|}{|p_d|}\right).$$

$$\delta < \min\left(\frac{|p_d|}{2}, \frac{\varepsilon^d|p_d|}{\sum_{i=0}^d A^i}, \frac{\varepsilon^d|p_d|}{2\sum_{i=0}^d B^i}, \right).$$

Soit $Q = q_0 + \cdots + q_d X^d$ de degré d vérifiant $|P-Q| < \delta$ et z une racine de Q.

En distinguant selon le signe de $|z|-1$, $|z| \leqslant \max\left(1, \sum_{i=0}^{d-1} \frac{|q_i|}{|q_d|}\right)$. Or

$$\forall i,\ \frac{|q_i|}{|q_d|} \leqslant 2\frac{|q_i|}{|p_d|} \leqslant 2\frac{|p_i| + \frac{|p_d|}{2}}{|p_d|} = 1 + 2\frac{|p_i|}{|p_d|}.$$

Donc $|z| \leqslant A$, d'où on déduit :

$$|P(z)| = |P(z) - Q(z)| \leqslant \sum_{i=0}^{d} |p_i - q_i||z|^i < \delta \sum_{i=0}^{d} A^i < |p_d|\varepsilon^d.$$

Ainsi, $|p_d||(X-x_1)|\cdots|(X-x_d)| < |p_d|\varepsilon^d$, d'où la présence de z à distance $< \varepsilon$ d'une racine de P.

De même, en considérant x une racine de P, $|x| \leqslant B$, d'où

$$|Q(x)| < \delta \sum_{i=0}^{d} B^i < \frac{|p_d|\varepsilon^d}{2} < |q_d|\varepsilon^d$$

et on conclut pareillement que x est à distance $< \varepsilon$ d'une racine de Q. □

Ces résultats généraux étant établis, il suffit maintenant d'étudier l'espace des polynômes irréductibles engendrant des extensions totalement ramifiées sur une extension totalement résiduelle K donnée de $\mathbb{Q}_p$.

Lemme A.0.7. *Soit L une extension totalement ramifiée de degré e d'un tel corps. Alors, L est engendrée au-dessus de K par une racine d'un polynôme d'Eisenstein $X^e + a_{e-1}X^{e-1} + \cdots + a_0$ avec $v(a_i) > 0$ pour tout i et $v(a_0) = 1$.*

Démonstration. Soit $\pi \in L$ tel que $ev(\pi) = 1$. Comme L est une extension immédiate du corps hensélien $K[\pi]$, le théorème 3.6.7 assure que π engendre K. Or, en utilisant le point 2. du théorème 3.4.3, on s'aperçoit que les conjugués de π sur K^{alg}/K ont même valuation que π, donc le polynôme minimal Π de π, de degré e, est à coefficients (non dominants) de valuation strictement positive. De plus, la valuation du coefficient est la somme des valuations des racines de Π, i.e. 1. Π est donc un polynôme d'Eisenstein. □

Remarque A.0.8. Les polynômes d'Eisenstein sont irréductibles.

La réciproque du lemme précédent se démontre alors de la même façon.

On déduit immédiatement des lemmes A.0.5 et A.0.6 que, à e fixé, dans une extension totalement résiduelle K de $\mathbb{Q}_p$, tout polynôme P irréductible de degré e admet un voisinage dans lequel les racines de chaque polynôme de degré e engendrent exactement les mêmes extensions de K que P.

Or, d'après le lemme A.0.7, les extensions totalement ramifiées de degré e de K sont engendrées par les racines des polynômes d'Eisenstein de degré e, c'est-à-dire d'un point de $\mathcal{M}_K \times \cdots \times \mathcal{M}_K \times v^{-1}(1)$: à un point de cet ensemble correspond un polynôme auquel correspond un nombre fini d'extensions totalement ramifiées, qui restent les mêmes dans un voisinage de ce point.

Or, cet ensemble est compact (en décomposant en base p, on voit que $\mathcal{O}_K$ est compact, or $\mathcal{M}_K \cong \mathcal{O}_K$, dont $v^{-1}(1)$ est un fermé), donc en considérant un sous-recouvrement fini de ces voisinages, le nombre d'extensions totalement ramifiées de K est fini. D'où la conclusion.

Annexe B

Rationnalité des séries convergentes

Dans cette partie, un "espace de solutions" sera un sous-ensemble de $\mathbb{Z}^n$ défini par un système fini d'inéquations linéaires à coefficients entiers (c'est-à-dire de la forme $\sum_{i=1}^n \alpha_i k_i \geqslant \beta$ avec les α_i et β entiers).

Lemme B.0.9. *Soit Λ un espace de solutions de $\mathbb{Z}^n$, p un entier > 1 et $A_1, \dots A_n$ des polynômes à coefficients entiers de degré $\leqslant 1$.*

Soit J la série suivante, supposée convergente sur un ouvert U de $\mathbb{R}$:

$$J(s) = \sum_{(k_1,\dots,k_n)\in\Lambda} p^{-\sum_{i=1}^n k_i A_i(s)}.$$

Alors, J est une fonction rationnelle en p^{-s} sur cet ouvert U :

$$\exists Q \in \mathbb{Q}(t) \ : \ \forall s \in U, \ J(s) = Q(p^{-s}).$$

Démonstration. On raisonne par récurrence sur n. $n = 0$ est clair.

Quitte à partitionner Λ en un nombre fini de sous-espaces de solution (correspondant au rajout des inéquations $k_i \gtreqless 0$), on peut supposer que $(k_1, ..., k_n) \in \Lambda$ implique $k_1, ..., k_n \geqslant 0$. On suppose de plus que $A_n \neq 0$.

Dans le système, après d'éventuelles multiplications avec les constantes idoines pour fixer λ, les inéquations concernant k_n sont de la forme

$$\begin{cases} \lambda k_n \leqslant u_i(k_1, \dots, k_{n-1}) \text{ pour } i = 1, \dots, \ell \\ \lambda k_n \geqslant v_j(k_1, \dots, k_{n-1}) \text{ pour } j = 1, \dots, m \end{cases}$$

avec λ un entier fixé et les u_i, v_j des polynômes affines à coefficients entiers.

On sait que $m \geqslant 1$ et on suppose que $\ell \geqslant 1$, le cas $\ell = 0$ étant analogue.

Pour $(i, j) \in [\![1; \ell]\!] \times [\![1; m]\!]$, on définit le sous-espace de solutions Λ_{ij} de Λ en lui rajoutant les $\ell + m - 2$ inéquations suivantes en $k_1, ..., k_{n-1}$:

$$\begin{cases} u_i(k_1, \dots, k_{n-1}) \leqslant u_\kappa(k_1, \dots, k_{n-1}) \text{ pour chaque } \kappa \in [\![1; \ell]\!] \backslash \{i\} \\ v_j(k_1, \dots, k_{n-1}) \geqslant v_\kappa(k_1, \dots, k_{n-1}) \text{ pour chaque } \kappa \in [\![1; m]\!] \backslash \{j\} \end{cases}$$

Clairement, dans Λ_{ij}, ces inéquations permettent de se restreindre à uniquement deux équations en ce qui concerne k_n :

$$\begin{cases} \lambda k_n \leqslant u_i(k_1, \dots, k_{n-1}) \\ \lambda k_n \geqslant v_j(k_1, \dots, k_{n-1}) \end{cases}$$

Les Λ_{ij} formant une partition finie en sous-espaces de solutions de Λ, cela justifie que l'on puisse supposer $\ell = m = 1$. On note $u = u_1$ et $v = v_1$.

Afin d'enlever λ, on décompose J selon les résidus modulo λ des k_i :

$$J(s) = \sum_{\overline{r} \in [\![0;\lambda-1]\!]^{n-1}} p^{-\sum_{i=1}^{n-1} r_i A_i(s)} \sum_{\substack{(c_1,\dots,c_n)\in\mathbb{Z}^n \\ (\lambda c_1 + r_1, \dots, \lambda c_{n-1} + r_{n-1}, k_n) \in \Lambda}} p^{-\sum_{i=1}^{n-1} \lambda c_i A_i(s) - k_n A_n(s)}$$

La première somme étant finie, la convergence de J est équivalente à celle des

$$\sum_{\substack{(c_1,\dots,c_n)\in\mathbb{Z}^n \\ (\lambda c_1 + r_1, \dots, \lambda c_{n-1} + r_{n-1}, k_n) \in \Lambda}} p^{-\sum_{i=1}^{n-1} \lambda c_i A_i(s) - k_n A_n(s)},$$

or, ces sommes sont de la forme

$$\sum_{(k_1,\dots,k_n)\in\tilde{\Lambda}} p^{-\sum_{i=1}^{n} k_i \tilde{A}_i(s)}.$$

avec $\tilde{\Lambda}$ un espace de solutions de $\mathbb{Z}^n$ et $\tilde{A}_i$ des polynômes à coefficients entiers de degré $\leqslant 1$.

Il suffit en effet de poser $\tilde{A}_n = A_n$ et $\tilde{A}_i = \lambda A_i$ si $i \neq n$ et $\tilde{\Lambda}$ l'espace des solutions où l'on a remplacé les inéquations de la forme $\sum_{i=1}^{n} \alpha_i k_i = \beta$ de Λ par $\sum_{i=1}^{n-1} \lambda\alpha_i k_i + \alpha_n k_n = \beta - \sum_{i=1}^{n-1} \alpha_k r_k$.

Etudions les inéquations définissant $\tilde{\Lambda}$.

Bien sûr, il n'y a toujours que deux équations concernant k_n :

$$\begin{cases} \lambda k_n \leqslant u(\lambda k_1 + r_1, \dots, \lambda k_{n-1} + r_{n-1}) \\ \lambda k_n \geqslant v(\lambda k_1 + r_1, \dots, \lambda k_{n-1} + r_{n-1}) \end{cases}$$

Ces équations s'écrivent pour des α_i, α'_i, β, β' appropriés comme :

$$\begin{cases} \lambda k_n \leqslant \sum_{i=1}^{n-1} \alpha_i \lambda k_i + \beta \\ \lambda k_n \geqslant \sum_{i=1}^{n-1} \alpha'_i \lambda k_i + \beta' \end{cases}$$

Or, ces deux équations sont clairement équivalentes à :

$$\begin{cases} k_n \leqslant \sum_{i=1}^{n-1} \alpha_i k_i + \lfloor \frac{\beta}{\lambda} \rfloor \\ k_n \geqslant \sum_{i=1}^{n-1} \alpha'_i k_i + \lambda \lceil \frac{\beta'}{\lambda} \rceil \end{cases}$$

Cela justifie que l'on puisse supposer $\lambda = 1$.

De plus, l'existence de k_n impliquant $u(k_1,...,k_{n-1}) \geqslant v(k_1,...,k_{n-1})$, on peut supposer que cette inéquation redondante fait partie du système. On pose Λ_{n-1} l'espace de solutions dans $\mathbb{Z}^{n-1}$ du système de toutes les inéquations définissant Λ qui ne concernent pas k_n.

Posons $\tilde{U} = U \backslash A_m^{-1}(0)$. Pour $s \in \tilde{U}$, on a alors :

$$\begin{aligned}
J(s) &= \sum_{(k_1,...,k_n)\in\Lambda} p^{-\sum_{i=1}^{n} k_i A_i(s)} \\
&= \sum_{(k_1,...,k_{n-1})\in\Lambda_{n-1}} p^{-\sum_{i=1}^{n-1} k_i A_i(s)} \sum_{v(k_1,...,k_{n-1})\leqslant k_n \leqslant u(k_1,...,k_{n-1})} p^{-k_n A_n(s)} \\
&= \sum_{(k_1,...,k_{n-1})\in\Lambda_{n-1}} p^{-\sum_{i=1}^{n-1} k_i A_i(s)} \frac{p^{-v(k_1,...,k_{n-1})A_n(s)} - p^{-u(k_1,...,k_{n-1})A_n(s)}}{1-p^{-A_n(s)}} \\
&= \frac{1}{1-p^{-A_n(s)}} \begin{pmatrix} \sum_{(k_1,...,k_{n-1})\in\Lambda_{n-1}} p^{-\sum_{i=1}^{n-1} k_i A_i(s) - v(k_1,...,k_{n-1})A_n(s)} \\ - \\ \sum_{(k_1,...,k_{n-1})\in\Lambda_{n-1}} p^{-\sum_{i=1}^{n-1} k_i A_i(s) - u(k_1,...,k_{n-1})A_n(s)} \end{pmatrix}
\end{aligned}$$

Or, chacune de ces sommes est une sous-somme de celle définissant J (en imposant la condition supplémentaire suffisante $k_n = v(k_1,...,k_{n-1})$ ou $k_n = u(k_1,...,k_{n-1})$) donc converge. Mais ces sommes s'écrivent clairement

$$p^{-\beta s} \sum_{(k_1,...,k_{n-1})\in\Lambda_{n-1}} p^{-\sum_{i=1}^{n-1} k_i \tilde{A}_i(s)}$$

pour des polynômes $\tilde{A}_i$ à coefficents entiers et de degré $\leqslant 1$ appropriés en notant β le coefficient constant de v (resp. u).

L'hypothèse de récurrence permet donc d'affirmer que ce sont des fonctions rationnelles en p^{-s}, d'où J également.

Enfin, on étend à U tout entier par continuité (des fonctions rationnelles et des séries de Laurent) puisque l'on a supposé $A_n \neq 0$. □

On remarque que le cas $\ell = 0$ est effectivement totalement analogue : on se réduit de la même façon à $m = 1$ puis à $\lambda = 1$, puis on observe que la convergence de J implique clairement la positivité de A_n, ce qui permet de conclure de la même façon en utilisant la série

$$\sum_{k_n=v(k_1,...,k_{n-1})}^{\infty} p^{-k_n A_n(s)} = \frac{p^{-v(k_1,...,k_{n-1})A_n(s)}}{1-p^{A_n(s)}}.$$

Bibliographie

[1] Zoé Chatzidakis *Théorie des modèles et corps valués, polycopies du cours.*

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

[3] S.Lang *Algebraic number theory*

[4] S. Lang *Algebra.* Springer Verlag, Graduate Texts in Mathematics

[5] I. Kaplansky *Maximal fields with valuations.* Duke Math. J. Volume 9, Number 2 (1942), 303-321.

[6] A.J.Engler, A.Prestle *Valued fields.* Springer monographs in mathematics