Silvain Rideau
École Normale Supérieure
L.M.F.I., Paris 7

27 avril 2013

Élimination des Imaginaires
dans les
Corps Valués

sous la direction de
Élisabeth Bouscaren
Orsay, Paris 11

Introduction

Le résultat historique qui a fait des corps valués un domaine de prédilection des théoriciens des modèles (et a peut être aussi attiré l'attention des géomètres algébristes sur la théorie des modèles) est le théorème démontré en 1965 par Ax et Kochen (et indépendamment par Ershov) dans [AK65]. Ce théorème énonce qu'en caractéristique résiduelle nulle, la théorie d'un corps valué est totalement déterminée par la théorie du groupe de valeur et du corps résiduel. Ce théorème était motivé par la démonstration d'une conjecture d'Artin sur les racines des polynômes homogènes dans le corps des nombres p-adiques $\mathbb{Q}_p$, dont il a fallu attendre jusqu'il y a quelques années une preuve purement algébrique.
Bien que le théorème d'Ax-Kochen-Ershov ne s'applique qu'en caractéristique résiduelle nulle et qu'il ne soit pas à proprement parler un résultat d'élimination des quantificateurs, il a néanmoins inspiré Macintyre en 1976 (voir [Mac76]) pour démontrer un résultat d'élimination des quantificateurs pour la théorie de $\mathbb{Q}_p$. Une des applications algébriques de ce résultat est l'article [Den84] de Denef en 1984, dans lequel l'auteur démontre (ou redémontre, pour certaines) la rationalité de séries de Poincaré : si (P_i) est une famille finie de polynômes de $\mathbb{Q}_p[X_1, \ldots, X_n]$, on note $a_n := \#\{x \mod p^n : x \in \mathbb{Z}_p^n \wedge \forall i\, P_i(x) \equiv 0 \mod p^n\}$ et $\widetilde{a}_n := \#\{x \mod p^n : x \in \mathbb{Z}_p^n \wedge \forall i\, P_i(x) = 0\}$. Le résultat que Denef démontre est que la série des $\sum_i \widetilde{a}_i T^i$ est rationnelle et sa preuve donne une nouvelle démonstration du fait que $\sum_i a_i T^i$ l'est aussi. La preuve de Denef consiste à remarquer que les coefficients de ces séries sont les mesures de sous-ensembles définissables de $\mathbb{Q}_p$ et comme, par le théorème de Macintyre, on sait exactement comment sont construits ces ensembles, cela nous donne des indications sur leur mesure.
En 1988, Grunewald, Segal et Smith dans [GSS88], ont appliqué ce genre de techniques pour montrer la rationalité de séries de comptage des sous-groupes : si G est un groupe, on note b_n le nombre de sous-groupes d'indice n. Ils ont alors montré que si G est finiment engendré et nilpotent, les b_n sont toujours finis et $\sum_i b_{p^i} T^i$ est rationnelle. Leur preuve procède en deux temps. Tout d'abord, montrer que l'ensemble des sous-groupes de G d'indice une puissance de p est en bijection avec l'ensemble des classes d'équivalences d'une relation d'équivalence définissable E sur un sous-ensemble définissable D de $\mathbb{Q}_p^n$. Et ensuite, trouver une fonction $f : D \to \mathbb{Q}_p$ telle que pour tout $x \in D$, la mesure de la E-classe de x est égale à $\nu_p(f(x))$, où ν_p est la valuation p-adique. Dans ce cas précis, la relation d'équivalence E est assez simple pour qu'on puisse trouver explicitement une telle fonction f, mais cette méthode atteint ses limites si le E devient trop compliquée, en particulier, si, au lieu de compter les sous-groupes d'indice p^n, on veut compter les caractères complexes irréductibles de dimension p^n.

De même que le résultat de Denef sur la rationalité de séries de Poincaré était possible grâce à un résultat d'élimination des quantificateurs qui permettait de savoir qu'il suffisait de rajouter, pour tout n, l'ensemble des puissances n-ièmes comme atomes pour pouvoir construire tous les ensembles définissables par des opérations booléennes ; on voudrait aussi savoir exactement quelles sont les classes de relations d'équivalence définissables dans $\mathbb{Q}_p$ qu'il faut rajouter pour pouvoir toutes les décrire simplement. En d'autres termes et pour reprendre la terminologie modèle théorique introduite par Poizat en 1983 dans [Poi83], on veut montrer un résultat d'élimination des imaginaires pour $\mathbb{Q}_p$.
En 2006, Haskell, Hrushovski et Macpherson dans [HHM06] démontrent l'élimination des imaginaires pour les corps valués algébriquement clos si on rajoute certains quotients de $GL_n(K)$. Deux ans plus tard, Hrushovski et Martin, dans [HM08], utilisent ce résultat pour montrer l'élimination des imaginaires pour $\mathbb{Q}_p$ avec les même sortes additionnelles et en déduisent la rationalités des séries de comptage des représentations des groupes finiment engendrés nilpotents.
Le but de ce mémoire est donc de démontrer le principal résultat de théorie des modèles de [HM08] : l'élimination des imaginaires pour la théorie de $\mathbb{Q}_p$ avec les sortes géométriques et d'en profiter pour démontrer la plupart des résultats préliminaires sur les corps valués algébriquement clos et les corps p-adiquement clos, i.e. les corps dont la théorie est celle de $\mathbb{Q}_p$.
Ce mémoire s'organise en deux parties. Une première, centrée autour des corps algébriquement clos, dans laquelle on introduit les notions de théorie des modèles (dont la notion d'imaginaire) et de théorie des corps valués qui sont nécessaires. On en profitera pour démontrer le résultat de A. Robinson (voir [Rob56]) d'élimination des quantificateurs pour les corps valués algébriquement clos et rappeler le résultat de [HHM06] d'élimination des imaginaires pour cette même théorie. La deuxième partie, quant à elle, contient une étude des corps p-adiquement clos : la clôture algébrique et définissable, les types, les extensions algébriques et pour finir une preuve de l'élimination des imaginaires dans les corps p-adiquement clos.
Profitons en pour fixer quelques notations :
- le langage $\mathcal{L}_A$ est le langage $\mathcal{L}$ augmenté d'une constante par élément de A. Être $\mathcal{L}_A$-définissable revient donc à être $\mathcal{L}$-définissable à paramètres dans A ;
- on notera $c \equiv_A c'$ pour c et c' ont le même type au dessus de A ;
- pour tout ensemble définissable (ou infiniment définissable) X et tout ensemble de paramètres A dans un modèle $\mathcal{M}$, on notera $X(A) := \{x \in A : \mathcal{M} \vDash X(a)\}$.

Enfin je tiens à remercier Élisabeth Bouscaren de m'avoir proposé ce sujet de mémoire et de m'avoir patiemment encadré au cours de ces derniers mois, Luc Belair et Pierre Simon pour leurs discussions éclairantes, tous les professeurs qui m'ont fait découvrir et aimer la théorie des modèles : François Loeser, René Cori, Martin Hils... Ainsi que Pierre-Yves Coudert pour sa grande vigilance orthographique et Catherine Kikuchi pour les synomymes et le thé.

Chapitre 1

Corps valués algébriquement clos

1.1 Langages des corps valués

Définition 1.1 (Corps valué) **:**
Soient K *un corps et* Γ *un groupe abélien totalement ordonné. Une valuation est une application* $v : K \to \Gamma \cup \{\infty\}$ *telle que :*

(i) pour tout $a \in K$, $v(a) = \infty \iff a = 0$ *;*

(ii) pour tous $a, b \in K$, $v(ab) = v(a) + v(b)$ *;*

(iii) pour tous $a, b \in K$, $v(a + b) \geqslant \min(v(a), v(b))$ *;*

(iv) pour tout $\gamma \in \Gamma$, $\gamma < \infty$ *et* $\gamma + \infty = \infty + \gamma = \infty$.

Une autre notion utile est celle d'anneau de valuation mais ces deux notion sont en fait identiques.

Définition 1.2 (Anneau de valuation) **:**
Un anneau intègre $\mathcal{O}$ *de corps de fractions* K *est dit de valuation si pour tout* $x \in K$, x *ou* x^{-1} *est dans* $\mathcal{O}$.

Remarque 1.3 :

(i) Soient (K, v) *un corps valué et* $\mathcal{O}_v = \{a \in k : v(a) \geqslant 0\}$, *alors* $\mathcal{O}_v$ *est un anneau de valuation.*
D'autre part, soit $\mathcal{O}$ *un anneau de valuation et* K *son corps de fraction, alors* K *peut être muni d'une valuation telle que* $\mathcal{O}$ *soit son anneau de valuation.*

(ii) Tout anneau de valuation est local. Si K *est un corps valué d'anneau de valuation* $\mathcal{O}$ *et* $\mathfrak{M}$ *est son idéal maximal, alors* $\mathcal{O}/\mathfrak{M}$ *est appelé le corps résiduel de* K.

Dans tout ce qui suit, si (K, v) est un corps valué, on notera $\mathcal{O}_v$ son anneau de valuation, $\mathfrak{M}_v$ son idéal maximal, Γ_v son groupe de valuation et k_v son corps résiduel. S'il n'y a pas d'ambiguïté sur la valuation on les notera $\mathcal{O}_K$, $\mathfrak{M}_K$, Γ_K et k_K, voire $\mathcal{O}$, $\mathfrak{M}$, Γ et k s'il n'y a pas d'ambiguïté sur le corps non plus.

Définition 1.4 :
Soient v_1 et v_2 deux valuations sur un même corps K, on dit que $v_1 \leqslant v_2$ si et seulement si $\mathcal{O}_{v_2} \subseteq \mathcal{O}_{v_1}$. C'est un pré-ordre. On dira que deux valuations sont équivalentes si elles sont équivalentes pour la relation associée à ce pré-ordre, i.e. $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$.

Remarque 1.5 :
Soient v_1 et v_2 deux valuations sur un même corps K, v_1 est équivalente à v_2 si et seulement si il existe $\sigma : \Gamma_{v_1} \to \Gamma_{v_2}$, isomorphisme de groupes ordonnés, tel que $v_2 = \sigma \circ v_1$.

Il suit de cette remarque qu'on ne considérera désormais les valuations qu'à équivalence près. La théorie des corps valués n'est donc pas tant la théorie des valuations que la théorie des anneaux de valuation.
Pour faire de la théorie des modèles, il faut introduire le langage qu'on utilisera. Il y en a un certain nombre qui sont classiquement utilisés dans la littérature. Celui qui sera le plus utilisé ici est le suivant :

Définition 1.6 ($\mathcal{L}_{\text{div}}$) :
Le langage $\mathcal{L}_{\text{div}}$ est $\{+, -, \times, 0, 1, \text{div}\}$ où $+$, $-$ et $\times$ sont des fonctions binaires, 0 et 1 sont des constantes et div *est une relation binaire. Dans un corps valué (K, v), on interprète $+$, $-$, $\times$, 0 et 1 par la structure d'anneau de K et $x \operatorname{div} y$ par $v(x) \leqslant v(y)$.*

La théorie des corps valués est alors donnée par les axiomes suivants :

(i) « K est un corps » ;

(ii) $1 \operatorname{div} 1 \wedge 1 \operatorname{div} 0$;

(iii) $\forall x \forall y\ 1 \operatorname{div} x \wedge 1 \operatorname{div} y \Rightarrow 1 \operatorname{div} x + y \wedge 1 \operatorname{div} xy$;

(iv) $\forall x \forall y\ xy = 1 \Rightarrow (1 \operatorname{div} x \vee 1 \operatorname{div} y)$;

(v) $\forall x \forall y \forall z\ xy = 1 \Rightarrow (x \operatorname{div} z \iff 1 \operatorname{div} yz)$.

On aurait pu tout simplement prendre le langage des anneaux $\{+, -, \times, 0, 1\}$ et ajouter un prédicat pour l'anneau de valuation, mais alors, à moins de rajouter l'inverse, les théories que l'on considère plus loin perdent l'élimination des quantificateurs.

Remarque 1.7 :
Une sous-$\mathcal{L}_{\text{div}}$-structure est un anneau dont le corps des fractions (qui est aussi une sous-structure) est un corps valué muni de la restriction de la valuation.

Il y a un autre langage classique, qui est peut être plus proche de l'intuition que l'on a de ce qu'est un corps valué, mais qui a le défaut d'être multi-sorté.

Définition 1.8 :
Le langage tri-sorté des corps valué est constitué de trois sortes K, Γ_∞ et k et des symboles suivants :
- $\{+, -, \times, 0, 1\}$ *sur K et k ;*
- $\{+, -, 0, \leqslant, \infty\}$ *sur Γ_∞ ;*
- $v : K \to \Gamma_\infty$ *;*
- $\text{res} : K \to k$.

Il faut alors faire attention que la théorie des corps valué dans ce langage contient le fait que v et res sont surjectives, bien que ce ne soit pas le cas de toutes les structures. À ce détail près, la théorie des corps valués a les même propriétés dans ces deux langages, et, en particulier, les sous-ensembles définissables de la sorte K sont exactement les même que ceux qui sont définissables dans $\mathcal{L}_{\text{div}}$.

Définition 1.9 (ACVF) **:**
On note ACVF *la théorie des corps valués algébriquement clos de valuation non triviale dans* $\mathcal{L}_{\text{div}}$*. Elle est composée des axiomes suivants :*
- « K *est un corps valué* » *(voir l'axiomatisation de la théorie des corps valués ci-dessus) ;*
- *pour tout* $n \in \mathbb{N}^*$*,* « *tout polynôme de* $K[X]$ *de degré* n *admet une racine* » *;*
- *il existe* x *tel que* $\neg(x \operatorname{div} 1)$*.*

Dans la suite de ce mémoire, à de rares exceptions près, les corps valués seront toujours non trivialement valués. On ne considérera des corps valués de valuation triviale que dans la preuve du théorème **(1.33)** car ils pourront apparaître lorsque l'on considère des sous-structures. Pour finir, nous allons définir une classe de corps valués particulière qui est trés présente en théorie des modèles. À vrai dire, tous les corps dont on étudie la théorie dans ce mémoire en font partie.

Définition 1.10 (Corps Hensélien) **:**
Un corps valué (K, v) *est dit Hensélien si pour tout polynôme* $P[X] \in \mathcal{O}[X]$ *et tout* $a \in \mathcal{O}$ *tel que* $\operatorname{res}(P(a)) = 0$ *et* $\operatorname{res}(P'(a)) \neq 0$*, il existe* $b \in \mathcal{O}$ *tel que* $P(b) = 0$ *et* $\operatorname{res}(a) = \operatorname{res}(b)$*.*

Proposition 1.11 :
Soit (K, v) *un corps valué, les conditions suivantes sont équivalentes :*

(i) K *est Hensélien.*

(ii) Il n'y a qu'une extension de v *à toute extension algébrique de* K *(à équivalence près).*

(iii) Il n'y a qu'une extension de v *à toute extension finie de* K *(à équivalence près).*

(iv) (Hensel-Rychlik) Soient $P[X] \in \mathcal{O}[X]$ *et* $a \in \mathcal{O}$ *tel que* $v(P(a)) > 2v(P'(a))$*, il existe alors* $b \in \mathcal{O}$ *tel que* $P(b) = 0$ *et* $v(b - a) = v(P(a)) - v(P'(a))$*.*

Proof.

(iv) $\Rightarrow$ (i) Soient $P \in \mathcal{O}[X]$ et $a \in \mathcal{O}$ tel que $\operatorname{res}(P(a)) = 0$ et $\operatorname{res}(P'(a)) \neq 0$ i.e. $v(P(a)) > 0 = v(P'(a))$. Alors par (iv) il existe $b \in \mathcal{O}$ tel que $P(b) = 0$ et $v(b-a) = v(P(a)) - 0 > 0$.

(i) $\Rightarrow$ (iv) Comme $v(P'(a))$ est strictement majoré par une valuation, on ne peut pas avoir $P'(a) = 0$. Soient $c = -P(a)/P'(a)$ et $Q(X) = P(Xc + a)/P(a)$. Si $P(x + a) = \sum_{i=0}^{n} \lambda_i X^i$ on a bien $\lambda_i \in \mathcal{O}$ et $Q(X) = \sum_{i=0}^{n} a_i(-1/P'(a))^i P(a)^{i-1} X^i$. Son coefficient constant est $a_0/P(a) = 1 \in \mathcal{O}$. Comme le coefficient de X est $-a_1/P'(a) = -1 \in \mathcal{O}$ et que, pour les autres,

$$\begin{aligned} v(a_i(-1/P'(a))^i P(a)^{i-1}) &\geqslant (i-1)v(P(a)) - iv(P'(a)) \\ &> (2(i-1) - i)v(P'(a)) \\ &\geqslant 0, \end{aligned}$$

il s'en suit bien que $Q(X) \in \mathcal{O}[X]$. De plus, $v(Q(1)) = v(\sum_{i=2}^{n} a_i(-1/P'(a))^i P(a)^{i-1})$ et tous les termes de la somme sont dans $\mathfrak{M}$ donc $v(Q(1)) > 0$. De même, $v(Q'(1) + 1) = v(\sum_{i=2}^{n} a_i i(-1/P'(a))^i P(a)^{i-1}) \geqslant v(Q(1)) > 0$ et donc $v(Q'(1)) = 0$. Le (i) nous donne alors $d \in \mathcal{O}$ tel que $Q(d) = 0$ et $v(d-1) > 0$, en particulier $v(d) = 0$. Si on pose $b = cd + a$, alors $P(b) = Q(d) = 0$ et $v(b-a) = v(c) + v(d) = v(P(a)) - v(P'(a))$.

(ii) $\Rightarrow$ (iii) C'est évident.

(iii) $\Rightarrow$ (ii) Soient $K \leqslant L$ une extension algébrique et $\mathcal{O}_1$ et $\mathcal{O}_2$ deux anneaux de valuation de L qui étendent $\mathcal{O}_v$. Pour tout $x \in L$, $K[x]$ est une extension finie de K et $\mathcal{O}_1 \cap K[x]$ et $\mathcal{O}_2 \cap K[x]$ en sont deux anneaux de valuation. Par (iii), ils sont égaux. Pour tout $x \in L$ on a donc $x \in \mathcal{O}_1 \iff x \in \mathcal{O}_1 \cap K[x] \iff x \in \mathcal{O}_2 \cap K[x] \iff x \in \mathcal{O}_2$.

(i) $\iff$ (ii) Se reporter à [EP05, Proposition 4.1.3, p. 87-90]. ■

Remarquons une conséquence immédiate de la proposition que l'on vient d'énoncer : comme un corps algébriquement clos n'a pas d'extension algébrique, il est Hensélien.

Corollaire 1.12 :
Toute extension algébrique d'un corps Hensélien est Hensélienne.

Proof. Soit $(K, v) \leqslant (L, w)$ une extension algébrique de corps valué, où K est Hensélien. Alors toute extension algébrique L' de L est une extension algébrique de K et comme toute valuation qui étend w étend v, il ne peut y avoir qu'une extension de w à L'. ■

Proposition 1.13 (Existence de l'Hensélianisé) **:**
Soit (K, v) *un corps valué, il existe un corps hensélien* (K^h, v^h) *et une injection de corps valué* $i : K \to K^h$*, qui est universelle au sens suivant : pour toute injection* j *de* K *dans un corps Hensélien* L*, il existe une unique injection* $\widehat{j}$ *de* K^h *dans* L *telle que* $j = \widehat{j} \circ i$

Proof. On peut en trouver une dans [EP05, 5.2.2, p.121] ■

1.2 Extensions des valuations

Le but de cette section est d'étudier comment les valuations peuvent s'étendre à une extension de corps. On montrera tout d'abord que de telles extensions existent toujours, et ensuite on se restreindra aux extensions algébriques pour démontrer le théorème de conjugaison (voir (**1.28**)). La preuve donnée ici de ce dernier théorème est inspirée de [Rib99 ; EP05]. On peut aussi en trouver une dans [Lan02, Corollary XII.4.9, p.485].

Définition 1.14 (Extension de valuation) **:**
Soient (K, v) *et* (L, w) *deux corps valués tels que* $K \leqslant L$*. On dit que* w *étend* v *(et on note* $(K, v) \leqslant (L, w)$*) si* $\mathcal{O}_w \cap K = \mathcal{O}_v$*.*

On remarque alors que $w_{|K}$ et v sont équivalentes et donc quitte à remplacer v par une valuation équivalente, on peut supposer $w_{|K} = v$.
Tout d'abord montrons le théorème d'extension de Chevalley, la preuve donnée ici est celle de [Rib64, Théorème 4, p. 43-45]

Théorème 1.15 (Extension de Chevalley) **:**

Soient K *un corps,* A *un sous-anneau de* K *et* $\mathfrak{p}$ *un idéal premier de* A*, il existe alors un anneau de valuation* $\mathcal{O}$ *de* K *d'idéal maximal* $\mathfrak{M}$*, tel que* $A \subseteq \mathcal{O}$ *et* $\mathfrak{M} \cap A = \mathfrak{p}$*.*

Proof. Soit $\mathcal{F} := \{(\mathcal{O}, \mathfrak{M}) : A \subseteq \mathcal{O} \subseteq K,\ \mathcal{O}$ est un sous-anneau local de K d'idéal maximal $\mathfrak{M}$ et $\mathfrak{M} \cap A = \mathfrak{p}\}$. Cette famille contient $A_\mathfrak{p}$ (le localisé de A en $\mathfrak{p}$) qui est bien un sous-anneau local de K qui contient A et dont l'idéal maximal est $\mathfrak{p}A_\mathfrak{p}$ dont l'intersection avec A est bien $\mathfrak{p}$. De plus, on peut ordonner cette famille par $(B, \mathfrak{M}) \leqslant (B', \mathfrak{M}')$ si $B \subseteq B'$ et $\mathfrak{M}' \cap B = \mathfrak{M}$. Muni de cette ordre $\mathcal{F}$ est inductive, en effet si $(\mathcal{O}_i, \mathfrak{M}_i)$ est une chaîne alors $\mathcal{O} = \bigcup_i \mathcal{O}_i$ est un sous anneau de K qui contient A et dont $\mathfrak{M} = \bigcup_i \mathfrak{M}_i$ est un idéal. Si I est un autre idéal de $\mathcal{O}$, alors, pour tout i, $I \cap \mathcal{O}_i$ est un idéal de $\mathcal{O}_i$ et donc $I \cap \mathcal{O}_i \subseteq \mathfrak{M}_i$. Comme tout point de I est dans un $\mathcal{O}_i$, il s'en suit que $I \subseteq \mathfrak{M}$ et ce dernier est donc bien l'unique idéal maximal de $\mathcal{O}$. Enfin $\mathfrak{M} \cap A = \bigcup_i \mathfrak{M}_i \cap A = \bigcup_i \mathfrak{p} = \mathfrak{p}$.
Par le lemme de Zorn, il existe $(\mathcal{O}, \mathfrak{M})$ maximal dans $\mathcal{F}$. Supposons qu'il existe $x \in K$ tel que $x \notin \mathcal{O}$ et $x^{-1} \notin \mathcal{O}$. Supposons alors que $\mathfrak{M}[x] \neq \mathcal{O}[x]$, il existe $\mathfrak{M}'$ un idéal maximal de $\mathcal{O}[x]$ qui contient $\mathfrak{M}[x]$. Montrons alors que $\mathcal{O}[x]_{\mathfrak{M}'}$ est un élément de $\mathcal{F}$. C'est un sous-anneau de K qui contient A et dont l'unique idéal maximal est $\mathfrak{M}'\mathcal{O}[x]_{\mathfrak{M}'}$. De plus, $\mathfrak{M}'\mathcal{O}[x]_{\mathfrak{M}'} \cap \mathcal{O} = (\mathfrak{M}'\mathcal{O}[x]_{\mathfrak{M}'} \cap \mathcal{O}[x]) \cap \mathcal{O} = \mathfrak{M}' \cap \mathcal{O} \supseteq \mathfrak{M}[x] \cap \mathcal{O} \supseteq \mathfrak{M}$, or $\mathfrak{M}'\mathcal{O}[x]_{\mathfrak{M}'} \cap \mathcal{O}$ est un idéal de $\mathcal{O}$ qui ne contient pas 1 (sinon $\mathfrak{M}'\mathcal{O}[x]_{\mathfrak{M}'}$ devrait le contenir, ce qui contredirait son caractère maximal) et donc $\mathfrak{M}'\mathcal{O}[x]_{\mathfrak{M}'} \cap \mathcal{O} = \mathfrak{M}$. En particulier $\mathfrak{M}'\mathcal{O}[x]_{\mathfrak{M}'} \cap A = (\mathfrak{M}'\mathcal{O}[x]_{\mathfrak{M}'} \cap \mathcal{O}) \cap A = \mathfrak{M} \cap A = \mathfrak{p}$. Comme $\mathcal{O} \subsetneq \mathcal{O}[x]$, cela contredirait le fait que $(\mathcal{O}, \mathfrak{M})$ soit maximal. On a donc montré que $\mathcal{O}[x]\mathfrak{M} = \mathcal{O}[x]$. Par le même argument appliqué à x^{-1}, on a aussi $\mathcal{O}[x^{-1}]\mathfrak{M} = \mathcal{O}[x^{-1}]$.
Il s'en suit que $1 = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} b_i x^{-i}$ où les a_i et les b_i sont dans $\mathfrak{M}$. De plus, on peut supposer que n et m sont minimaux et que $m \leqslant n$ (l'autre cas est identique). On a alors $\sum_{i=1}^{m} b_i x^{-i} = 1 - b_0 \in \mathcal{O} \setminus \mathfrak{M}$ et donc, en posant $c_i = \frac{b_i}{1-b_0}$ qui est toujours dans $\mathfrak{M}$, on a $1 = \sum_{i=1}^{m} c_i x^{-i}$, d'où $x^n = \sum_{i=1}^{m} c_i x^{n-i}$ et $1 = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n-1} a_i x^i + \sum_{i=n-m}^{n-1} a_n c_{n-i} x^i$ ce qui contredit la minimalité de n.
Il s'en suit donc que pour tout $x \in K$, soit x soit x^{-1} est dans $\mathcal{O}$ et ce dernier est donc bien un anneau de valuation. ∎

On peut en déduire immédiatement l'existence d'extensions pour les valuations.

Corollaire 1.16 :
Soient (K, v) *un corps valué et* $K \leqslant L$ *une extension de corps, il existe alors une valuation* w *sur* L *qui étend* v*.*

Proof. On applique le théorème (**1.15**) dans L avec $A = \mathcal{O}_K$ et $\mathfrak{p} = \mathfrak{M}_K$. Il existe donc $\mathcal{O}$ un anneau de valuation de L d'idéal maximal $\mathfrak{M}$ qui contient $\mathcal{O}_K$ et tel que $\mathfrak{M} \cap K = \mathfrak{M}_K$. Si on avait $x \in (\mathcal{O} \cap K)$ qui ne soit pas dans $\mathcal{O}_K$, on aurait $x^{-1} \in \mathfrak{M}_K \subseteq \mathfrak{M}$, mais comme $x \in \mathcal{O}$, on aurait $1 \in \mathfrak{M}$ ce qui est absurde. On a donc bien $\mathcal{O} \cap K = \mathcal{O}_K$ et donc toute valuation sur L associée à $\mathcal{O}$ étend v. ∎

Remarque 1.17 :
La principale conséquence de ce théorème est que tout corps valué (K, v) *peut être plongé dans un corps valué algébriquement clos muni d'une valuation qui étend* v*. Cela sera particulièrement utile*

quand on voudra étudier la théorie de $\mathbb{Q}_p$ car tout modèle de cette théorie se plonge donc dans un corps valué algébriquement clos, théorie que l'on connaît mieux.

Rappelons ensuite le théorème des restes chinois qui sera utilisée dans la preuve du théorème d'approximation (**1.19**).

Théorème 1.18 (Théorème des restes chinois) **:**

> *Soient A un anneau, $(\mathfrak{A}_i)_{i=1\dots n}$ des idéaux tels que $\mathfrak{A}_i + \mathfrak{A}_j = A$ pour tout $i \neq j$, alors la flèche canonique $A \to \prod_i A/\mathfrak{A}_i$ est surjective.*

On prouve maintenant une version très faible du théorème d'approximation, mais qui suffira à notre démonstration. On peut en trouver des versions plus fortes dans [EP05] ou [Rib99].

Théorème 1.19 (Théorème d'approximation) **:**

> *Soient $(v_i)_{i=1\dots n}$ des valuations incomparables d'un corps K et $\mathfrak{M}_i$ l'idéal maximal de $\mathcal{O}_i$ l'anneau de valuation associé à la valuation v_i, alors pour tout $(a_i) \in \prod_i \mathcal{O}_i$, il existe $a \in \bigcap_i \mathcal{O}_i$ tel que pour tout i, $a - a_i \in \mathfrak{M}_i$.*

Commençons par démontrer un lemme technique.

Lemme 1.20 :
En reprenant les notation précédentes, soit $A = \bigcap_i \mathcal{O}_i$ et $\mathfrak{p}_i = A \cap \mathfrak{M}_i$. Alors pour tout i, $\mathcal{O}_i = A_{\mathfrak{p}_i}$ (i.e. le localisé de A en $\mathfrak{p}_i$).

Proof. Comme $A \subseteq \mathcal{O}_i$ et que $A \backslash \mathfrak{p}_i \subseteq \mathcal{O}_i \backslash \mathfrak{M}_i = \mathcal{O}_i^\star$, il s'en suit que $A_{\mathfrak{p}_i} \subseteq \mathcal{O}_i$. Soit maintenant $a \in \mathcal{O}_i$ (on peut supposer a non nul sinon c'est fini). Soit p un nombre premier supérieur à la caractéristique de tous les $k_j = \mathcal{O}_j/\mathfrak{M}_j$ et tel que le résidu de a dans k_j (quand il existe) n'est pas une racine p-ième de l'unité. On pose $b = \sum_{k=0}^{p-1} a^k$, et on va montrer que $b^{-1} \in A \backslash \mathfrak{p}_i$ et $ab^{-1} \in A$.
Soit j tel que $a \in \mathcal{O}_j$ et soit $\hat{a}_j$ son résidu dans k_j. Si $\hat{a}_j = 1$ le résidu de b, noté $\hat{b}_j$, est égal à p qui est non nul. Sinon $\hat{b}_j = (1 - \hat{a}_j^p)(1 - \hat{a}_j)^{-1} \neq 0$. Dans les deux cas $v_j(b) = 0$ et donc $b^{-1} \in \mathcal{O}_j^\star = \mathcal{O}_j \backslash \mathfrak{M}_j$ et bien sûr $ab^{-1} \in \mathcal{O}_j$. Comme $a \in \mathcal{O}_i$, on a, en particulier, que $b^{-1} \notin \mathfrak{M}_i \supseteq \mathfrak{p}_i$.
Si $a \notin \mathcal{O}_j$, alors $v_j(a) < 0$ et donc $a^{-1} \in \mathfrak{M}_j$. Si on pose $c = \sum_{k=0}^{p-1} a^{-k}$, on a alors $a^{p-1}b = c \in \mathcal{O}_j$ et de plus, par les même considérations que précédemment, c est inversible dans $\mathcal{O}_j$. On a donc $b^{-1} = a^{-(p-1)}c^{-1}$ et $ab^{-1} = a^{-(p-2)}c^{-1}$ ils sont bien tous les deux dans $\mathcal{O}_j$.
On a donc bien montré que ab^{-1} et b^{-1} sont dans $\bigcap_j \mathcal{O}_j$ et que $b^{-1} \notin \mathfrak{p}_i$. Il s'en suit immédiatement que $a = ab^{-1}/b^{-1} \in A_{\mathfrak{p}_i}$. ∎

Proof (Théorème (**1.19**)).
En reprenant les notations du lemme, si $\mathfrak{p}_i \subseteq \mathfrak{p}_j$, comme $A_{\mathfrak{p}_i} = \mathcal{O}_i$, on aurait alors $\mathcal{O}_j \subseteq \mathcal{O}_i$, ce qui est impossible car les valuations sont incomparables.
Montrons de plus que les $\mathfrak{p}_j$ sont maximaux. En fait on va montrer que tout idéal propre $\mathfrak{A}$ de A est inclus dans un $\mathfrak{p}_i$. Cela suffira car si on a un idéal propre de A tel que $\mathfrak{p}_i \subseteq \mathfrak{A}$ alors il existe j tel que $\mathfrak{p}_i \subseteq \mathfrak{A} \subseteq \mathfrak{p}_j$. Comme les $\mathfrak{p}_j$ sont incomparables, on doit alors avoir $i = j$ et $\mathfrak{p}_i = \mathfrak{A}$.
Par l'absurde, soit donc $\mathfrak{A}$ qui n'est inclus dans aucun $\mathfrak{p}_i$, on a alors pour tout i un $a_i \in \mathfrak{A} \backslash \mathfrak{p}_i$. De plus, comme $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$ pour $i \neq j$, soit $b_{ij} \in \mathfrak{p}_i \backslash \mathfrak{p}_j$. On pose alors $c_j = \prod_{i \neq j} b_{ij}$ qui est donc un

élément de $\mathfrak{p}_i$ pour tout $i \neq j$. De plus comme $\mathfrak{p}_j$ est premier, $c_j \notin \mathfrak{p}_j$. Les $a_j c_j$ sont donc des éléments de $\mathfrak{A}$ qui sont dans tous les $\mathfrak{p}_i$ pour $i \neq j$ et mais pas dans $\mathfrak{p}_j$. Et si on pose $d = \sum_j a_j c_j$ on obtient alors un élément de $\mathfrak{A}$ qui n'est dans aucun des $\mathfrak{p}_i$. Comme $\mathfrak{p}_i = A \cap \mathfrak{M}_i$ ils ne sont dans aucun des $\mathfrak{M}_i$. Comme les $\mathcal{O}_i$ sont des anneaux locaux, $d^{-1} \in \mathcal{O}_i$ pour tout i et donc $d^{-1} \in A$ ce qui implique que $\mathfrak{A}$ contient un élément inversible et donc $\mathfrak{A} = A$.
Comme les $\mathfrak{p}_i$ sont maximaux et distincts, le théorème des restes chinois (**1.18**) implique que la flèche canonique $A \to \prod_i A/\mathfrak{p}_i$ est surjective. De plus, le morphisme canonique $A \to A_{\mathfrak{p}_i} \to A_{\mathfrak{p}_i}/\mathfrak{p}_i A_{\mathfrak{p}_i}$ qui a $a \in A$ associe $a/1 + \mathfrak{p}_i A_{\mathfrak{p}_i}$ est une surjection. En effet, soit $a/b \in A_{\mathfrak{p}_i}$, i.e. $b \in A \backslash \mathfrak{p}_i$. Comme $\mathfrak{p}_i$ est maximal, l'idéal engendré par $\mathfrak{p}_i$ et b est A. Il existe donc $c \in A$ tel que $a - cb \in \mathfrak{p}_i$ et donc $a/b - c = (a - cb)/b \in \mathfrak{p}_i A_{\mathfrak{p}_i}$ et donc $a/b + \mathfrak{p}_i A_{\mathfrak{p}_i}$ est l'image de $c \in A$. De plus cette surjection passe au quotient et on a donc une surjection $A/\mathfrak{p}_i \to A_{\mathfrak{p}_i}/\mathfrak{p}_i A_{\mathfrak{p}_i}$. Mais ces deux anneaux sont des corps et le morphisme est donc injectif, i.e. $A/\mathfrak{p}_i \cong A_{\mathfrak{p}_i}/\mathfrak{p}_i A_{\mathfrak{p}_i}$. Comme par le lemme (**1.20**) on a $A_{\mathfrak{p}_i} = \mathcal{O}_i$ et que son idéal maximal est $\mathfrak{p}_i A_{\mathfrak{p}_i} = \mathfrak{M}_i$, on a une flèche $A \to \prod_i \mathcal{O}_i/\mathfrak{M}_i$ qui est surjective et il suffit de prendre pour a l'antécédent de $(a_i + \mathfrak{M}_i)_{i=1\ldots n}$. ■

Lemme 1.21 :
Soit $(K, v) \leqslant (L, w)$ une extension algébrique de corps, alors :

(i) $\Gamma_L \subseteq \mathrm{div}(\Gamma_K)$ *;*

(ii) $k_K \leqslant k_L$ *est une extension algébrique.*

Proof.

(i) Soit $w(x) \in \Gamma_L$, comme $K \leqslant L$ est algébrique, il existe $P \in K[X]$ tel que $P(x) = \sum_i a_i x^i = 0$. Mais alors, comme $w(P(x)) = \infty$ il existe i et j distincts tels que $w(a_i x^i) = w(a_j x^j)$ et donc $(j - i)w(x) = v(a_i) - v(a_j) \in \Gamma_K$.

(ii) Soient $\mathrm{res}(x) \in k_L$ et $P \in K[X]$ tel que $P(x) = \sum_i a_i x^i = 0$. Soit a_{i_0} de valuation minimale parmi les a_i, on a alors $Q(x) = \sum_i a_i a_{i_0}^{-1} x^i \in \mathcal{O}_v[x]$ qui annule x. Comme le coefficient i_0 de Q est 1, celui de $\mathrm{res}\, Q$ aussi, i.e. $\mathrm{res}(Q)$ est un polynôme non nul, et $\mathrm{res}(Q)(\mathrm{res}(x)) = \mathrm{res}(Q(x)) = 0$. ■

Corollaire 1.22 :
Soit $(K, v) \leqslant (L, w)$ une extension algébrique de corps valués. Si v est triviale alors w est triviale aussi.

Proof. Comme $\mathrm{div}(\{0\}) = \{0\}$, c'est une conséquence immédiate du lemme qui précède. ■

Lemme 1.23 :
Soit $\mathcal{O}$ un anneau de valuation, alors $\mathcal{O}$ est intégralement clos (dans son corps de fractions K).

Proof. Soient $P \in \mathcal{O}[X]$ unitaire et $x \in K$ tel que $P(x) = 0$. Notons $P = \sum_{i=0}^n a_i x^i$ et supposons que $v(x) < 0$. Alors pour tout $i < n$, on a $v(a_i x^i) = v(a_i) + i \cdot v(x) \geqslant i v(x) > n \cdot v(x) = v(a_n x^n)$ et donc $v(P(a)) = n \cdot v(x) \neq \infty = v(0)$, ce qui est absurde, donc $x \in \mathcal{O}$. ■

Lemme 1.24 :
Soit (K, v) un corps valué algébriquement clos, on a alors :

(i) Γ_K *est divisible ;*

(ii) k_K *est algébriquement clos.*

Proof.

(i) Soient $v(x) \in \Gamma_K$ et $n \in \mathbb{N}$. Comme K est algébriquement clos, il existe $y \in K$ tel que $y^n = x$. On a alors $nv(y) = v(x)$.

(ii) Soit $P \in k_K[X]$ unitaire il existe alors $Q \in \mathcal{O}_v[X]$ unitaire tel que $\mathrm{res}(Q) = P$. Comme K est algébriquement clos il existe $x \in K$ tel que $Q(x) = 0$. Comme $\mathcal{O}_v$ est intégralement clos par le lemme (**1.23**), on a $x \in \mathcal{O}_v$ et $P(\mathrm{res}(x)) = \mathrm{res}(Q(x)) = 0$. ■

Lemme 1.25 :
Soit $(K, v) \leqslant (L, w)$ *une extension normale de corps valués. Alors* $w \circ \sigma$ *est une valuation sur* L *pour tout* $\sigma \in \mathrm{Aut}(L/K)$ *et* $\bigcap_{\sigma \in \mathrm{Aut}(L/K)} \mathcal{O}_{w\circ\sigma}$ *est la clôture intégrale de* $\mathcal{O}_v$ *dans* L.

Proof. Le fait que $w \circ \sigma$ soit une valuation suit de vérifications évidentes. De plus, comme $\mathcal{O}_{w\circ\sigma}$ est intégralement clos dans L (voir lemme (**1.23**)), la clôture intégrale de $\mathcal{O}_v$ est incluse dans $\bigcap_{\sigma\in\mathrm{Aut}(L/K)} \mathcal{O}_{w\circ\sigma}$. Réciproquement, soit $x \in \bigcap_{\sigma\in\mathrm{Aut}(L/K)} \mathcal{O}_{w\circ\sigma}$. Comme l'extension est normale, $P(X) = \prod_{\sigma\in\mathrm{Aut}(L/K)}(X - \sigma(x)) \in K[X]$ et comme $\mathcal{O}_{w\circ\sigma} = \sigma^{-1}(\mathcal{O}_w)$, pour tout $\sigma \in \mathrm{Aut}(L/K)$, $w(\sigma(x)) \leqslant 0$ et donc $P \in \mathcal{O}_w[X]$. Mais, comme $\mathcal{O}_w \cap K = \mathcal{O}_v$, on a $P \in \mathcal{O}_v[X]$ et ce polynôme est unitaire et annule x. ■

Lemme 1.26 :
Soit (K, v) *un corps valué,* $K \leqslant L$ *une extension algébrique de corps et* $\mathcal{O}_1 \subseteq \mathcal{O}_2$ *deux anneaux de valuation de* L *au dessus de* $\mathcal{O}_v$*, alors* $\mathcal{O}_1 = \mathcal{O}_2$.

Proof. Montrons tout d'abord que $\mathfrak{M}_2 \subseteq \mathcal{O}_1$, où $\mathfrak{M}_2$ est l'idéal maximal de $\mathcal{O}_2$. Soit $x \in \mathfrak{M}_2$, comme $\mathcal{O}_1$ est un anneau de valuation, on a $x \in \mathcal{O}_1$ ou $x^{-1} \in \mathcal{O}_1$. Si $x^{-1} \in \mathcal{O}_1 \subseteq \mathcal{O}_2$ alors x est inversible dans $\mathcal{O}_2$ ce qui est absurde. De plus comme $\mathfrak{M}_2$ est un idéal de $\mathcal{O}_2 \supseteq \mathcal{O}_1$ c'est aussi un idéal de $\mathcal{O}_1$. On a alors $\widehat{\mathcal{O}_1} = \mathcal{O}_1/\mathfrak{M}_2 \subseteq \mathcal{O}_2/\mathfrak{M}_2 = k_2$.
Comme $\mathcal{O}_1$ et $\mathcal{O}_2$ sont des anneaux de valuation au dessus de $\mathcal{O}_K$, on a en particulier que $\mathfrak{M}_K \subseteq \mathfrak{M}_2 \cap \mathcal{O}$ et donc que $k_K = \mathcal{O}_K/\mathfrak{M}_K \subseteq \widehat{\mathcal{O}_1}$. D'après le lemme (**1.21**), $k_K \leqslant k_2$ est une extension algébrique, et comme on a $k_K \subseteq \widehat{\mathcal{O}_1} \subseteq k_2$, il s'en suit que pour tout $x \in \widehat{\mathcal{O}_1}$, $k_K[x]$ est une k-algèbre de dimension finie, intègre, donc un corps. Comme tout élément de $\widehat{\mathcal{O}_1}$ est inversible, c'est donc un corps. Mais $\widehat{\mathcal{O}_1}$ est un anneau de valuation de k_2. En effet, soit $\widehat{x} \in k_2$, où $x \in \mathcal{O}_2 \subseteq K_2$. Si $x \in \mathcal{O}_1$ alors $\widehat{x} \in \widehat{\mathcal{O}_1}$ et si $x^{-1} \in \mathcal{O}_1$ alors $(\widehat{x})^{-1} = \widehat{x^{-1}} \in \widehat{\mathcal{O}_1}$. On a donc $\widehat{\mathcal{O}_1} = \mathrm{Frac}(\widehat{\mathcal{O}_1}) = k_2$. Il s'en suit immédiatement que $\mathcal{O}_1 = \mathcal{O}_2$. ■

Lemme 1.27 :
Soient v *et* $(v_i)_{i=1\ldots n}$ *des valuations non triviales de K telles que* $\bigcap_i \mathcal{O}_{v_i} \subseteq \mathcal{O}_v$*, alors il existe un indice* i_0 *tel que* $\mathcal{O}_v$ *et* $\mathcal{O}_{v_{i_0}}$ *sont comparables.*

Proof. Quitte à retirer les j tels que $\mathcal{O}_{v_i} \subseteq \mathcal{O}_{v_j}$ pour un certain $i \neq j$, on peut supposer qu'aucune des valuations v_i ne sont comparables. Supposons alors que v n'est comparable à aucune des valuations v_i, alors par le théorème (**1.19**), il existe $x \in \bigcap_i \mathcal{O}_{v_i} \cap \mathcal{O}_v$ tel que $v(x - 1) > 0$ et $v_i(x) > 0$ pour tour i. Mais alors comme $v(x) > 0$ implique $v(x - 1) = 0$, on

a donc $v(x) = 0$. De même on trouve $y \in K$ tel que $v(y) > 0$ et $v_i(y) = 0$ pour tout i. Mais alors $v(x/y) = -v(y) < 0$ et $v_i(x/y) = v_i(x) > 0$ pour tout i, ce qui contredit le fait que $\bigcap_i \mathcal{O}_{v_i} \subseteq \mathcal{O}_v$. ■

Théorème 1.28 (Théorème de conjugaison) **:**

> *Soit (K, v) un corps valué et $(K, v) \leqslant (L, w)$ une extension normale de corps valué, alors toute valuation w' sur L qui étend v est de la forme (à équivalence près) $w \circ \sigma$ pour $\sigma \in \mathrm{Aut}(L/K)$.*

Proof. Le cas où v est triviale est traitée dans le corollaire (**1.22**), on peut donc supposer qu'elle ne l'est pas.
Comme w' étend v, $\mathcal{O}_{w'} \cap K = \mathcal{O}_v$. De plus, d'après le lemme (**1.23**), $\mathcal{O}_{w'}$ est intégralement clos dans L et d'après le lemme (**1.25**), $\bigcap_{\sigma \in \mathrm{Aut}(K/K)} \mathcal{O}_{w\circ\sigma}$ est la clôture intégrale de $\mathcal{O}_v$ dans L, on a donc $\bigcap_{\sigma\in\mathrm{Aut}(L/K)} \mathcal{O}_{w\circ\sigma} \subseteq \mathcal{O}_{w'}$. Mais alors d'après le lemme (**1.27**), comme $\mathrm{Aut}(L/K)$ est fini, il existe $\sigma \in \mathrm{Aut}(L/K)$ tel que $\mathcal{O}_{w'}$ et $\mathcal{O}_{w\circ\sigma}$ sont comparables et donc, par le lemme (**1.26**), w' et $w \circ \sigma$ sont équivalentes. ■

Le résultat que l'on utilisera vraiment est une extension de ce théorème à toute la clôture algébrique.

Corollaire 1.29 :
Soient (K, v) un corps valué, K_1 et K_2 deux clôtures algébriques de K. Soient v_1 et v_2 des valuations sur K_1 et K_2 respectivement qui étendent v. Alors il existe $\sigma \in \mathrm{Iso}_K(K_1, K_2)$ tel que $v_1 = v_2 \circ \sigma$ (à équivalence près).

Proof. Soit $X := \{(L_1, \sigma) : K \leqslant L_1 \leqslant K_1, \sigma \in \mathrm{End}_K(L_1, K_2) \text{ et } v_{1\,|L_1} = v_2 \circ \sigma\}$. Cet ensemble ordonné par l'inclusion est inductif et donc par le lemme de Zorn, il existe $(L_1, \sigma) \in X$ maximal. Montrons que $L_1 = K_1$. On aura alors $K \leqslant \sigma(K_1) \leqslant K_2$ et $\sigma(K_1)$ algébriquement clos d'où $\sigma(K_1) = K_2$ et on aura terminé.
Supposons donc, par l'absurde, qu'on ait $a \in K_1 \backslash L_1$. Soit L_1' la clôture normale de $L_1[a]$. Comme K_1 est la clôture algébrique de L_1, par unicité de la clôture algébrique (au dessus d'un isomorphisme), on peut étendre σ en $\sigma' \in \mathrm{Iso}_K(K_1, K_2)$. Le corps L_1' est muni de deux valuations qui sont les restrictions de v_1 et $v_2 \circ \sigma'$, et ces deux valuations coïncident sur L_1. Par le théorème (**1.28**), il existe $\tau \in \mathrm{Aut}(L_1'/L_1)$ tel que $v_{1\,|L_1'} = v_2 \circ \sigma' \circ \tau$. Mais alors $(L_1', \sigma' \circ \tau) \in X$, ce qui contredit le fait que (L_1, σ) soit maximal. ■

1.3 Élimination des quantificateurs dans ACVF

La preuve de l'élimination des quantificateurs pour les corps valués est adaptée de celle de [Cha08] en utilisant un autre critère, plus élémentaire.

Lemme 1.30 (Critère d'élimination des quantificateurs) **:**
Une théorie T dans un langage $\mathcal{L}$ admet l'élimination des quantificateurs si et seulement si pour tous modèles $\mathcal{M}$ et $\mathcal{N}$ de T qui contiennent une $\mathcal{L}$-structure commune $\mathcal{A}$, toute formule φ sans quantificateurs de $\mathcal{L}_A$ et $\bar{m} \in M$ tel que $\mathcal{M} \vDash \varphi[\bar{m}]$, il existe $\bar{n} \in N$ tel que $\mathcal{N} \vDash \varphi[\bar{n}]$.

On veut maintenant utiliser le critère précédent, mais il est plus simple de d'abord supposer que $\mathcal{A}$ est un modèle, puis en déduire le cas où $\mathcal{A}$ n'est qu'une structure en utilisant le théorème de conjugaison.

Lemme 1.31 :
Soient (K, v) *et* (L, w) *deux modèles de* ACVF *tels que* (K, v) *est une sous-structure de* (L, w) *et* φ *une formule sans quantificateurs de* $\mathcal{L}_A$*, on a* $L \vDash \exists x \varphi[x]$ *si et seulement si* $K \vDash \exists x \varphi[x]$

Proof. D'après la remarque (**1.7**), K est un sous-corps de L muni de la restriction de la valuation. Soit alors $m \in L$ tel que $L \vDash \varphi[m, \bar{a}]$. On veut montrer qu'il existe $m' \in K$ tel que $K \vDash \varphi[m', \bar{a}]$. Si $m = 0$ alors il est déjà dans K et c'est évident. On peut donc supposer m inversible et comme toute formule sur m est équivalente à une formule sur m^{-1} (il suffit de remplacer x par $1/x$ dans les polynômes qui apparaissent et multiplier par la bonne puissance de x pour que cela garde un sens), on peut supposer que $w(m) \geqslant 0$. De même, si m est algébrique sur K, qui est algébriquement clos, on a $m \in L$ et c'est fini. On peut donc aussi supposer que m est transcendant sur K.
Il y a donc trois cas qui correspondent aux différentes formes d'extension transcendante.

Extension purement ramifiée : Supposons qu'il existe $b \in K$ tel que $w(m - b) \notin \Gamma_K$. Quitte à considérer $\varphi[x + b, \bar{a}]$, on peut considérer que $w(m) \notin \Gamma_K$. On peut alors supposer (comme toujours) que φ est une conjonction d'atomes et de négation d'atomes, i.e. de la forme suivante :

$$\bigwedge_{i=1}^{n} \neg P_i(x) = 0 \wedge \bigwedge_{j=1}^{n'} R_j[x] \operatorname{div} R'_j[x] \wedge \bigwedge_{j=n'+1}^{n''} \neg R_j[x] \operatorname{div} R'_j[x]$$

Notons $R_j = \lambda_1 \prod_k (x - a_{j,k})^{n_{j,k}}$ et de même pour R'_j. Quitte à agrandir $\bar{a}$, on peut supposer que toutes les racines sont dedans. Soit alors (G, D) la coupure de $w(m)$ dans $v(\bar{a})$, i.e. $G = \{x \in \bar{a} : w(x) < w(m)\}$ et $D = \{x \in \bar{a} : w(m) < w(x)\}$. On a alors

$$w(R_j(m)) = w(\lambda) + \sum_{a_{j,k} \in G} n_{j,k} w(a_{j,k}) + \sum_{a_{j,k} \in D} n_{j,k} w(m)$$

et donc $R_j(m) \operatorname{div} R'_j(m)$ si et seulement si :

$$w(\frac{\lambda_j}{\lambda'_j}) + \sum_{a_{j,k} \in G} n_{j,k} w(a_{j,k}) - \sum_{a'_{j,k} \in G} n'_{j,k} w(a'_{j,k}) + (\sum_{a_{j,k} \in D} n_{j,k} - \sum_{a'_{j,k} \in D} n'_{j,k}) w(m) \leqslant 0,$$

c'est-à-dire $n_j w(m) \leqslant b_j$ avec $n_j \in \mathbb{Z}$ et $b_j \in \Gamma_K$. Comme L est algébriquement clos, Γ_K est divisible (voir lemme (**1.24**)) et comme $w(m) \notin \Gamma_K$, $R_j(m) \operatorname{div} R'_j(m)$ est donc équivalent à $w(m) < b'_j$ ou $w(m) > b'_j$ avec $b'_j \in \Gamma_K$. Quitte à supposer que les b'_j sont dans $v(\bar{a})$, les conditions sur la valuation de m (même les négations) sont donc toutes équivalentes à la réalisation de la coupure de $w(m)$ sur $v(\bar{a})$. Mais comme $\Gamma_K \vDash$ DLO dont tous les modèles sont ω-saturés, il existe $m' \in K$ qui réalise cette coupure. De plus pour tout $u \in K$ tel que $w(u) > w(m')$, $w(m' + u) = w(m')$ réalise aussi cette coupure et il y a donc une infinité de valeurs possibles pour m'. Il suffit d'en prendre une qui n'annule aucun des P_i et on a alors $K \vDash \varphi[m', \bar{a}]$.

Extension purement inertielle : Supposons qu'il existe b et $c \in K$ tel que $\mathrm{res}((m-b)/c) \notin k_K$. Quitte à considérer $\varphi[cx+b, \bar{a}]$, on peut considérer que $\mathrm{res}(m) \notin k_K$.
Si on a $b \in K$ tel que $v(b) = w(m)$, on a alors $w(m-b) \geqslant w(m) \geqslant 0$. Mais si $w(m-b) > 0$ on a alors $\mathrm{res}(m-b) = 0$ et donc $\mathrm{res}(m) = \mathrm{res}(b) \in k_K$ ce qui est absurde. Donc $w(m-b) = 0$. Soit alors (G, E, D) la coupure de $w(m)$ dans $v(\bar{a})$, où $E = \{x \in \bar{a} : w(x) = w(m)\}$. On a alors :

$$w(R_j(m_1)) = w(\lambda_j) + \sum_{a_{j,k} \in G} n_{j,k} w(a_{j,k}) + \sum_{a_{j,k} \in D} n_{j,k} w_1(m_1).$$

Comme k_K est algébriquement clos pas le lemme (**1.24**), il est infini et il y a donc une infinité de $m' \in K$ tels que $w(m') = 0$ et $\mathrm{res}(m') \neq \mathrm{res}(b)$ pour tout $b \in \bar{a}$. On en choisit un qui n'annule aucun des P_i. On peut alors vérifier que pour tout $b \in \bar{a}$ on a $w(m-b) = w(m'-b)$. En effet, si $b \in D$, $w(m'-b) = w(m') = 0 = w(m-b)$, si $b \in G$, $w(m'-b) = w(b) = w(m-b)$ et si $w(b) = 0$, $w(m'-b) \geqslant 0$ mais comme $\mathrm{res}(m') \neq \mathrm{res}(b)$, $w(m'-b) \leqslant 0$ et donc $w(m'-b) = 0 = w(m-b)$. Il s'en suit donc que $K \vDash \varphi[m', \bar{a}]$.

Extension immédiate : Il reste le cas où, pour tout $b \in K$, $w(m-b) \in \Gamma_K$ et pour tous $b, c \in K$, $\mathrm{res}((m-b)/c) \in k_K$. L'ensemble $X = \{w(m-b) : b \in K\}$ n'a alors pas de maximum. En effet soit $b, c \in K$ tel que $w(m-b) = w(c)$. On a alors $w((m-b)/c) = 0$ et il existe donc $u \in K$ tel que $\mathrm{res}(u) = \mathrm{res}((m-b)/c)$. On a donc $w((m-b)/c - u) > 0$ et donc $w(m-(b+uc)) > w(c) = w(m-b)$. On peut donc trouver $m' \in K$ tel que $w(m'-m) > w(m-b)$ pour tout $b \in \bar{a}$. On a alors $w(m'-b) = w(m'-m_1+m_1-b) = w(m-b)$ et donc pour tout polynôme $P \in K[X]$ à racines dans $\bar{a}$, $w(P(m)) = w(P(m'))$. De plus comme X n'a pas de maximum, il y a une infinité de m' qui conviennent. On peut donc en prendre un qui n'annule aucun des P_i. On a alors $K \vDash \varphi[m', \bar{a}]$. ∎

Remarque 1.32 :

(i) *La modèle complétude nous permet de comprendre la clôture algébrique dans* ACVF. *En effet, soit* $(K, v) \vDash$ ACVF *et* $A \subseteq K$. *Comme* $\mathcal{L}_{\mathrm{div}}$ *contient le langage des anneaux, il est évident que* $\mathrm{acl}(A)$ *contient* $K' = \overline{\mathrm{Frac}(<A>)}^{\mathrm{alg}}$, *i.e. la clôture algébrique du corps des fractions de l'anneau engendré par* A *(que l'on notera dorénavant* $\overline{A}^{\mathrm{alg}}$ *même si* A *n'est qu'un ensemble quelconque de paramètres). De plus, il est évident que* K' *est un corps valué algébriquement clos et donc* $K' \preccurlyeq K$, *ce qui implique que* $\mathrm{acl}(A) \subseteq K' = \overline{A}^{\mathrm{alg}}$ *et donc* $\mathrm{acl}(A) = \overline{A}^{\mathrm{alg}}$.

(ii) *En revanche,* dcl *n'est pas la clôture rationnelle comme c'est le cas dans les corps algébriquement clos. C'est en fait l'hensélianisé. En reprenant les notations précédentes, comme* $\mathcal{L}_{\mathrm{div}}$ *contient le langage des anneaux,* $\mathrm{Frac}(<A>) \subseteq \mathrm{dcl}(A)$ *on peut donc supposer que* $A = \mathrm{Frac}(<A>)$ *et donc que* A *est un corps. On choisit alors* A^h *un Hensélianisé de* A. *Comme* K *est algébriquement clos (et donc Hensélien) il s'en suit que* A^h *s'injecte dans* K. *Quitte à l'identifier à son image, on peut donc considérer que c'est un sous-corps de* K. *Soit alors* σ *un automorphisme de* K *(en tant que corps valué) qui fixe* A. *Il s'en suit que si on note* $i : A \to A^h$ *et* $j : A^h \to K$ *les injections induites par l'inclusion, on a* $\sigma \circ i = \sigma_{|A} = j \circ i$ *et donc par la propriété universelle de l'Hensélianisé,* $\sigma_{|A^h} = j$ *i.e.* A^h *est fixé point par point*

par σ. Il s'en suit donc que $A^h \subseteq \mathrm{dcl}(A)$. Toujours comme $\mathcal{L}_{\mathrm{div}}$ contient le langage des anneaux, $\mathrm{dcl}(A)$ *doit contenir $K' = \overline{A^h}^{\mathrm{ins}}$, la clôture inséparable de A^h. Montrons alors que* $\mathrm{dcl}(A) = K'$.

Soit $x \notin \backslash K'$. Comme x est séparable au dessus de K', il existe un automorphisme σ de K qui fixe K' mais pas x. Mais comme K' est Hensélien par le corollaire (1.12), v est $v \circ \sigma$ qui sont deux valuations de K qui coïcident sur K' sont équivalentes, i.e. $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ et donc σ est un automorphisme de K en temps que corps valué. On a donc $x \notin \mathrm{dcl}(A)$.

Théorème 1.33 :

La théorie ACVF *admet l'élimination des quantificateurs dans le langage $\mathcal{L}_{\mathrm{div}}$.*

Proof. Soient (K_1, v_1) et (K_2, v_2) deux modèles de ACVF et (K, v) un sous-corps valué commun (qui est bien une sous-$\mathcal{L}_{\mathrm{div}}$-structure de chacun des modèles par la remarque (1.7)). Soient (K_1', v_1') et (K_2', v_2') les clôtures algébriques de K dans K_1 et K_2 respectivement, munis des restrictions des valuations. Par le corollaire (1.29), il existe $\sigma \in \mathrm{Iso}_K(K_1', K_2')$ qui soit un isomorphisme de corps valué. Il induit un plongement de K_1' dans K_2 et on peut donc remplacer K par K_1', i.e. considérer que K est algébriquement clos.
Soient alors $\varphi[x] \in \mathcal{L}_{\mathrm{div}}$ sans quantificateurs à paramètres dans K et $m_1 \in K_1$ tel que $K_1 \vDash \varphi[m_1]$. D'après le lemme (1.30), il suffit de vérifier qu'il existe $m_2 \in K_2$ tel que $K_2 \vDash \varphi[m_2]$. Si K est de valuation non triviale, c'est un modèle de ACVF et donc par le lemme (1.31), $K_1 \vDash \exists x \varphi[x]$ implique $K \vDash \exists x \varphi[x]$, qui implique $K_2 \vDash \exists x\, \varphi[x]$.
Reste le cas où K est trivialement valué. La preuve du lemme (1.31) marche encore et permet de trouver un $m \in K$ tel que $K \vDash \varphi[m]$ et donc, comme φ est sans quantificateurs, $K_2 \vDash \varphi[m]$, sauf dans le cas de l'extension totalement ramifiée, car on a alors $\{0\} \nvDash \mathrm{DLO}$. Mais dans ce cas-là, la coupure de m_1 sur K se résume à savoir si $v(m_1) > 0$ ou pas. Il suffit alors de choisir $m_2 \in K_2$ qui n'annule aucun des P_i et tel que $v(m_2) > 0$ si et seulement si $v(m_1) > 0$. On aura alors bien $K_2 \vDash \varphi[m_2]$. ∎

Une première remarque que l'on peut faire est que l'élimination des quantificateurs dans le langage tri-sorté se déduit assez facilement du résultat que l'on donne ici et permet de démontrer que Γ est un pur groupe abélien totalement ordonné, divisible et sans torsion et que k est un pur corps algébriquement clos.
Comme souvent, il n'est pas difficile de déduire les complétions d'une théorie, une fois que l'on sait qu'elle admet l'élimination des quantificateurs.

Corollaire 1.34 (Complétude de ACVF) **:**
Les complétions de ACVF *sont données par la caractéristique du corps et celle du corps résiduel (appelée caractéristique résiduelle). Les cas possibles sont $(0,0)$, $(0,p)$ et (p,p) où p est un nombre premier. On note $\mathrm{ACVF}_{(n,m)}$ ces différentes complétions.*

Proof. Le fait qu'un corps est de caractéristique $p \neq 0$ s'exprime au premier ordre dans $\mathcal{L}_{\mathrm{div}}$ par $\sum_{i=1}^{p} 1 = 0$. De même, le fait qu'il soit de caractéristique résiduelle p s'exprime par $v(p) > 0$ i.e. $\neg(\sum_{i=1}^{p} 1 \operatorname{div} 1)$. Les complétions de ACVF fixent donc bien ces deux caractéristiques.
D'autre part, comme on a un morphisme d'anneau qui va de $\mathcal{O}$ l'anneau de valuation (qui est de même caractéristique que le corps valué) vers k, le corps résiduel, il s'en suit que la

caractéristique résiduelle divise la caractéristique et les cas possibles sont donc bien $(0,0)$, $(0,p)$ et (p,p).
Si un corps valué K est de caractéristique $(0,0)$, alors $\mathbb{Z} \subseteq K$. Comme pour tout $n \in \mathbb{Z}\backslash\{0\}$, $v(n) = v(\sum_{i=1}^{n} 1) \geqslant v(1) = 0$ mais qu'on ne peut pas avoir $v(n) > 0$, on a $v(n) = 0$ et donc $\mathbb{Z}$ muni de la valuation triviale est une sous-structure de tous les corps valués de caractéristique $(0,0)$, par élimination des quantificateurs, cela suffit pour montrer que $\mathrm{ACVF}_{(0,0)}$ est complète.
Si un corps K est de caractéristique $(0,p)$, alors $\mathbb{Z} \subseteq K$, mais maintenant, pour tout $n \in \mathbb{Z}\backslash\{0\}$ on a $v(n) > 0 \iff \mathrm{res}(n) = 0 \iff p|n$. D'où $\mathbb{Z}$ muni de la valuation p-adique (voir définition (**2.6**)) est une sous-structure commune à tous les modèles de $\mathrm{ACVF}_{(0,p)}$. Enfin, si K est de caractéristique (p,p), alors $\mathbb{Z}/p\,\mathbb{Z}$ muni de la valuation triviale est une sous-structure de K. ■

Une autre conséquence de ce résultat d'élimination des quantificateurs est un résultat de Holly (voir la proposition (**1.36**)), qui donne une description canonique des ensembles définissables de ACVF. Cette description utilise des sous-ensembles d'un corps valués qui sont particulièrement importants : les boules. Si (K,v) est un corps valué, pour tout $\gamma \in \Gamma_K$ et $a \in K$, on note $B_{\geqslant\gamma}(a) := \{x \in K : v(x-a) \geqslant \gamma\}$, la boule fermée de centre a et de rayon γ et $B_{>\gamma}(a) := \{x \in K : v(x-a) > \gamma\}$, la boule ouverte de centre a et de rayon γ. Une boule de K est alors n'importe quel ensemble définissable qui soit d'une de ces deux formes. Il faut cependant faire attention au fait que si $K \leqslant L$, l'empreinte d'une boule de L dans K n'est pas forcément une boule.

Définition 1.35 (Fromage suisse) **:**
Soit (K,v) un corps valué. Un fromage suisse de K est un ensemble de la forme $b\backslash(\bigcup_{i=1}^{n} b_i)$ où b et les b_i sont des boules. On dira que deux fromages suisses sont trivialement emboîtés si la boule extérieure de l'un est un trou de l'autre.

Proposition 1.36 ([Hol95, Théorème 3.26]) **:**
Soit $(K,v) \models \mathrm{ACVF}$, tout sous-ensemble définissable de K s'écrit de manière unique comme une union finie de fromages suisses non trivialement emboîtés.

Enfin, maintenant que l'on sait que ACVF admet l'élimination des quantificateurs, l'étude des formules faite dans la preuve de (**1.31**) permet de décrire le cardinal des ensemble définissables.

Proposition 1.37 :
Soit $(K,v) \models \mathrm{ACVF}$, alors tout ensemble définissable dans K est soit fini soit du cardinal de K.

Proof. Montrons tout d'abord qu'il suffit de considérer les ensembles à une variable. Soient $X \subseteq K^n$ définissable et π_i la projection sur la i-ième composante. Si tous les $\pi_i(X)$ sont finis, alors X est inclus dans un produit fini d'ensemble finis et est donc fini. Par contre, si l'un des $\pi_i(X)$ est infini, il suffit de montrer que ce $\pi_i(X)$ est de même cardinal que K car c'est alors aussi le cas de X qui se surjecte sur cet ensemble.
Soit alors $X \subseteq K$ définissable par une formule φ. Par élimination des quantificateurs, on peut supposer que c'est une disjonction de conjonctions d'atomes et de négations d'atomes. Il suffit alors de le montrer pour les conjonctions. En effet si elles définissent toutes un ensemble fini alors X aussi et si l'une d'entre elles définit un ensemble infini, il serait alors du même

cardinal que K et donc X aussi car il le contient. On peut donc supposer que X est défini par une conjonction. Si un atome de la forme $P(x) = 0$ apparaît alors X est fini. On peut donc supposer que X est défini par une formule de la forme :

$$\bigwedge_{i=1}^{n} \neg P_i(x) = 0 \wedge \bigwedge_{j=1}^{n'} R_j[x] \operatorname{div} R'_j[x] \wedge \bigwedge_{j=n'+1}^{n''} \neg R_j[x] \operatorname{div} R'_j[x].$$

De plus, on peut écrire tous les polynômes qui apparaissent sous forme scindée et supposer que les racines sont dans l'ensemble fini A des paramètres qui définissent X. Si X est vide alors c'est fini, sinon soit $m \in X$. L'ensemble $\{v(m-a) : a \in A\}$ est fini et soit γ qui le majore. Montrons que la boule $B_{>\gamma}(m) \subseteq X$. Tous les points de cette boule sont distincts des racines des P_i car par définition de γ, $v(m-a) \leqslant \gamma$. De plus, soit $m' \in B_{>\gamma}(m)$, pour tout $a \in A$, $v(m'-a) = v(m'-m+m-a) = v(m-a)$ car $v(m'-m) > \gamma \geqslant v(m-a)$. Pour tout polynôme Q qui apparaît dans la formule, on a donc $v(Q(m')) = v(\lambda \prod_i (m'-a_i)) = v(\lambda) + \sum_i v(m'-a_i) = v(\lambda) + \sum_i v(m-a_i) = v(Q(m))$ et il s'en suit que m' vérifie aussi la formule.
Il suffit donc de montrer que toute les boules ouvertes de rayon fini sont de même cardinal que K, et comme elles sont toutes de la forme $a + x\mathfrak{M}$ où $v(x)$ est le rayon de la boule, il suffit de montrer que $\mathfrak{M}$ a le même cardinal que K. Mais comme on a un morphisme de groupe $v : K^* \to \Gamma$ dont le noyau est $R\backslash\mathfrak{M}$ et que la valuation est non triviale, $\mathfrak{M}$ contient au moins un translaté du noyau et comme $K = \mathfrak{M} \cup (R\backslash\mathfrak{M}) \cup \mathfrak{M}^{-1}$, il s'en suit que $\mathfrak{M}$ est de même cardinal que K. ■

1.4 Élimination des imaginaires dans un cadre abstrait

Une fois la question de l'élimination des quantificateurs traitée, l'autre question qui se pose comme préliminaire à l'étude de toute théorie est celle de l'élimination des imaginaires. En effet, l'élimination des quantificateurs permet une description extrêmement simple de tous les ensembles définissables, mais il reste le problème des quotients définissables. A priori, ils ne sont pas représentées comme de « vrais » points des structures mais n'existent qu'en tant qu'ensembles de classes d'équivalence, ce qui les rend compliqués à traiter. Le but de l'élimination des imaginaires est justement d'en faire de vrais points.
Dans les définitions qui suivent, on distinguera, comme dans [Hod93], des notions uniformes et non-uniformes d'élimination des imaginaires. On ne définira cependant pas la notion d'élimination semi-uniforme qu'il introduit car, par compacité, elle est équivalente à l'élimination non-uniforme. Dans tout ce qui suit, $\mathcal{L}$ sera un langage.

Définition 1.38 (Code et code uniforme) **:**
Soient $\mathcal{M}$ une $\mathcal{L}$-structure et X un ensemble M-définissable. On dit que $\bar{a} \in M$ est un code pour X via $\varphi[\bar{x}, \bar{y}]$ une $\mathcal{L}$-formule, si $X = \varphi[\mathcal{M}, \bar{a}]$ et que $\bar{a}' \neq \bar{a}$ implique $\varphi[\mathcal{M}, \bar{a}] \neq \varphi[\mathcal{M}, \bar{a}']$.
Si $X = \theta[\mathcal{M}, \bar{b}]$, on dit que X est codé uniformément via $\varphi[\bar{x}, \bar{y}]$ si pour tout $\bar{b}' \in A$ (bien sorté), il existe un code de $\theta[\mathcal{M}, \bar{b}']$ via $\varphi[\bar{x}, \bar{y}]$.

Dans la définition de code, on autorise la variable $\bar{y}$ à représenter un 0-uplet, dans le cas où X est $\varnothing$-définissable.

Il est évident que la notion de codage uniforme sera beaucoup plus pratique que sa version non-uniforme, mais dans le cas où la théorie admet suffisamment de constantes, ces deux notions coïncident.

Lemme 1.39 :
Soit $\mathcal{M}$ une $\mathcal{L}$-structure telle que $\mathrm{dcl}(\varnothing)$ *contient au moins deux éléments de la même sorte et un élément de chaque sorte. Soit $\theta[\bar{x},\bar{y}]$ une $\mathcal{L}$-formule telle que pour tout $\bar{m} \in M$ (bien sorté), $\theta[\mathcal{M},\bar{m}]$ ait un code, alors ce codage peut être choisi uniformément.*

Proof. Pour tout $\bar{m} \in M$, on a $\varphi_{\bar{m}}[\bar{x},\bar{z}]$ et $\bar{a}_{\bar{m}}$ qui est un code de $\theta[\mathcal{M},\bar{m}]$ via $\varphi_{\bar{m}}[\bar{x},\bar{z}]$. L'ensemble de formules $\{\forall \bar{a}\,(\forall \bar{a}'\ \bar{a} \neq \bar{a}' \Rightarrow \neg(\forall \bar{x}\,\varphi[\bar{x},\bar{a}] \iff \varphi[\bar{x},\bar{a}'])) \Rightarrow \neg(\forall \bar{x}\,\varphi[\bar{x},\bar{a}] \iff \theta[\bar{x},\bar{m}]) : \varphi[\bar{x},\bar{z}] \in \mathcal{L}\}$ n'est donc pas satisfaisable et, par compacité, il n'est donc pas finiment satisfaisable. Il existe donc des formules $(\varphi_i[\bar{x},\bar{z}_i])_{i=1\dots n}$ telles que pour tout $\bar{m}$, il existe $\bar{a}$ et i tel que $\bar{a}$ est un code de $\theta[\mathcal{M},\bar{m}]$ via $\varphi_i[\bar{x},\bar{z}_i]$. De plus, on peut supposer que les $\bar{z}_i$ sont sortés de la même manière, quitte à rajouter des variables de la bonne sorte et spécifier qu'elles doivent être égales à une constante dans φ_i. On peut donc remplacer les $\bar{z}_i$ par un unique uplet de variables $\bar{z}$.
Quitte à remplacer les φ par $\varphi[\bar{x},\bar{z}] \wedge (\bigwedge_{j<i} \neg(\exists^{=1}\bar{z}'\forall \bar{x}\varphi_j[\bar{x},\bar{z}'] \iff \varphi_i[\bar{x},\bar{z}])$, on a alors que pour tout $\bar{m}$ il existe un unique $i_{\bar{m}}$ tel qu'il existe un code $a_{\bar{m}}$ de $\theta[\mathcal{M},\bar{m}]$ via φ_i. Soient c_1 et c_2 les deux constantes de même sorte, on pose alors $\psi[\bar{x},\bar{z},\bar{t}] = \bigvee_i(\bigwedge_{j\neq i} t_j = c_2 \wedge t_i = c_1) \wedge \varphi_i[\bar{x},\bar{z}]$, $\bar{c}^i$ le n-uplet de c_2 avec un c_1 à la i-ième place et pour tout $\bar{m}$, $\bar{b}_{\bar{m}} = \bar{a}_{\bar{m}}\bar{c}^{i_{\bar{m}}}$. Il est alors clair que pour tout $\bar{m}$, $\theta[\mathcal{M},\bar{m}]$ est codé par $\bar{b}_{\bar{m}}$ via ψ et donc que le codage est bien uniforme. ∎

Dorénavant, on dira qu'un théorie admet suffisamment de constantes si elle admet deux constantes d'une même sorte et une de chaque sorte.
Dans certains cas (voir les exemples (**1.48**)), les ensembles définissables ne sont pas exactement codés, mais c'est presque le cas (voir lemme (**1.47**)). Il existe donc une notion un peu plus large de codage, celui de codage faible.

Définition 1.40 (Code faible) **:**
Soient $\mathcal{M}$ une $\mathcal{L}$-structure et X un ensemble M-définissable. On dit que $\bar{a} \in M$ est un code faible pour X s'il existe une $\mathcal{L}$-formule $\varphi[\bar{x},\bar{y}]$ telle que $X = \varphi[\mathcal{M},\bar{a}]$ et qu'il n'existe qu'un nombre fini de $\bar{a}'$ tel que $X = \varphi[\mathcal{M},\bar{a}']$.
Comme précédemment on a aussi une notion de code faible uniforme.

Il existe une autre définition classique de la notion de code qui utilise les automorphismes. Le lemme suivant donne l'équivalence entre ces deux notions.

Proposition 1.41 :
Soient $\mathcal{M}$ une $\mathcal{L}$-structure, X un ensemble M-définissable et $\bar{a} \in M$. On a alors que $\bar{a}$ est un code de X si et seulement si tout automorphisme d'une extension assez saturée et homogène de $\mathcal{M}$ fixe $\bar{a}$ si et seulement si il fixe X.

Proof. Supposons que $\bar{a}$ soit un code de X. Comme X est $\bar{a}$-définissables, tout automorphisme qui fixe $\bar{a}$ fixe X et réciproquement si X est codé par $\bar{a}$ via $\varphi[\bar{x},\bar{y}]$ et que σ est un automorphisme qui fixe X, alors $\varphi[\bar{x},\sigma(\bar{a})]$ définit X et donc par définition d'un code, $\sigma(\bar{a}) = \bar{a}$.

D'autre part soit $\mathcal{N}$ une extension assez saturée et homogène de $\mathcal{M}$ et supposons que tout automorphisme de $\mathcal{N}$ fixe $\bar{a}$ si et seulement si il fixe X. Tout d'abord, comme X est $\mathrm{Aut}(\mathcal{N}/\bar{a})$-invariant et que $\mathcal{N}$ est assez saturé et homogène, il existe une formule $\varphi[\bar{x},\bar{y}]$ telle que $\varphi[\bar{x},\bar{a}]$ définit X. Posons $p = \mathrm{tp}(\bar{a})$, l'ensemble de formules $p[\bar{y}] \cup \{\forall \bar{x}\ \varphi[\bar{x},\bar{y}] \iff \varphi[\bar{x},\bar{a}], \bar{y} \neq \bar{a}\}$ n'est alors pas satisfaisable. En effet s'il l'était, il le serait dans $\mathcal{N}$ et il existerait donc σ un automorphisme de $\mathcal{N}$ qui fixe X mais pas $\bar{a}$ ce qui contredit notre hypothèse. Il existe donc $\psi[\bar{y}] \in \mathrm{tp}(\bar{a})$ telle que $\mathcal{N} \vDash \forall \bar{y}(\psi[\bar{y}] \wedge \forall \bar{x}\ \varphi[\bar{x},\bar{y}] \iff \varphi[\bar{x},\bar{a}]) \Rightarrow \bar{y} = \bar{a}$. Il s'en suit donc que X est codé par $\bar{a}$ via $\varphi[\bar{x},\bar{y}] \wedge \psi[\bar{y}]$. ■

Définition 1.42 (Élimination des imaginaires) **:**
Une théorie T *élimine (faiblement) les imaginaires si tout ensemble définissable d'un modèle de* T *admet un code (faible). L'élimination (faible) est dite uniforme si tout ensemble définissable est codé (faiblement) uniformément.*

Une conséquence immédiate du lemme (**1.39**) est que si une théorie admet suffisamment de constantes, alors elle a l'élimination des imaginaires si et seulement si elle a l'élimination uniforme des imaginaires.
La présentation qu'on a choisi de prendre ici passe par la notion de code mais, comme je l'ai fait remarquer précédemment, l'élimination des imaginaires est essentiellement, et historiquement, liée à la question de représenter les classes d'équivalence définissables (qui sont en quelque sorte des points « imaginaires ») par de « vrais » points du modèle.

Lemme 1.43 :
Soit T *une $\mathcal{L}$-théorie, elle élimine uniformément les imaginaires si et seulement si pour toute $\mathcal{L}$-formule qui définit une relation d'équivalence* E *dans* T*, il existe une $\mathcal{L}$-formule qui défini une fonction* f *dans* T *telle que* $T \vdash E[\bar{x},\bar{y}] \iff f(\bar{x}) = f(\bar{y})$.

Proof. Supposons que T élimine uniformément les imaginaires et soit $\mathcal{M} \vDash T$ et E une relation d'équivalence définissable. Comme les classes d'équivalence de E sont toutes définies par des formules de la forme $E[\bar{x},\bar{a}]$, où $\bar{a} \in M$, par élimination uniforme des imaginaires, il existe une $\mathcal{L}$-formule $\varphi[\bar{x},\bar{y}]$ telle que $E[\mathcal{M},\bar{a}]$ est codée via φ. La formule $\forall \bar{x}\ \varphi[\bar{x},\bar{y}] \iff E[\bar{x},\bar{z}]$ définit donc une fonction qui vérifie bien les propriétés voulues.
Réciproquement, soit $\varphi[\bar{x},\bar{y}]$ une $\mathcal{L}$-formule, on définit $E[\bar{y},\bar{y}'] := \forall \bar{x}\ \varphi[\bar{x},\bar{y}] \iff \varphi[\bar{x},\bar{y}']$ qui est bien une relation d'équivalence. Par hypothèse, il existe une fonction définissable f_E telle que $E[\bar{y},\bar{y},] \iff f_E(\bar{y}) = f_E(\bar{y}')$. Il est alors facile de voir que $f_E(\bar{a})$ code uniformément $\varphi[\mathcal{M},\bar{a}]$ via $\theta[\bar{x},\bar{z}] := \exists \bar{y}\ \varphi[\bar{x},\bar{y}] \wedge f_E(\bar{y}) = \bar{z})$. ■

La notion d'imaginaire a été introduite par S. Shelah (voir [She78, Definition 6.2, p. 129]) à travers la construction suivante, dont l'utilité en théorie des modèle n'est plus à démontrer.

Définition 1.44 (T^{eq} et $\mathcal{M}^{eq}$) **:**
Soit T *une $\mathcal{L}$-théorie, on lui associe un langage $\mathcal{L}^{eq}$ qui contient, pour toute relation $E[\bar{x},\bar{y}]$ $\varnothing$-définissable (où $\bar{x}$ et $\bar{y}$ ont la même longueur) telle que* $T \Rightarrow$ « E *est une relation d'équivalence », une sorte S_E et un symbole de fonction $f_E : S_= \to S_E$. Ce langage contient $\mathcal{L}$ sur la sorte $S_=$ (si $\mathcal{L}$ est déjà un langage multi-sorté, la sorte $S_=$ est en fait une union de sortes...). On définit alors la théorie T^{eq} qui contient* T *ramenée à la sorte $S_=$ et les formules $\forall \bar{x} \forall \bar{y}\ f_E(\bar{x}) = f_E(\bar{y}) \iff E[\bar{x},\bar{y}]$.*

À tout modèle $\mathcal{M}$ de T on associe $\mathcal{M}^{eq} \models T^{eq}$ en interprétant S_E par l'ensemble des classes d'équivalence de E et f_E par la surjection canonique.

La structure $\mathcal{M}^{eq}$ est alors, en quelque sorte la structure de $\mathcal{M}$ et de tous ses imaginaires.

Remarque 1.45 (Quelques propriétés de $\mathcal{M}^{eq}$) **:**

(i) *Soit $\varphi[x_1, \dots, x_n] \in \mathcal{L}^{eq}$, il existe alors $\psi[y_1, \dots y_n] \in \mathcal{L}$ tel que*

$$T^{eq} \vdash \varphi[f_{E_1}(y_i), \dots, f_{E_n}(y_n)] \iff \psi[y_1, \dots, y_n]$$

où S_{E_i} est la sorte de x_i.

(ii) *Si $\mathcal{M} \models T^{eq}$ et $N \subseteq M$ alors $\mathcal{N} \models T^{eq}$ si et seulement si $S_=(N) \models T$.*

(iii) *Si $\mathcal{N} \preccurlyeq \mathcal{M}$ alors $\mathcal{N}^{eq} \preccurlyeq \mathcal{M}^{eq}$.*

(iv) *Si T est modèle-complète alors T^{eq} l'est aussi. Néanmoins, en règle générale, si T élimine les quantificateurs, ce n'est pas forcément le cas de T^{eq}.*

(v) *T^{eq} élimine uniformément les imaginaires.*

Lemme 1.46 :
Soient $\mathcal{M}$ une $\mathcal{L}$-structure, X un ensemble définissable et $\bar{a} \in M$. Alors, X est codé par $\bar{a}$ si et seulement si $\mathrm{dcl}^{eq}(\bar{a}) = \mathrm{dcl}^{eq}(\langle X \rangle)$, où $\langle X \rangle$ est un code de X dans M^{eq} et X est faiblement codé par $\bar{a}$ si et seulement si $\langle X \rangle \in \mathrm{dcl}^{eq}(\bar{a})$ et $\bar{a} \in \mathrm{acl}^{eq}(\langle X \rangle)$.

Proof. Quitte à agrandir $\mathcal{M}$, on peut le supposer assez saturé et homogène. Si X est codé par $\bar{a}$, un automorphisme de $\mathcal{M}^{eq}$ fixe X et donc $\langle X \rangle$ si et seulement si il fixe $\bar{a}$ et on a donc bien que $\bar{a} \in \mathrm{dcl}^{eq}(\langle X \rangle)$ et $\langle X \rangle \in \mathrm{dcl}^{eq}(a)$. La réciproque est évidente.
Si X est faiblement codé par $\bar{a}$ via $\varphi[\bar{x}, \bar{y}]$, tout automorphisme qui fixe $\langle X \rangle$ et donc X ne peut envoyer $\bar{a}$ que sur l'un des $\bar{a}'$ en nombre fini tel que $\varphi[x, \bar{a}']$ définit aussi X et donc $\bar{a} \in \mathrm{acl}^{eq}(\langle X \rangle)$. Comme X est définissable sur $\bar{a}$ on a aussi bien sûr $\langle X \rangle \in \mathrm{dcl}^{eq}(\bar{a})$. Réciproquement, si $\langle X \rangle \in \mathrm{dcl}^{eq}(\bar{a})$, il existe $\varphi[x, \bar{a}]$ qui définit X. Si l'on note $p = \mathrm{tp}(\bar{a})$ et n la taille de son orbite au dessus de $\langle X \rangle$, par une compacité à peine plus compliquée que dans la proposition (**1.41**), il existe $\psi \in p$ tel que si on a n éléments distincts de M qui vérifient ψ et qui définissent X via $\varphi[\bar{x}, \bar{y}]$ alors l'un d'entre eux est $\bar{a}$. Il est alors facile de voir que X est codé faiblement pas $\bar{a}$ via $\varphi[\bar{x}, \bar{y}] \wedge \psi[\bar{y}]$. ∎

Enfin, montrons que ce qui fait la différence entre les codes et les codes faibles, c'est simplement la capacité de coder les ensembles finis.

Lemme 1.47 :
Soit $\mathcal{M}$ une $\mathcal{L}$-structure qui admet des codes pour les ensembles finis. Un ensemble définissable a alors un code si et seulement si il a un code faible.

Proof. Tout d'abord, il est évident qu'un code est aussi un code faible. Réciproquement, soit E l'ensemble fini des conjugués de $\bar{a}$ au dessus de $\langle X \rangle$ (un code dans $\mathcal{M}^{eq}$) et $\sigma \in \mathrm{Aut}(M^{eq}/\langle X \rangle)$. Comme σ fixe $\langle X \rangle$, on a $\sigma(X) = X$, i.e. $\varphi[\mathcal{M}, \sigma(\bar{a})] = X$. Il s'en suit donc que pour tout $\bar{a}' \in E$, $\varphi[x, \bar{a}']$ défini X. Tout automorphisme qui fixe X envoie un conjugué de a au dessus de $\langle X \rangle$ sur un conjugué de a au dessus de $\langle X \rangle$ et donc fixe E. Réciproquement, tout automorphisme

qui fixe globalement E fixe X comme on vient de le démontrer. Tout code de E est donc un code de X. ■

Exemple 1.48 :

(i) *La théorie des corps algébriquement clos élimine uniformément les imaginaires. C'est l'exemple qui a motivé la définition de cette notion dans [Poi83]. La théorie des corps réels clos élimine aussi uniformément les imaginaires.*

(ii) $\mathrm{Th}(\mathbb{Q},<)$ *élimine les imaginaires, mais pas uniformément. Soit* $\varphi[x,y,y'] := y = y'$*, on a alors* $\varphi[\mathcal{M},a,b] = M$ *ou* $\varnothing$*. Si le codage était uniforme, il existerait* $\theta[x,\bar{z}]$ *et deux uplets* $\bar{c}_1$ *et* $\bar{c}_2$ *tels que* $\theta[\mathcal{M},\bar{c}_1] = M$ *et* $\theta[\mathcal{M},\bar{c}_2] = \varnothing$ *et ce sont les seuls à vérifier ces deux propriétés. Mais* $\bar{c}_1$ *serait alors définissable sur le vide et* $\bar{c}_2$ *aussi, or* $\mathrm{Th}(\mathbb{Q},<)$ *ne contient aucune constante. On a donc (si le langage n'a qu'une sorte) une réciproque du lemme (**1.39**).*

(iii) *La théorie de l'ensemble infini élimine faiblement les imaginaires. Elle ne les élimine que faiblement car les ensembles finis ne sont pas codés. De plus, pour des raisons semblables à celles de l'exemple précédent l'élimination ne peut pas être uniforme sinon* $\mathrm{acl}(\varnothing)$ *ne serait pas vide.*

Soit T une théorie dans un langage $\mathcal{L}$ multi-sorté. On dit que T a des sortes dominantes $(S_i)_{i\in I}$ si pour toute sorte de $\mathcal{L}$, il existe une fonction $\varnothing$-définissable d'un produit des S_i qui soit surjective sur S. Pour tout modèle $\mathcal{M} \models T$, on note alors $\mathrm{dom}(M) = \bigcup_{i\in I} S_i(\mathcal{M})$.
Prouvons maintenant un critère d'élimination des imaginaires qui a été introduit dans [HHMo6, Remarque 3.2.2] et qui sera utile par la suite.

Lemme 1.49 (Critère d'élimination des imaginaires) **:**
Soit T *une* $\mathcal{L}$*-théorie qui admet suffisamment de constantes, si pour tout* $\mathcal{M} \models T$ *et toute fonction* $f : S \to M^n$ M*-définissable (totale) telle que* S *soit une sorte dominante, le graphe de* f *a un code, alors* T *admet l'élimination des imaginaires.*

Proof . Soit R une relation M-définissable sur $\prod_{i=1}^n S_i$. Il existe une fonction définissable sans paramètres (et donc fixée par tout automorphisme) $f : \prod_{j=1}^m T_i \to \prod_{i=1}^n S_i$, où les T_i sont des sortes dominantes. De plus, si c_1 et c_2 sont deux constantes d'une même sorte et qu'on pose χ_R la fonction qui vaut c_1 sur R et c_2 ailleurs, un code de R est exactement un code de $\chi_R \circ f$. Il suffit donc de démontrer que toute fonction $f : \prod_{i=1}^n S_i \to M$, où les S_i sont dominantes, a un code.
Pour cela, procédons par induction sur n. Si $n = 1$ c'est exactement notre hypothèse. Sinon supposons qu'on ait démontré que la propriété est vraie pour n et considérons $f : \prod_{i=1}^{n+1} S_i \to M$ définie par la formule $\varphi[x_1,\dots,x_{n+1},y,\bar{m}]$, où $\bar{m} \in M$. Pour tout $c \in S_1$, on pose $f_c : x_2 \dots x_{n+1} \mapsto f(c,x_2,\dots,x_n)$. Par récurrence, tous les f_c sont codés et comme tous les f_c sont définis par la formule φ avec différents paramètres, on peut supposer que ce codage est uniforme. Il existe donc $\theta[x_2,\dots,x_n,y,\bar{t}]$ tel que, pour tout c, il existe un unique $\langle f_c\rangle$ tel que $\theta[x_2,\dots,x_n,y,\langle f_c\rangle]$ définit f_c. La formule $\forall x_2 \dots x_n y\ (\theta[x_2,\dots,x_n,y,\forall t] \iff \varphi[c,x_2,\dots,x_n,y,\bar{m}])$ définit donc une fonction $g : S_1 \to M^m$. Par hypothèse elle est donc codée par un élément $\langle g\rangle \in M$.

Vérifions alors que $\langle g \rangle$ code aussi f. Supposons que $\langle g \rangle$ code g via $\chi[x_1, \bar{t}, \bar{s}]$. Quitte à remplacer $\chi[x_1, \bar{t}, \bar{s}]$ par « $\chi[x_1, \bar{t}, \bar{s}]$ définit une fonction totale » $\wedge \chi[x_1, \bar{t}, \bar{s}]$, on peut supposer que pour tout m $\chi[x_1, \bar{t}, \bar{m}]$ est soit vide, soit définit une fonction totale. La formule $\psi[\bar{x}, y, \langle g \rangle] = \exists \bar{t}\, \theta[x_2, \dots, x_n, y, \bar{t}] \wedge \chi[x_1, \bar{t}, \langle g \rangle]$ définit alors f. En effet, si $(\bar{x}, y) \in f$, cette formule est vérifiée pour $\bar{t} = \langle f_{x_1} \rangle$. Réciproquement, si $(\bar{x}, y)$ vérifie cette formule, comme g est une fonction, on a alors forcément $\bar{t} = \langle f_{x_1} \rangle$ et donc $(x_2 \dots x_n y) \in f_{x_1}$, i.e. $(\bar{x}, y) \in f$. Enfin, si $\bar{m} \neq \langle g \rangle$, soit $\chi[x, y, \bar{m}]$ définit l'ensemble vide et donc ψ aussi, soit elle définit une fonction $g_{\bar{m}}$, mais il existe alors $c_1 \in M$ tel que $g_{\bar{m}}(c_1) \neq g(c_1) = \langle f_{c_1} \rangle$. Il y a alors deux cas possibles. Soit il existe $(c_2 \dots c_n, d) \notin f_{c_1}$, i.e. $(\bar{c}, d) \notin f$, tel que $\mathcal{M} \vDash \theta[c_2, \dots, c_n, d, g_m(c_1)]$. On a alors $\mathcal{M} \vDash \psi[c, d, \bar{m}]$ mais $(c, d) \notin f$. Soit il existe $(c_2 \dots c_n)$ tel qu'il n'existe pas de d tel que $\mathcal{M} \vDash \theta[c_2, \dots, c_n, d, g_m(c_1)]$, mais alors $\psi[\bar{c}, \mathcal{M}, \bar{m}]$ est l'ensemble vide. Comme f est totale, $\psi[\bar{x}, y, \bar{m}]$ ne peut pas définir f. On a donc que f est codé par $\langle g \rangle$ via $\psi[\bar{x}, y, \bar{z}]$. ■

Prouvons maintenant un théorème de [HM08] qui permet de déduire l'élimination des imaginaires dans une théorie en utilisant une autre théorie qui les élimine. C'est le théorème qui sera utilisé pour montrer l'élimination des imaginaires dans la théorie de $\mathbb{Q}_p$ en utilisant les corps valués algébriquement clos. On a cependant besoin pour la preuve de la notion de germe que l'on commence donc par définir.

Définition 1.50 (Germe) **:**
Soient $\mathcal{M}$ une $\mathcal{L}$-structure, f une fonction M-définissable définie par $\varphi[\bar{x}, \bar{y}, \bar{m}]$, où $\bar{m} \in M$ et $p \in S(M)$ un type tel que f soit définie sur p. On note $\partial_p f$ la classe d'équivalence de f pour la relation d'équivalence $E(m, m') := (\forall \bar{y},\ \varphi[\bar{x}, \bar{y}, \bar{m}] = \varphi[\bar{x}, \bar{y}, \bar{m}'] \in p)$, i.e. l'ensemble des fonctions qui coïncident avec f sur une réalisation de p dans une extension élémentaire de $\mathcal{M}$.
Si le type p est définissable, cette relation d'équivalence est définissable et si, de plus, $\mathrm{Th}(\mathcal{M})$ élimine les imaginaires, $\partial_p f$ est un point.
Dans tous les cas, si on a $A \subseteq M$ tel que p est $\mathrm{Aut}(\mathcal{M}/A)$-invariant, on peut parler de l'action de $\mathrm{Aut}(\mathcal{M}/A)$ sur $\partial_p f$ (même si ce n'est pas un point), en posant $\sigma(\partial_p f) = \partial_p \sigma(f)$.

La preuve nécessite aussi un lemme combinatoire sur les groupes d'automorphismes d'un modèle assez saturé et homogène qui découle du lemme de Neumann.

Lemme 1.51 (Lemme de Neumann) **:**
Soient G un groupe et $(g_i H_i)_{i=1\dots n}$ des translatés de sous-groupes de G tels que :

$$G = \bigcup_{i=1\dots n} g_i H_i,$$

alors l'un des H_i au moins est d'indice fini.

Ce lemme est énoncé et prouvé dans [Neu54, Lemma 4.1, p. 239].

Corollaire 1.52 :
Soient M un modèle assez universel et homogène et $(e_i)_{i \in \mathbb{N}}$ une famille de points telle que tout automorphisme de M fixe tous les e_i sauf un nombre fini. Il y a alors au plus un nombre fini de e_i qui ont une orbite infinie sous l'action des automorphismes de M.

Proof. Supposons par l'absurde qu'il y ait une infinité de e_i qui ont une orbite infinie et montrons qu'il existe alors un automorphisme qui ne fixe aucun de ces e_i. Quitte à en oublier,

on peut supposer qu'ils ont tous une orbite infinie. Montrons tout d'abord que pour tout ensemble fini de e_i il existe des automorphismes qui n'en fixent aucun. Soient donc $e_{i_1}, \dots e_{i_n}$ et supposons que tout automorphisme de $\mathcal{M}$ en fixe au moins un. Si on note H_j le stabilisateur de e_j dans G, on a alors $G = \bigcup_j H_j$, mais comme tous ces sous-groupes sont d'indice infini (leur indice est égal au cardinal de l'orbite du e_i correspondant), on a une contradiction par le lemme de Neumann (voir (**1.51**)).
Notons alors $p_i = \mathrm{tp}(e_i/e_{j<i})$. L'ensemble de formules $\bigcup p_i[c_i] \cup \bigcup p_i[d_i]\{c_i \neq d_i\}$ est alors finiment satisfaisable dans $\mathcal{M}$. En effet, il suffit de prendre $c_i = e_i$ pour tous les i qui apparaissent et si σ est un automorphisme qui ne fixe aucun des e_i qui apparaissent, de prendre $d_i = \sigma(e_i)$. Soit alors $\mathcal{N}$ un modèle (petit) dans lequel cet ensemble est satisfaisable. Par universalité, $N \subseteq M$ et on a une application élémentaire qui envoie $c_i^{\mathcal{N}}$ sur e_i. On peut l'étendre en un automorphisme de $\mathcal{M}$ et on a alors une application élémentaire qui envoie $\sigma(c_i^{\mathcal{N}}) = e_i$ sur $\sigma(d_i^{\mathcal{N}})$. Comme $c_i^{\mathcal{N}} \neq d_i^{\mathcal{N}}$ et que σ est injective, cette dernière application élémentaire s'étend en un automorphisme de $\mathcal{M}$ qui ne fixe aucun des e_i, ce qui est absurde. ■

Proposition 1.53 :
Soient $\widetilde{\mathcal{L}} \subseteq \mathcal{L}$ deux langages, $\widetilde{T}$ une $\widetilde{\mathcal{L}}$-théorie complète qui admet l'élimination des quantificateurs (en conséquence, toutes les $\widetilde{\mathcal{L}}$-formules considérées seront sans quantificateurs) et l'élimination uniforme des imaginaires, T une $\mathcal{L}$-théorie complète telle que $\widetilde{T}_\forall \subseteq T$ (i.e. tout modèle de T se plonge en tant que $\widetilde{\mathcal{L}}$-structure dans un modèle de $\widetilde{T}$) qui admet assez de constantes.
Soient $\mathcal{M} \models T$ suffisamment saturé et homogène et $\widetilde{\mathcal{M}} \models \widetilde{T}$ tel que $\mathcal{M}_{|\widetilde{\mathcal{L}}}$ est une sous-structure de $\widetilde{\mathcal{M}}$ (quitte à le grossir, on peut également le supposer suffisamment saturé et homogène). On note $\mathrm{dcl}_{\widetilde{\mathcal{L}}}$ la clôture définissable par des $\widetilde{\mathcal{L}}$-formules sans quantificateurs dans $\widetilde{\mathcal{M}}$ et $\mathrm{dcl}_{\mathcal{L}}$ la clôture définissable par des $\mathcal{L}$-formules dans $\mathcal{M}^{\mathrm{eq}}$. De même pour $\mathrm{acl}_{\mathcal{L}}$, $\mathrm{acl}_{\widetilde{\mathcal{L}}}$, $\mathrm{tp}_{\mathcal{L}}$ et $\mathrm{tp}_{\widetilde{\mathcal{L}}}$[1].
On suppose alors que :

(i) *pour tout $\mathcal{M}' \preccurlyeq \mathcal{M}$ et $c \in \mathrm{dom}(M)$, $\mathrm{dcl}_{\mathcal{L}}(M'c) \cap M \subseteq \mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c)$;*

(ii) *pour tout $A \subseteq M$ tel que $A = \mathrm{acl}_{\mathcal{L}}(A)$ et $c \in \mathrm{dom}(M)$, $\mathrm{acl}_{\mathcal{L}}(Ac) \cap M \subseteq \mathrm{dcl}_{\mathcal{L}}(Ac) \cap M$;*

(iii) *soit $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$, il existe $e' \in M$ tel que tout $\widetilde{\mathcal{L}}$-automorphisme de $\widetilde{\mathcal{M}}$ qui fixe globalement M, fixe e si et seulement si il fixe e' ;*

(iv) *tout ensemble $X \subseteq \mathrm{dom}(M)$ M-définissable*[2] *a un code dans M ;*

(v) *soient $c \in \mathrm{dom}(M)$ et $A \subseteq M$ tel que $\mathrm{acl}_{\mathcal{L}}(A) \cap M = A$. Il existe un type $\widetilde{p} \in S_{\widetilde{\mathcal{L}}}(\widetilde{M})$ $\mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A)$-invariant tel que $\widetilde{p}|M$ soit consistant avec $\mathrm{tp}_{\mathcal{L}}(c/A)$ et que pour toute fonction r $\widetilde{\mathcal{L}}_{\widetilde{M}}$-définissable on ait :*
(*) il existe $(e_i)_{i\in\mathbb{N}} \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$ tel que $\sigma \in \mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A)$ fixe $\partial_{\widetilde{p}} r$ si et seulement si σ fixe tous les e_i sauf un nombre fini ;
(**) soit $B \supseteq A$ tel que $B = \mathrm{acl}_{\widetilde{\mathcal{L}}}(B)$ et $\partial_{\widetilde{p}} r$ est fixé par $\mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/B)$, il existe alors une fonction $\widetilde{\mathcal{L}}_B$-définissable h qui a le même germe sur $\widetilde{p}$ que r.

La théorie T élimine alors les imaginaires.

1. Il faut cependant faire attention que M^{eq} n'est pas, a priori, inclus dans $\widetilde{M}$ et donc que pour $A \subseteq M$, $\mathrm{dcl}_{\mathcal{L}}(A)$ et $\mathrm{acl}_{\mathcal{L}}(A)$ ne sont pas inclus dans $\widetilde{M}$.
2. Cette propriété est alors aussi vraie pour les ensembles M^{eq}-définissables

Proof. Commençons par remarquer une conséquence immédiate de la condition (iii).

Lemme 1.54 :
Les ensembles finis sont codés dans $M \models T$.

Proof. Soit $E \subseteq M^n$ un ensemble fini. Comme E est définissable (avec l'égalité et sans quantificateurs) sur M, il l'est aussi dans $\widetilde{\mathcal{M}}$. Soit e un code dans $\widetilde{\mathcal{M}}$, on a alors que $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$ et soit $e' \in M$ donné par (iii). Soit alors $\sigma \in \mathrm{Aut}_{\mathcal{L}}(M)$, c'est alors aussi une $\widetilde{\mathcal{L}}$-application élémentaire qui peut donc s'étendre en $\widetilde{\sigma} \in \mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}})$. On a alors que σ fixe E si et seulement si $\widetilde{\sigma}$ fixe E (car $E \subseteq M$) si et seulement si $\widetilde{\sigma}$ fixe e, si et seulement si $\widetilde{\sigma}$ fixe e' (par définition car $\widetilde{\sigma}$ laisse M globalement invariant), si et seulement si σ fixe e' (car $e' \in M$). ✠

Revenons maintenant à la preuve de l'élimination des imaginaires. Par le lemme (**1.49**) il suffit de montrer que le graphe d'une fonction $\mathcal{L}_M$-définissable $f : \mathrm{dom}(M) \to M^n$ est codé. Par les lemmes (**1.47**) et (**1.54**), il suffit de montrer qu'il est faiblement codé. On pose $A' = \mathrm{acl}_{\mathcal{L}}(\langle f \rangle)$ et $A = A' \cap M$ où $\langle f \rangle$ est pris dans M^{eq}. Il suffit alors de montrer que f est A-définissable, par le lemme (**1.46**).

Lemme 1.55 :
Il existe une relation $R[x, \bar{y}]$ $\widetilde{\mathcal{L}}_M$*-définissable telle que, pour tout* $c \in \mathrm{dom}(M)$, $R(c) = \{\bar{d} \in \widetilde{M} : \widetilde{\mathcal{M}} \models R[c, \bar{d}]\}$ *est fini et* $f(c) \in R(c)$.

Avant de démontrer ce lemme, remarquons que, comme R est définie sans quantificateurs, pour tout $c, \bar{d} \in M$, $\mathcal{M} \models R[c, \bar{d}]$ si et seulement si $\widetilde{\mathcal{M}} \models R[c, \bar{d}]$. En particulier pour tout $c \in \mathrm{dom}(M)$, $\{\bar{d} \in M : \mathcal{M} \models R[c, \bar{d}]\}$ est aussi fini.

Proof. Soit $\mathcal{M}' \preccurlyeq \mathcal{M}$ (petit) tel que f soit M'-définissable et soit $\varphi[x, \bar{y}]$ une $\mathcal{L}_{M'}$-formule qui la définit, alors pour tout c, par (i), $f(c) \in \mathrm{dcl}_{\mathcal{L}}(M'c) \cap M \subseteq \mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c)$. Considérons alors l'ensemble de formules suivant :

$$\Sigma[x, \bar{y}] = \{\varphi[x, \bar{y}]\} \cup \{\neg\psi[x, \bar{y}] \in \widetilde{\mathcal{L}}_{M'} : \widetilde{\mathcal{M}} \models \forall x \exists^{\leqslant n} \bar{y}\ \psi[x, \bar{y}] \text{ pour un } n \in \mathbb{N}\}.$$

Il est évident que cet ensemble de formules n'est pas satisfaisable dans $\mathcal{M}$ car pour toute formule $\psi[x, \bar{y}] \in \widetilde{\mathcal{L}}_{M'}$ (sans quantificateurs donc) et $c, \bar{d} \in \mathrm{Mod}$, $\mathcal{M} \models \psi[c, \bar{d}]$ si et seulement si $\widetilde{\mathcal{M}} \models \psi[c, \bar{d}]$. Par compacité, il existe donc $(\psi_i)_{i=1\ldots N} \in \widetilde{\mathcal{L}}_{M'}$ telles que $\mathcal{M} \models \forall x \bar{y}\ \varphi[x, \bar{y}] \Rightarrow \bigvee_i \psi_i[x, \bar{y}]$ et que, par définition, il existe n tel $\widetilde{\mathcal{M}} \models \forall x \exists^{\leqslant n} \bar{y}\ \bigvee_i \psi_i[x, y]$. ✠

Lemme 1.56 :
Soient $c \in \mathrm{dom}(M)$ *et* $p = \mathrm{tp}_{\mathcal{L}}(c/A)$. *Il existe alors une fonction* g A*-définissable telle que* f *et* g *coïncident sur toute réalisation de* p *et* $\{x : f(x) = g(x)\}$ *est* A*-définissable.*

Proof. Soit $\widetilde{p}$ le type $\mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A)$-invariant qui étend p donné par (ν). Pour tout R comme au lemme (**1.55**), on a alors $\exists^{=n} \bar{y}\ R[x, \bar{y}] \in \widetilde{p}$ pour un certain n. Ainsi, le cardinal de $R(x)$ est constant sur l'ensemble des réalisations de $\widetilde{p}$. On choisit alors un R comme au lemme (**1.55**) tel que le cardinal de $R(x)$ sur une réalisation de $\widetilde{p}$ soit minimal (parmi tous les R qui vérifient le lemme (**1.55**)) et on note $r : x \mapsto \langle R(x) \rangle$ (une telle fonction existe car $\widetilde{T}$ admet l'élimination uniforme des imaginaires). Soit alors $\sigma \in \mathrm{Aut}_{\mathcal{L}^{eq}}(\mathcal{M}^{eq}/A')$, $\sigma_{|M}$ est alors aussi une $\widetilde{\mathcal{L}}$-application élémentaire qui peut donc s'étendre à $\tilde{\sigma} \in \mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A)$ qui fixe globalement M. Comme σ fixe A', il fixe f et donc $\tilde{\sigma}$ le fixe aussi. De plus, pour tout $x \in \widetilde{M}$, $\tilde{\sigma}(R)(x)$

est fini (de même cardinal que $R(x)$) et donc $\tilde{\sigma}(R)$ vérifie aussi la conclusion du lemme (**1.55**). Il est alors facile de voir que la relation $R \wedge \tilde{\sigma}(R)$ vérifie aussi la conclusion de ce lemme et donc, comme R a été choisi de cardinal minimal sur les réalisations de $\widetilde{p}$, pour tout $x \vDash \widetilde{p}$, on a $R(x) = R(x) \cap \tilde{\sigma}(R)(x)$ et donc $R(x) = \tilde{\sigma}(R)(x)$ car ils ont le même cardinal. Comme il est évident que $\tilde{\sigma}(r)(x)$ code $\tilde{\sigma}(R)(x)$, il s'en suit que $\tilde{\sigma}(\partial_{\widetilde{p}} r) = \partial_{\widetilde{p}} \tilde{\sigma}(r) = \partial_{\widetilde{p}} r$.
Considérons alors les $e_i \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$ comme dans le $(*)$ et pour tout i, le $e'_i \in M$ donné par le (iii). On a montré que toute extension (au sens décrit ci-dessus) $\tilde{\sigma}$ à $\widetilde{\mathcal{M}}$ d'un $\sigma \in \mathrm{Aut}_{\mathcal{L}^{eq}}(M^{eq}/A')$ fixe $\partial_{\widetilde{p}} r$; $\tilde{\sigma}$ doit donc fixer tout les e_i sauf un nombre fini, par définition des e_i et donc tous les e'_i sauf un nombre fini, par définition des e'_i. Par le corollaire (**1.52**) (appliqué dans le modèle $\mathcal{M}^{eq}_{A'}$), tous les e'_i sauf un nombre fini ont une orbite finie, i.e. il existe I_0 fini tel que $i \notin I_0$ implique $e'_i \in \mathrm{acl}_{\mathcal{L}}(A') = A'$, de plus comme $e'_i \in M$, on a alors $e'_i \in A = A' \cap M$.
Pour tout $x \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$, l'action de $\mathrm{Aut}_{\mathcal{L}}(M)$ sur x est bien définie car toute extension de $\sigma \in \mathrm{Aut}_{\mathcal{L}}(M)$ à $\widetilde{\mathcal{M}}$ donnera la même image à x. Posons alors $A^* = \{x \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M) : x \text{ est fixé par } \mathrm{Aut}_{\mathcal{L}}(\mathcal{M}/A)\}$. Pour $i \notin I_0$, comme $e'_i \in A$, on a (par définition de e'_i), $e_i \in A^*$. Tout automorphisme de $\mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A^*)$ fixe donc tous les e_i qui ne sont pas dans I_0, i.e. tous sauf un nombre fini. Il s'en suit donc que $\partial_{\widetilde{p}} r$ est fixé par $\mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A^*)$. Par l'hypothèse $(**)$, il existe s $\widetilde{\mathcal{L}}_{\mathrm{acl}_{\widetilde{\mathcal{L}}}(A^*)}$-définissable qui a le même germe que r au dessus de $\widetilde{p}$.
Comme $r(c)$ est un code de $R(c)$, il existe $\varphi[\bar{y}, \bar{z}] \in \widetilde{\mathcal{L}}$ telle que pour tout $c \in \widetilde{M}$ $R(c) = \varphi[\widetilde{\mathcal{M}}, r(c)]$. Soit alors la relation S définie par $\varphi[\bar{y}, s(x)] \in \widetilde{\mathcal{L}}_{\mathrm{acl}(A^*)}$. Quitte à remplacer S par l'union de ses conjugués au dessus de A^*, on peut supposer que S est A^* définissable et que pour tout $t \vDash \widetilde{p}|M$, $S(t)$ est fini et contient $R(t)$. Comme tout isomorphisme de $\mathrm{Aut}_{\mathcal{L}}(\mathcal{M}/A)$ fixe A^* et donc S, il s'en suit que $S \cap M$ est $\mathrm{Aut}_{\mathcal{L}}(\mathcal{M}/A)$-invariant. Il suffit donc de montrer que c'est un ensemble définissable (dans $\mathcal{M}$) pour savoir qu'il est A-définissable. Mais comme S est A^*-définissable, il existe $\psi[x, \bar{y}, \bar{a}] \in \widetilde{\mathcal{L}}$, où $\bar{a} \in A^*$, qui définit S. De plus, comme $\bar{a} \in A^* \subseteq \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$, il existe $\theta[\bar{z}, \bar{t}] \in \widetilde{\mathcal{L}}$ et $\bar{m} \in M$ tels que $\theta[\widetilde{\mathcal{M}}, \bar{m}] = \{\bar{a}\}$. La formule $\exists \bar{z}\, \theta[\bar{z}, \bar{m}] \wedge \psi[x, \bar{y}, \bar{z}]$ définit donc S et est équivalente à une formule sans quantificateurs $\chi[x, \bar{y}, \bar{t}]$. Cette formule définit donc, dans $\mathcal{M}$, l'ensemble $S \cap M$ que l'on peut donc supposer A-définissable. Soit alors $c \vDash \widetilde{p}|B \cup p$ (qui existe par hypothèse) où $B \subseteq M$ est tel B contienne A et r soit défini sur B. On a alors $R(c) \subseteq S(c)$ et donc $f(c) \in S(c) \cap M$. Il s'en suit que $f(c) \in \mathrm{acl}_{\mathcal{L}}(Ac) = \mathrm{dcl}_{\mathcal{L}}(Ac)$ par (ii). Il existe donc g $\mathcal{L}_A$-définissable telle que $g(c) = f(c)$. On pose alors $E = \{x \in M : f(x) = g(x)\}$. C'est un ensemble unaire qui est A'-définissable. Par (iv), il a un code $e \in \mathcal{M}$, mais alors $e \in \mathrm{dcl}_{\mathcal{L}}(A') = A'$ et donc $e \in A = A' \cap M$, i.e. E est A-définissable. Comme $c \in E$ et $c \vDash p$, on a bien $E \in p$ et donc $\partial_p f = \partial_p g$. ✠

Revenons donc à la preuve de la proposition et montrons que f est A-définissable. Comme $\mathcal{M}$ est saturé, tout $p \in S_1(A)$ tel que son unique variable est dans les sortes dominantes, est de la forme $\mathrm{tp}_{\mathcal{L}}(c/A)$ pour $c \in \mathrm{dom}(M)$. Par le lemme (**1.56**), si g_p est la fonction A-définissable telle que $\partial_p f = \partial_p g_p$ et l'ensemble $\{x : f(x) = g_p(x)\}$ est A-définissable, on a $S_1(A) = \bigcup_{p \in S_1(A)} [f(x) = g_p(x)]$ (où $[\varphi]$ est l'ouvert engendré par φ). Par compacité, il existe donc $(D_i : 1 \leqslant i \leqslant n)$ des ensembles A-définissables et $(g_i : 1 \leqslant i \leqslant n)$ des fonctions A-définissables telles que f coïncide avec g_i sur D_i et les D_i recouvrent M. Il s'en suit bien que f est A-définissable. ■

1.5 Sortes géométriques

Dans [HHM06], il est démontré que la théorie $\mathrm{ACVF}_{(m,n)}$ élimine (uniformément) les imaginaires si l'on rajoute certaines sortes de réseaux. Le but de cette section est de rappeler la définition de ces sortes et le langage dans lequel on à la fois élimination des imaginaires et des quantificateurs.

Définition 1.57 (Réseaux) **:**
Soit (K, v) *un corps valué. On note* $\mathcal{S}_n(K)$ *l'ensemble des sous-*$\mathcal{O}_K$*-modules de* K^n *libres de rang* n*. Un élément de* $\mathcal{S}(K) = \bigcup_{n\geqslant 1} \mathcal{S}_n(K)$ *est appelé un réseau de* K*.*

Un réseau de K a donc une base $e_1 \dots e_n$ dans K. Deux bases engendrent le même réseau s'il existe une matrice dans $\mathrm{GL}_n(\mathcal{O}_K)$ qui conjugue ces deux bases. On a donc $\mathcal{S}_n(K) \simeq \mathrm{GL}_n(K)/\mathrm{GL}_n(\mathcal{O}_K)$. Il s'en suit donc que pour tout n, $\mathcal{S}_n$ est bien une sorte de K^{eq}. De plus l'ensemble S_1 n'est rien d'autre que l'ensemble des boules fermées centrées en 0 de rayon fini appartenant à K. On a donc $S_1(K) \simeq \Gamma_K$. D'ailleurs, la surjection canonique $K^\star \to S_1(K) \simeq \mathrm{GL}_1(K)/\mathrm{GL}_1(\mathcal{O}_K) = K^\star/\mathcal{O}_K^\star = \Gamma_K$ est v.
On peut aussi remarquer que la sorte $\mathcal{S}$ contient des codes non seulement pour les réseaux mais aussi pour tous les translatés de réseaux :

Lemme 1.58 :
Soient (K, v) *un corps valué,* $s \in \mathcal{S}_n(K)$ *et* $a \in K$*. Le sous-*$\mathcal{O}_K$*-module de* K^{n+1} *engendré par* $(a + s) \times \{1\}$ *est un réseau et il code* $a + s$*.*

Proof. Soit $(e_1, \dots, e_n)$ une base de s. On pose $e_0 = 0$, la famille des $(a + e_i, 1)$ est alors une base du sous-$\mathcal{O}_K$-module de K^{n+1} engendré par $(a + s) \times \{1\}$, que l'on notera $h(a + s)$. Supposons que l'on ait $\sum_i \lambda_i(a + e_i, 1) = 0$, où $\lambda_i \in \mathcal{O}_K$. On a alors $(\sum_i \lambda_i a + \sum_{i\geqslant 1} \lambda_i e_i, \sum_i \lambda_i) = (0, 0)$. Il s'en suit donc que $\sum_i \lambda_i = 0$ et donc $\sum_{i\geqslant 1} \lambda_i e_i = 0$. Or c'est une famille libre donc pour tout $i \geqslant 1$, $\lambda_i = 0$ et donc, $\lambda_0 = 0$. Pour ce qui est du fait que ce soit une famille génératrice, tout élément de $h(a+s)$ est de la forme $x = \sum_i \lambda_i(a+x_i, 1)$, où $x_i \in s$. En particulier, $x_i = \sum_{j\geqslant 1} \mu_j^i e_j$. On a donc $x = \sum_i \lambda_i(a+e_0, 1)+\sum_{i,j} \lambda_i\mu_j(e_j, 0)$. Or $(e_j, 0) = (a+e_j, 1)-(a+e_0, 1)$ et donc x est bien combinaison linéaire des $(a + e_i, 1)$.
Le module $h(a+s)$ est donc bien un réseau. De plus, $h(a+s)\cap K^n\times\{1\} = (a+s)\times\{1\}$. En effet, si $x \in h(a+s)\cap K^n\times\{1\}$, il existe $\lambda_i \in \mathcal{O}_K, x_i \in s$ et $y \in K^n$ tels que $\sum_i \lambda_i(a+x_i, 1) = (y, 1) = x$. Il s'en suit que $\sum_i \lambda_i = 1$ et donc $y = \sum_i \lambda_i a + \sum_i \lambda_i x_i = a + \sum_i \lambda_i x_1 \in a + s$. L'inclusion réciproque est évidente. Il s'en suit donc que h est une fonction $\varnothing$-définissable qui injecte les translatés d'éléments de S_n dans S_{n+1}, i.e. $a + s$ est codé par $h(a + s)$ via la fonction qui définit h. ∎

On en déduit immédiatement que l'ensemble des boules fermées dont le rayon est dans Γ_K s'injecte dans $S_2(K)\cup K$. En effet l'ensemble des boules fermées de rayon infini est exactement K. Pour ce qui est des boules fermées de rayon fini, ce sont des translatés de boules centrées en 0, i.e. d'éléments de S_1, par le lemme précédent, ils s'injectent bien dans S_2.

Définition 1.59 (Torseurs) **:**
Soit (K, v) *un corps valué. On pose* $\mathcal{T}_n(K) = \bigsqcup_{s\in\mathcal{S}_n(K)} s/(\mathfrak{M}\, s)$*. Un élément de* $\mathcal{T}(K) = \bigcup_{n\geqslant 1} \mathcal{T}_n(K)$ *est appelé un torseur de* K*.*

Il est clair que $\mathcal{T}$ vit aussi dans K^{eq} vu que ses points sont des classes de congruences d'un réseau s (qui est bien un ensemble définissable) par $\mathfrak{M}$ s qui est bien un sous-groupe définissable.
De plus, comme $k_K = \mathcal{O}_K/\mathfrak{M}_K$ et que $\mathcal{O}_K$ est évidemment un réseau de rang 1, il s'en suit que $k_K \subseteq \mathcal{T}_1(K)$. L'application res est aussi définissable car c'est celle qui à $a \in \mathcal{O}_K$ associe sa classe dans $\mathcal{O}_K/\mathfrak{M}_K$.
Pour pouvoir définir le langage dans lequel on a à la fois élimination des imaginaires et élimination des quantificateurs pour $ACVF_{m,n}$, il faut introduire une dernière notion, celle de base générique. Il faut cependant commencer par montrer le lemme suivant :

Lemme 1.60 :
Soient (K, v) *un corps valué algébriquement clos,* $A \subseteq K$ *et* a *un élément générique de* k_K *au-dessus de* A *(au sens de la stabilité). Tous les* $b \in \mathcal{O}_K$ *tels que* $\mathrm{res}(b) = a$ *ont alors le même type.*

Proof. Quitte à agrandir K, on peut le supposer assez saturé. Soient b et c tels que $\mathrm{res}(b) = a = \mathrm{res}(c)$, i.e. en se rappelant que a est un translaté de $\mathfrak{M}_K$, b et c sont dans a. S'ils n'ont pas le même type sur A, il existe un ensemble A-définissable $X \subseteq \mathcal{O}_K$ tel que $b \in X$ et $c \notin X$. Mais alors pour tout a' générique dans k_K au-dessus de A (on peut en construire une infinité en prenant un élément générique au-dessus de ceux que l'on a déjà construits), il existe b' et c' dans a' tels que $b' \in X$ et $c' \notin X$. Mais cela contredit le fait que X est A-définissable. En effet, on aurait alors, par la proposition (**1.36**), $X = \bigcup_{i=1}^{n}(t_i \setminus (\bigcup_{j=1}^{m_i} t_i^j))$, où les t_i et t_i^j sont des translatés de sous-$\mathcal{O}$-modules de $\mathcal{O}$, i.e. des idéaux. Si t_i est un translaté d'un idéal strict de $\mathcal{O}$, il est contenu dans un translaté de $\mathfrak{M}$ et ne peut donc contenir qu'un seul des b'. On doit donc avoir $i = 1$ et $t_1 = \mathcal{O}$. Mais pour la même raison on ne peut alors pas éviter tous les c' sans avoir $t_1^j = \mathcal{O}$ et donc $X = \varnothing$, ce qui est absurde. ∎

Définition 1.61 (Base générique) **:**
Soient K *un corps valué algébriquement clos,* $A \subseteq K^{eq}$ *et* $s \in \mathcal{S}_n(A)$. *Si l'on note* $\mathrm{res}(s) = s/\mathfrak{M}s$, $\mathrm{res}(s)^n$ *est définissablement isomorphe à* k^{n^2}. *Comme* k *est un pur corps algébriquement clos, cet ensemble est de degré* 1 *et a donc un type générique* $q_{\mathrm{res}(s)^n}$, *qui est l'unique type de rang maximal de l'ensemble. Soit alors* q_s *tel que pour tout* $(\bar{a}_1 \dots \bar{a}_n)$, *on a* $(\bar{a}_1 \dots \bar{a}_n) \vDash q_s$ *si et seulement si* $(\mathrm{res}(\bar{a}_1) \dots \mathrm{res}(\bar{a}_n)) \vDash q_{\mathrm{res}(s)^n}$, *où* $\mathrm{res}(\bar{a}_i) = \bar{a}_i + \mathfrak{M}s$.
Soit $B \subseteq A$, *une base générique de* s *au-dessus de* B *est une réalisation de* $q_s|B$.

Cette définition a un sens car $\mathrm{res}(\bar{a}_i)$ est générique au-dessus de $A\bar{a}_1 \dots \bar{a}_{i-1}$ pour tout i et donc, par le lemme (**1.60**), tous les choix possibles de $\bar{a}_i$ ont le même type au-dessus de ces paramètres. De plus, comme $q_{\mathrm{res}(s)^n}$ est A-définissable (tous les types sont définissables dans une théorie stable), q_s l'est aussi ; en effet $\varphi[\bar{x}_1, \dots \bar{x}_n] \in q_s$ si et seulement si $(\forall \bar{x}_1 \dots \bar{x}_n \ \bigwedge_i y_i = \mathrm{res}(\bar{x}_i) \Rightarrow \varphi[x_1, \dots x_n]) \in q_{\mathrm{res}(s)^n}$ (il n'est d'ailleurs pas très compliqué de voir que ce type est définissable uniformément en s). Si l'on a plusieurs réseaux $s_1, \dots s_n$, on définit le type $q_{s_1,\dots,s_n}$ comme le type des bases de s_i génériques au dessus des paramètres et des bases déjà choisies pour les $(s_j)_{j<i}$.
On peut alors donner la définition du langage des sortes géométriques :

Définition 1.62 ($\mathcal{L}^{\mathcal{G}}_{\mathrm{div}}$) **:**
Le langage $\mathcal{L}^{\mathcal{G}}_{\mathrm{div}}$ *est un langage muni d'une infinité de sortes :* K *et pour tout* $n \in \mathbb{N}^*$, $\mathcal{S}_n$ *et* $\mathcal{T}_n$. *La sorte* K *est munie du langage* $\mathcal{L}_{\mathrm{div}}$. *On a aussi, pour tout* n *un symbole de relation* $\in_n$ *sur* $K^n \times \mathcal{S}_n$,

un symbole de fonction $\tau_n : T_n \to \mathcal{S}_n$ *et un symbole de fonction* $\nu_n : K^n \times \mathcal{S}_n \to \mathcal{T}_n$. *Enfin pour toute formule atomique* $\varphi[\bar{x}_1, \dots, \bar{x}_n, \bar{y}]$, *où* $\bar{x}_i$ *est un* n_i^2*-uplet de variables de corps, on a un symbole* $\varphi^\star[z_1, \dots, z_n, \bar{y}]$, *où les* z_i *sont des variables dans* $\mathcal{S}_{n_i}$.

Soit (K, v) un corps valué, on en fait une $\mathcal{L}_{\text{div}}^{\mathcal{G}}$-structure $K^{\mathcal{G}}$ en interprétant K par le corps, pour tout $n \geqslant 1$ $\mathcal{S}_n$ par $\mathcal{S}_n(K)$ et $\mathcal{T}_n$ par $\mathcal{T}_n(K)$. On pose :
- $\in_n (a, s)$ si et seulement si $a \in s$;
- $\tau_n(t) = s$ si et seulement si $t \in \mathrm{res}(s)$;
- $\nu_n(a, s) = a + \mathfrak{M}\, s$ si $a \in s$ sinon $\nu_n(a, s) = \mathfrak{M}^n$;
- $\varphi^\star(s_1, \dots, s_n, a)$ si et seulement si, dans $\overline{K}^{\text{alg}}$, $\varphi[x_1, \dots, x_n, a] \in q_{s_1,\dots,s_n}$.

Il se pose alors la question de savoir si on a bien défini une extension définissable de $\mathcal{L}_{\text{div}}^{\text{eq}}$. Pour ce qui est des symboles $\in_n$, τ_n et ν_n, même si ce ne sont pas directement des symboles de $\mathcal{L}_{\text{div}}^{\text{eq}}$, il n'est pas dur de voir qu'ils sont définissables (dans la théorie des corps valués). Pour ce qui est des $\varphi^\star$, le problème est un peu plus compliqué. Comme q_s est un type définissable (uniformément en s), il s'en suit que dans $\mathrm{ACVF}^{\text{eq}}$, les $\varphi^\star$ sont bien définissables. On note donc $\mathrm{ACVF}^{\mathcal{G}}_{m,n}$ la théorie des corps valués algébriquement clos de caractéristique (m, n), dans le langage $\mathcal{L}_{\text{div}}^{\mathcal{G}}$ (qui est bien une théorie complète). On a donc pour toute formule sans quantificateurs $\varphi[\bar{x}_1, \dots, \bar{x}_n, y]$ une formule θ telle que $\mathrm{ACVF}^{\mathcal{G}} \vdash \varphi^\star[z_1, \dots, z_n, \bar{y}] \iff \theta[z_1, \dots, z_n, \bar{y}]$. La formule $\theta[f(\bar{x})]$, où f est la surjection canonique de K^n vers les autres sortes, est alors une formule à variables dans le corps qui est donc équivalente, par élimination des quantificateurs dans ACVF, à une formule $\psi[\bar{x}]$ sans quantificateurs. On a alors $\mathrm{ACVF}^{\text{eq}} \vdash \forall \bar{x}_1 \bar{x}_2,\ f(\bar{x}_1) = f(\bar{x}_2) \Rightarrow \psi[\bar{x}_1] \iff \psi[\bar{x}_2]$ et donc

$$\mathrm{ACVF}^{\mathcal{G}} \vdash \varphi^\star[\bar{z}] \iff (\forall \bar{x}\ f(\bar{x}) = \bar{z} \Rightarrow \psi[\bar{x}]) \iff (\exists \bar{x}\ f(\bar{x}) = \bar{z} \wedge \psi[\bar{x}]). \tag{1.1}$$

On peut alors montrer que si $(K, v) \leqslant (L, w)$ est une extension de corps valués alors $K^{\mathcal{G}} \subseteq L^{\mathcal{G}}$. En effet, si $s \in \mathcal{S}_n(K)$ alors $\mathcal{O}_L\, s \in \mathcal{S}_n(L)$ et $\mathcal{O}_L\, s \cap K^n = s$. On peut donc injecter $\mathcal{S}(K)$ dans $\mathcal{S}(L)$ en respectant les $\in_n$. Il s'en suit facilement qu'on peut aussi injecter $\mathcal{T}(K)$ dans $\mathcal{T}(L)$ en respectant les τ_n et les ν_n. Reste alors le problème de savoir si les $\varphi^\star$ sont respectés. Cependant, comme $\overline{K}^{\text{alg}} \preccurlyeq \overline{L}^{\text{alg}}$ (en munissant $\overline{L}^{\text{alg}}$ d'une valuation qui étend w et $\overline{K}^{\text{alg}}$ de la restriction de cette valuation), on a $(\overline{K}^{\text{alg}})^{\text{eq}} \preccurlyeq (\overline{L}^{\text{alg}})^{\text{eq}}$ et comme $\mathcal{L}_{\text{div}}^{\mathcal{G}}$ est une extension définissable dans les corps valués algébriquement clos $(\overline{K}^{\text{alg}})^{\mathcal{G}} \preccurlyeq (\overline{L}^{\text{alg}})^{\mathcal{G}}$. Comme par définition $\varphi^\star[K^{\mathcal{G}}] = \varphi^\star[(\overline{K}^{\text{alg}})^{\mathcal{G}}] \cap K^{\mathcal{G}}$, on a $\varphi^\star[L^{\mathcal{G}}] \cap K^{\mathcal{G}} = (\varphi^\star[(\overline{L}^{\text{alg}})^{\mathcal{G}}] \cap L^{\mathcal{G}}) \cap K^{\mathcal{G}} = \varphi^\star[(\overline{L}^{\text{alg}})^{\mathcal{G}}] \cap (\overline{K}^{\text{alg}})^{\mathcal{G}}) \cap K^{\mathcal{G}} = \varphi^\star[(\overline{K}^{\text{alg}})^{\mathcal{G}}] \cap K^{\mathcal{G}} = \varphi^\star[K^{\mathcal{G}}]$.

Il s'en suit que les $\varphi^\star$ sont en fait définissables par les même formules qu'en (**1.1**). En effet, soit (K, v) un corps valué quelconque, on a alors, par définition $K^{\mathcal{G}} \models \varphi^\star[\bar{z}]$ si et seulement si $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \varphi^\star[\bar{z}]$ et donc $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \forall \bar{x}\ f(\bar{x}) = \bar{z} \Rightarrow \psi[\bar{x}]$. Comme ψ est sans quantificateurs, on a donc $K^{\mathcal{G}} \models \forall \bar{x}\ f(\bar{x}) = \bar{z} \Rightarrow \psi[\bar{x}]$. Mais comme $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \mathrm{ACVF}^{\mathcal{G}}$, et que $K^{\mathcal{G}} \subseteq (\overline{K}^{\text{alg}})^{\mathcal{G}}$, on a aussi $K^{\mathcal{G}} \models \forall \bar{x}_1 \bar{x}_2,\ f(\bar{x}_1) = f(\bar{x}_2) \Rightarrow \psi[\bar{x}_1] \iff \psi[\bar{x}_2]$ et donc $K^{\mathcal{G}} \models (\forall \bar{x}\ f(\bar{x}) = \bar{z} \Rightarrow \psi[\bar{x}]) \iff (\exists \bar{x}\ f(\bar{x}) = \bar{z} \wedge \psi[\bar{x}])$. Comme cette dernière formule est existentielle, si $K^{\mathcal{G}} \models \exists \bar{x}\ f(\bar{x}) = \bar{z} \wedge \psi[\bar{x}]$, on a aussi $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \exists \bar{x}\ f(\bar{x}) = \bar{z} \wedge \psi[\bar{x}]$, d'où $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \varphi^\star[\bar{z}]$ et donc $K^{\mathcal{G}} \models \varphi^\star[\bar{z}]$. On a donc bien démontré que tout corps valué vérifie en fait la formule (**1.1**) et donc qu'on a bien défini une extension définissables du langage dans tout corps valué.

Pour finir, énonçons le théorème qui a motivé toutes ces définitions.

Théorème 1.63 :

Pour tout (m, n)*, la théorie* $\mathrm{ACVF}^{\mathcal{G}}_{m,n}$ *élimine les quantificateurs et les imaginaires.*

Ce sont les principaux résultats de [HHM06]. L'élimination des quantificateurs est prouvée au théorème 3.1.2 et celle des imaginaires au théorème 3.4.10.

Chapitre 2

Corps des nombres p-adiques et sa théorie

2.1 Corps p-adiquement clos

Cette section est particulièrement définitionnelle. On y introduit toutes les notions nécessaires pour étudier les corps p-adiquement clos.

Définition 2.1 (Groupes Archimédien) **:**
Soit Γ *un groupe abélien totalement ordonné, on dit que* Γ *est Archimédien si pour tout* a *et* $b \in \Gamma$ *tels que* $a > 0$ *il existe* $n \in \mathbb{Z}$ *tel que* $na \geqslant b$.

Remarque 2.2 :
Un théorème classique que l'on peut trouver dans [Rib64, Proposition 1, p.9] dit que les groupes Archimédien sont exactement les sous-groupes de $(\mathbb{R}, +)$ *à isomorphisme près.*

Définition 2.3 (Norme) **:**
Soient (K, v) *un corps valué dont le groupe de valeur est inclus dans* $(\mathbb{R}, +)$ *et* V *un* K*-espace vectoriel. Une norme (ultramétrique) sur* V *est une application* $\nu : V \to \mathbb{R} \cup \infty$ *qui vérifie les propriétés suivantes :*

(i) Pour tout $x \in V$, $\nu(x) = \infty \iff x = 0$.

(ii) Pour tous $x \in V$ *et* $\lambda \in K$, $\nu(\lambda x) = \nu(\lambda) + \nu(x)$.

(iii) Pour tous $x, y \in V$, $\nu(x + y) \geqslant \min(\nu(x), \nu(y))$.

Avec les conventions habituelles que pour tout $\gamma \in \Gamma$, $\gamma < \infty$ *et* $\gamma + \infty = \infty + \gamma = \infty$.
Deux normes sur V, ν_1 *et* ν_2, *sont dites équivalentes si il existe* α *et* $\beta \in \mathbb{R}$ *tel que pour tout* $x \in V$, $\nu_1(x) + \alpha \geqslant \nu_2(x) \geqslant \nu_1(x) + \beta$.

Il est évident qu'une valuation sur un corps L de K qui étend v est une norme sur L en tant que K-espace vectoriel.

Lemme 2.4 :
Soient (K, v) *un corps valué et* $K \leqslant L$ *un extension finie. Deux valuations* w_1 *et* w_2 *sur* L *qui étendent* v *sont équivalentes en temps que normes si et seulement si elles sont égales.*

Proof. Si w_1 et w_2 sont équivalentes en tant que normes alors il existe α et β dans $\mathbb{R}$ tels que pour tout $x \in L$, $w_1(x) + \alpha \leqslant w_2(x) \leqslant w_1(x) + \beta$. En appliquant cette inégalité à x^n on a alors pour tout n, $nw_1(x) + \alpha \leqslant nw_2(x) \leqslant nw_1(x) + \beta$ et donc $w_1(x) + \alpha/n \leqslant w_2(x) \leqslant w_1(x) + \beta/n$. Il s'en suit donc que pour tout x, $w_1(x) = w_2(x)$.
La réciproque est évidente. ■

Définition 2.5 :
Soient (K, v) *un corps valué de groupe de valeur Archimédien et* (V, v) *un* K*-espace vectoriel normé. Une suite* $(a_n)_{n\in\mathbb{N}}$ *d'éléments de* V *est dite convergente s'il existe* $a \in V$ *tel que pour tout* $A \in \Gamma$*, il existe* $N \in \mathbb{N}$ *tel que pour tout* n *supérieur à* N*, on ait* $v(a_n - a) \geqslant A$*. Elle est dite de Cauchy si pour tout* $A \in \Gamma$*, il existe* $N \in \mathbb{N}$ *tel que pour tout* n *et* m *supérieurs à* N*, on ait* $v(a_n - a_m) \geqslant A$*.*
Enfin, on dit que V *est complet si toute suite de Cauchy converge.*

L'existence d'un complété (qui est aussi un corps) pour tout corps valué est un résultat classique. On peut trouver dans [Lan02, Proposition XII.2.1]. De plus, il est facile de voir que le complété d'un corps valué à le même groupe de valeur et le même corps résiduel.

Définition 2.6 (Valuation p-adique) **:**
On peut munir $\mathbb{Q}$ *de la valuation suivante : tout rationnel s'écrit d'une façon unique sous la forme* $p^n a/b$ *où* a*,* b *et* $n \in \mathbb{Z}$ *et* a *et* b *ne sont pas divisibles par* p*. On pose alors* $v_p(p^n a/b) = n$*. On définit le corps* $\mathbb{Q}_p$ *comme le complété de* $\mathbb{Q}$ *pour cette valuation.*

Lemme 2.7 :
Soient (K, v) *un corps valué complet et* V *un* K*-espace vectoriel normé, alors toutes les normes sur* V *sont équivalentes et* V *est complet pour toutes ces normes.*

Proof. Voir [Lan02, Proposition XII.2.2] ■

Corollaire 2.8 :
Soient (K, v) *un corps complet et* $K \leqslant L$ *une extension finie, alors* L *ne peut être munie que d'une seule valuation (et pas seulement à équivalence près) qui étend* v *et, muni de cette valuation, c'est un corps complet.*

Proof. L est alors un K-espace vectoriel de dimension finie, toutes les valuations sur L qui étendent v sont donc équivalentes en tant que normes par le lemme (**2.7**) et par le lemme (**2.4**), elles sont donc égales. De plus le lemme (**2.7**) précise aussi que L est alors complet pour n'importe quelle norme et donc a fortiori son unique valuation. ■

Corollaire 2.9 :
Soit (K, v) *un corps valué complet alors il est Hensélien.*

Proof. D'après le corollaire (**2.8**), toute extension finie de K ne peut être munie que d'une seule valuation qui étend v. Par la proposition (**1.11**), on a alors bien que K est hensélien. ■

Définition 2.10 :
Soit (K, v) *un corps valué. On dit qu'il est à valuation discrète si* $v(K)$ *a un plus petit élément strictement positif. Une uniformisante d'un tel corps est* π *tel que* $v(\pi)$ *est le plus petit élément strictement positif.*

Remarque 2.11 :
Il est facile de voir que le groupe de valeur d'un corps valué de valuation discrète et Archimédienne est monogène.

Lemme 2.12 :
Soit (K, v) *un corps valué de valuation discrète, d'uniformisante* π *et dont le corps résiduel est fini alors toute boule de rayon* γ *est recouverte par un nombre fini de boules de rayon* $\gamma + v(\pi)$.

Proof. Soit b une boule de centre a et de rayon γ. Supposons que le corps résiduel soit de cardinal q et qu'il existe $q+1$ boules disjointes de rayon $\gamma + v(\pi)$ incluses dans b. Soient alors $x_0, \dots, x_q$ des points dans chacune de ces $q+1$ boules. On a alors pour tous $i \neq j$, $v(x_i - x_j) \leqslant \gamma$, sinon ils seraient dans la même boule de rayon $\gamma + v(\pi)$. Mais d'un autre côté on a $v(x_i - x_j) = v(x_i - a - (x_j - a)) \geqslant \gamma$ car x_i et x_j sont tous les deux dans b. On a donc pour tous $i \neq j$, $v(x_i - x_j) = \gamma$. Posons $\hat{x}_i = (x_i - a)y$ où $v(y) = -\gamma$. On a alors $v(\hat{x}_i) = 0$ et pour tous $i \neq j$, $\mathrm{res}(\hat{x}_i - \hat{x}_j) \neq 0$, i.e. $\mathrm{res}(\hat{x}_i) \neq \mathrm{res}(\hat{x}_j)$. On a donc $q+1$ éléments de résidus distincts, ce qui est absurde. Il ne peut donc exister au plus que q boules disjointes de rayon $\gamma + v(\pi)$ incluses dans b. Comme deux boules de même rayon sont soit égales soit disjointes, on a bien le résultat recherché. ∎

Lemme 2.13 :
Soient (K, v) *un corps valué complet à valuation discrète,* R *un ensemble de représentants de* $k = \mathcal{O}/\mathfrak{M}$ *et* π_i *une suite d'éléments de* K *tels que* $v(\pi_i) = v(\pi)^i$ *où* π *est une uniformisante de* K. *Alors tout élément* $x \in K$ *se développe de façon unique comme une série convergente* $\sum_{i=N}^{\infty} r_i \pi_i$ *où* $N \in \mathbb{Z}$ *et pour tout* i, $r_i \in R$.

Proof. Voir [Lan02, p. 488]. ∎

Remarque 2.14 :
On peut alors remarquer que tout élément de $\mathbb{Q}_p$ *s'écrit de façon unique comme une série convergente* $\sum_{i \geqslant N} a_i p^i$ *où* $a_i \in [\![0 \dots p-1]\!]$. *Il s'en suit aussi immédiatement que tout élément de* $\mathbb{Z}_p$ *s'écrit de façon unique comme une série convergente* $\sum_{i \geqslant 0} a_i p^i$ *et est donc limite d'éléments de* $\mathbb{Z}$, *i.e.* $\mathbb{Z}$ *est dense dans* $\mathbb{Z}_p$.

Définition 2.15 :
On définit $\mathcal{L}_{\mathbb{Q}_p} = \mathcal{L}_{\mathrm{div}} \cup \{P_n : n \in \mathbb{N}^*\}$. *La théorie* pCF *des corps* p*-adiquement clos dans le langage* $\mathcal{L}_{\mathbb{Q}_p}$ *est donnée par les axiomes suivants :*

(i) K *est un corps valué Hensélien.*

(ii) P_n *définit l'ensembles des puissances* n*-ièmes.*

(iii) Le groupe de valuation est un $\mathbb{Z}$*-groupe dont le plus petit élément strictement positif est* $v(p)$.

(iv) Le corps résiduel est $\mathbb{F}_p$.

Remarque 2.16 :
Il n'est pas totalement évident que cette théorie soit axiomatisable, montrons donc que toutes ces propriétés peuvent être traduites au premier ordre dans $\mathcal{L}_{\mathbb{Q}_p}$.

(i) *Le seul problème est d'exprimer qu'il est Hensélien, mais il suffit d'énoncer que le corps vérifie le lemme de Hensel : pour tout* $a_1 \dots a_n$ *et* a, *si* $1 \operatorname{div} a_i$, $1 \operatorname{div} a$, $\neg(\sum_i a_i a^i \operatorname{div} 1)$ *et* $\sum_i a_i i a^{i-1} \operatorname{div} 1$, *alors il existe* b *tel que* $1 \operatorname{div} b$, $\sum_i a_i b^i = 0$ *et* $\neg(a - b \operatorname{div} 1)$.

(ii) $\forall x(P_n x \iff \exists y\ x = y^n)$.

(iii) *Les axiomes précédents impliquent que le groupe de valuation est un groupe abélien totalement ordonné. Il reste cependant à dire qu'il a un plus petit élément strictement positif (qui est* $v(p)$*) :* $\neg(p \operatorname{div} 1)$ *et pour tout* x, $x \operatorname{div} p$ *implique* $x \operatorname{div} 1$ *; et que pour tout* $n \in \mathbb{N}^\star$, $[\Gamma : n\Gamma] = n$ *: pour tout* x, *il existe* y *tel que* $\bigvee_{i=0\dots n-1} x \operatorname{div} p^i y^k \wedge p^i y^k \operatorname{div} x$.

(iv) *On a déjà dit dans les axiomes que* $v(p) > 0$ *et donc* $\operatorname{res}(p) = 0$. *Il s'en suit que la caractéristique résiduelle est forcément* p *et donc il suffit de dire que le corps résiduel à au plus* p *éléments :* $\forall x_0 \dots x_p \bigvee_{i \neq j} \neg(x_1 - x_j \operatorname{div} 1)$.

Proposition 2.17 :
Le corps $\mathbb{Q}_p$ *est un modèle de* pCF. *De plus cette théorie admet l'élimination des quantificateurs dans* $\mathcal{L}_{\mathbb{Q}_p}$ *et est complète. On a donc* $\operatorname{Th}(\mathbb{Q}_p) = \mathrm{pCF}$.

Proof. La seule chose à vérifier pour montrer que $\mathbb{Q}_p \vDash \mathrm{pCF}$ est que $\mathbb{Q}_p$ est Hensélien mais c'est une conséquence immédiate du corollaire (**2.9**). L'élimination des quantificateurs a été montrée par Macintyre dans [Mac76], on en trouve aussi une preuve dans [Cha08, Théorème 5.1 p. 50]. La complétude de la théorie suit immédiatement du fait que tous les modèles contiennent $\mathbb{Q}$ muni de la valuation p-adique. ■

Comme pour ACVF, on peut démontrer un résultat d'élimination des quantificateurs dans une extension du langage tri-sorté qui permet de montrer que Γ stablement plongé au sens que tout ensemble définissable de Γ, l'est avec seulement des paramètres de Γ.
On définit aussi le langage $\mathcal{L}^{\mathcal{G}}_{\mathbb{Q}_p}$ en rajoutant les prédicats P_n au langage $\mathcal{L}^{\mathcal{G}}_{\mathrm{div}}$ et en les interprétants toujours par l'ensemble des puissances n-ièmes. La théorie $\mathrm{pCF}^{\mathcal{G}}$ est alors la théorie de $\operatorname{Th}(\mathbb{Q}_p^{\mathcal{G}})$. C'est l'extension définissables de $\mathrm{pCF}^{\mathrm{eq}}$ donnée par les considérations qui suivent la définition (**1.62**). Il suit aussi de ces considérations que la restriction à $\mathcal{L}^{\mathcal{G}}_{\mathrm{div}}$ de tout modèle de $\mathrm{pCF}^{\mathcal{G}}$ se plonge dans un modèle de $\mathrm{ACVF}^{\mathcal{G}}_{0,p}$.

Lemme 2.18 :
Soient $K \vDash \mathrm{pCF}$, $x \in K$ *et* $k \in \mathbb{N}^\star$ *alors* $x \in (K^\star)^k$ *si et seulement si*

$$(K^\star)^k \cap B_{\geqslant(1+v(x)+2v(k))}(x) \neq \varnothing.$$

Proof. Soient $y \in (K^\star)^k \cap B_{\geqslant(1+v(x)+2v(k))}(x)$ et $P(X) = X^k - x/y$. On a $v(P(1)) = v(1-y/x) = v(x-y) - v(x) \geqslant 1 + 2v(k)$ et $v(P'(1)) = v(k)$. On a donc bien $v(P(1)) > 2v(P'(1))$ et donc par le lemme de Hensel-Rychlik (voir (**1.11.iv**)) il existe $b \in \mathcal{O}$ tel que $P(b) = 0$, i.e. $b^k = y/x$. Comme $y \in (K^\star)^k$, il s'en suit directement que x aussi. La réciproque est évidente. ■

Une conséquence immédiate de ceci est que $(K^\star)^k$ est ouvert et fermé. Cela a des conséquences sur le cardinal des ensembles définissables dans pCF. La preuve est similaire à celle pour ACVF dans la proposition (**1.37**).

Proposition 2.19 :
Soit $(K, v) \models \mathrm{pCF}$*, alors tout sous-ensemble définissable de* K *est soit fini soit du cardinal de* K*.*

Proof. Soit X un ensemble définissable, par élimination des quantificateurs et par le même argument que dans la preuve de la proposition (**1.37**), on peut supposer que la formule que l'on considère est en une seule variable et que c'est une conjonction d'atomes et de négations d'atomes. Elle est donc de la forme $\varphi[x] \wedge \bigwedge_i P_{k_i}(R_i(x)) \wedge \bigwedge_j \neg P_{k_j}(R_j(x))$, où $\varphi \in \mathcal{L}_{\mathrm{div}}$ et les R_k sont des polynômes à coefficients dans K. Le cas où X est vide étant très peu intéressant, on peut supposer qu'on a un $m \in X$.

Comme φ est sans quantificateurs, on a $\varphi[K] = \varphi[\overline{K}^{\mathrm{alg}}] \cap K$. Or, on a montré dans la preuve de la proposition (**1.37**) que si $m \in \varphi[\overline{K}^{\mathrm{alg}}]$ alors cet ensemble contient une boule ouverte centrée en m. Quitte à augmenter son rayon, comme $\Gamma_{\overline{K}^{\mathrm{alg}}} = \mathrm{div}(\Gamma_K)$, on peut supposer qu'il est dans Γ_K. On a donc $m + y\mathfrak{M}_{\overline{K}^{\mathrm{alg}}} \subseteq \varphi[\overline{K}^{\mathrm{alg}}]$ où $y \in K$ et donc, comme tous ces ensembles sont définis sans quantificateurs, $m + y\mathfrak{M}_K \subseteq \varphi[K]$. Il s'en suit que $\varphi[K]$ est ouvert.
Montrons à présent que les P_k définissent des ensembles ouverts-fermés. Soit $x \in K$ tel que $K \models P_k(x)$ alors tout la boule ouverte $B_{>v(x)+2v(k)}(x)$ est aussi dans $P_k(K)$. En effet, soit $y \in B_{>v(x)+2v(k)}(x)$ alors $v(y) = v(y - x + x) = v(x)$ car $v(y - x) > v(x) + 2v(k) \geqslant v(x)$ et $x \in (K^\star)^k \cap B_{\geqslant(1+v(y)+2v(k))}(y)$, d'où, par le lemme (**2.18**), $y \in P_k(K)$. Réciproquement, si $x \notin P_k(K)$ alors si on avait $P_k(K) \cap B_{\geqslant(1+v(x)+2v(k))}(x) \neq \varnothing$, on aurait $x \in P_K(K)$ ce qui est absurde, donc $B_{\geqslant(1+v(x)+2v(k))}(x) \subseteq \neg P_k(K)$.
Comme les polynômes définissent des fonctions continues, $R_i^{-1}(P_{k_i})$ et $R_j^{-1}(\neg P_{k_j})$ sont ouverts et donc X est une intersection finie d'ouverts. C'est donc lui même un ouvert qui contient un sous-ensemble de la forme $m + y\mathfrak{M}_K$. Par les même considérations que dans la preuve de la proposition (**1.37**), on montre que $\mathfrak{M}_K$ à le même cardinal que K. C'est donc aussi le cas de X. ∎

Lemme 2.20 :
Soient $K \models \mathrm{pCF}$*,* $x \in K$ *tel que* $v(x) = 0$ *et* $k \in \mathbb{N}^\star$*, il existe alors* $n \in \mathbb{N}^\star$ *avec* $n < p^{1+2v(k)}$ *tel que* $x/n \in (K^\star)^k$ *et* $v(n) = 0$*.*

Proof. Cet énoncé peut s'exprimer au premier ordre par

$$\forall x\, v(x) = 0 \Rightarrow \bigvee_{0<n<1+v(k), v(n)=0} \exists y\, x = ny^k.$$

Il suffit donc de le démontrer dans $\mathbb{Q}_p$. Comme $B_{1+2v(k)}(x)$ est une boule (ouverte) de $\mathbb{Z}_p$ et que $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$, il existe $n \in \mathbb{Z}$ tel que $x - n \in p^{1+2v(k)}\mathbb{Z}_p$. Quitte à lui ajouter un multiple de $p^{1+2v(k)}$, on peut supposer que $0 \leqslant n < p^{1+2v(k)}$. De plus si $n = 0$ on aurait $x \in p^{1+2v(k)}\mathbb{Z}_p$, ce qui contredit le fait que $v(x) = 0$. De même, si $v(n) > 0$, on aurait alors $v(x - n) = 0 \ngeqslant 1 + 2v(k)$. On a donc $v(x/n - 1) = v(x - n) - v(n) = v(x - n) \geqslant 1 + 2v(k)$ et donc par le lemme (**2.18**), comme 1 est une puissance k-ième, x/n aussi. ∎

Corollaire 2.21 :
Soient $K \models \mathrm{pCF}$ *et* $k \in \mathbb{N}^\star$ *alors* $K^\star/(K^\star)^k$ *est fini. De plus il existe un système de représentants dans* $\mathbb{Q}$*.*

Proof. Soit $x \in K$, comme Γ_K est un $\mathbb{Z}$-groupe de plus petit élément strictement positif $v(p)$, il existe $n \in [\![0 \dots k-1]\!]$ et $y \in K$ tel que $v(x) = kv(y) + nv(p)$. D'après le lemme (**2.20**), il existe $m \in [\![1 \dots p^{1+2v(k)}]\!]$ tel que $v(m) = 0$ et que $\frac{x}{y^k p^n m}$ est une puissance k-ième. Il s'en suit donc que x est dans la même classe d'équivalence que mp^n modulo $(K^*)^k$. Il existe donc bien un système de représentants dans $\mathbb{Q}$ et il est fini vu les bornes imposées à n et m. ■

Corollaire 2.22 :
Soit $(K, v) \models \mathrm{pCF}$ *et* $A \subseteq K$ *un sous-corps valué. Pour que* A *soit un modéle de* pCF*, il faut et il suffit que* A *soit Hensélien et* $A \models \forall x\, P_n x \Rightarrow \exists y\, x = y^n$.

Proof. D'après la remarque (**2.16**), A vérifie bien tous les axiomes de pCF sauf la définition de P_n et celui qui dit que pour tout n, $[\Gamma_A : n\Gamma_A] = n$. Comme par hypothèse $A \models \forall x\, P_n x \Rightarrow \exists y\, x = y^n$, il suffit de montrer la réciproque. Soit donc $x \in A$ tel que $A \models \exists y\, x = y^n$. Mais on a alors aussi $K \models \exists y\, x = y^n$, i.e. $K \models P_n x$ et donc $A \models P_x$.
De plus, soient $x \in A$ et $n \in \mathbb{N}^*$. Comme Γ_K est un $\mathbb{Z}$-groupe, il existe $k \in [\![0 \dots n-1]\!]$ et $y \in K$ tels que $v(x) = nv(y) + kv(p)$. Par le lemme (**2.20**), il existe $m \in \mathbb{Z}$ tel que $v(m) = 0$ et $xp^{-k}y^{-n}m^{-1} \in P_n$ et donc $xp^{-k}m^{-1} \in P_n$. Comme la définition de P_n est aussi vérifiée dans A, il existe $y \in A$ tel que $xp^{-k}m^{-1} = y^n$ et donc que $v(x) \in kv(p) + n\Gamma_A$. ■

Pour finir prouvons un lemme technique sur $\mathbb{Q}_p$ qui sera utile pour déterminer la clôture définissables dans pCF.

Lemme 2.23 :
On a $\bigcap_{k \geqslant 1} (\mathbb{Q}_p)^k = \{1\}$.

Proof. Soit $x \in \bigcap_{k \geqslant 1} (\mathbb{Q}_p)^k$, quitte à le remplacer par x^{-1}, on peut supposer que $x \in \mathbb{Z}_p$ et on a alors $x \in \bigcap_{k \geqslant 1} (\mathbb{Z}_p)^k$. Pour tout k il existe donc y tel que $y^{p^k - 1} = x$, mais y peut s'écrire comme $\sum_i y_i p^i$, où $a_i \in [\![0 \dots p-1]\!]$ et donc en posant $y' = \sum_{i=0}^{k-1} a_i p^i \in \mathbb{Z}$ et $y'' = \sum_{i \geqslant k} a_i p^{i-k}$, on a $y = y' + p^k y''$. D'après le petit théorème de Fermat, on a $y'^{p^k - 1} \equiv 1 \mod p^k$ et donc, en appliquant un binôme de Newton, il existe $z \in \mathbb{Z}_p$ tel que $y^{p^k - 1} = 1 + p^k z$. Il s'en suit donc que pour tout $k \in \mathbb{N}$, il existe z tel que $x = 1 + p^k z$. Par unicité du développement en série p-adique de x, on a donc $x = 1$. ■

2.2 Clôture algébrique et définissable dans pCF

Cette section se propose de démontrer quelles sont les clôtures algébriques et définissables dans pCF, comme on l'a fait à la remarque (**1.32**) pour ACVF.

Proposition 2.24 :
Soient $(K, v) \models \mathrm{pCF}$ *et* $A \subseteq K$*, on a alors* $\overline{A}^{\mathrm{alg}} \cap K \models \mathrm{pCF}$.

Proof. D'après le corollaire (**2.22**), il suffit de montrer que $K' = \overline{A}^{\mathrm{alg}} \cap K$ est Hensélien et $K' \models \forall x\, P_n x \Rightarrow \exists y\, x = y^n$. Soient alors $P \in \mathcal{O}_{K'}[X]$ et a tel que $\mathrm{res}(P(a)) = 0$ et $\mathrm{res}(P'(a)) \neq 0$. Ces même conditions sont vérifiées dans K qui est hensélien, il existe donc $b \in \mathcal{O}_K$ tel que $P(b) = 0$ et $\mathrm{res}(b) = \mathrm{res}(a)$. Mais ce b est alors algébrique sur K' qui est relativement algébriquement clos dans K, donc $b \in K'$. Le corps K' est donc bien Hensélien.

De plus la définition des P_n est préservée, en effet si on a $K' \models P_n(x)$, c'est aussi vrai dans K car K' est muni de la structure induite et donc il existe $y \in K$ tel que $y^n = x$, mais ce y est algébrique sur K' et donc appartient à K'. ■

Corollaire 2.25 :
Soient $(K, v) \models \mathrm{pCF}$ *et* $A \subseteq K$, *on a alors* $\mathrm{acl}(A) = \overline{A}^{\mathrm{alg}} \cap K$.

Proof. On a montré dans la proposition (**2.24**) que $\overline{A}^{\mathrm{alg}} \cap K$ est une sous-structure de K qui est un modèle de pCF. Comme pCF est modèle complète, $\overline{A}^{\mathrm{alg}} \cap K$ est sous-structure élémentaire qui contient A et donc $\mathrm{acl}(A)$. Mais comme $\mathcal{L}_{\mathbb{Q}_p}$ contient le langage des anneaux, on a aussi $\overline{A}^{\mathrm{alg}} \cap K \subseteq \mathrm{acl}(A)$. Ils sont donc égaux. ■

Lemme 2.26 :
Soit T *une théorie modèle complète, telle que pour tout modèle* $\mathcal{M}$ *et tout* $A \subseteq M$, $\mathrm{acl}(A) \models T$, *alors* T *a un modèle premier et minimal au dessus de tout ensemble de paramètres, qui est justement* $\mathrm{acl}(A)$.

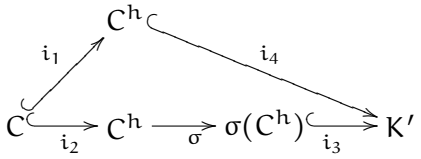
Proof. Montrons tout d'abord que $\mathrm{acl}(A)$ ne dépend pas de $\mathcal{M}$. Soient donc $\mathcal{M}_1$ et $\mathcal{M}_2$ deux modèles de $\mathcal{D}_{\mathrm{el}}(A)$, le diagramme élémentaire de A. Par la propriété du plongement commun, ils se plongent tous deux élémentairement dans un modèle $\mathcal{M} \models \mathcal{D}_{\mathrm{el}}(A)$. Mais alors $\mathrm{acl}_{\mathcal{M}_1}(A) = \mathrm{acl}_{\mathcal{M}}(A) = \mathrm{acl}_{\mathcal{M}_2}(A)$. De plus tout modèle de $\mathcal{D}_{\mathrm{el}}(A)$ contient $\mathrm{acl}(A)$ qui par modèle complétude est une sous-structure élémentaire. Enfin, si on a $A \subseteq M \preccurlyeq \mathrm{acl}(A)$ où $\mathcal{M} \models \mathcal{D}_{\mathrm{el}}(A)$, alors $\mathrm{acl}(A) \subseteq M$ et donc ils sont égaux. ■

Corollaire 2.27 :
Soit $A \subseteq K \models \mathrm{pCF}$ *alors* $\overline{A}^{\mathrm{alg}} \cap K$ *est un modèle premier et minimal au dessus de* A.

Proof. C'est une conséquence immédiate du lemme (**2.26**), du corollaire (**2.25**) et de la proposition (**2.24**). ■

Proposition 2.28 :
Soit $A \subseteq K \models \mathrm{pCF}$ *alors* $K' = \overline{A}^{\mathrm{alg}} \cap K$ *est rigide au dessus de* A.

Proof. Soit $\sigma \in \mathrm{Aut}(K'/A)$ et soit B la sous-structure fixée par σ. Montrons alors que $B \models \mathrm{pCF}$. D'après le corollaire (**2.22**), il suffit de montrer que B est hensélien et que $B \models \forall x\, P_n(x) \Rightarrow \exists y\, x = y^n$. Tout d'abord, comme K' est hensélien, il contient $C^h = \mathrm{Frac}(< A >)^h$ et comme $C = \mathrm{Frac}(< A >) \subseteq \mathrm{dcl}(A)$, il est fixé par σ. On a donc le diagramme commutatif suivant :



où les injections vérifient toutes $i(x) = x$. Par la propriété universelle de l'Hensélianisé (voir (**1.13**)) on a $i_3 \circ \sigma = i_4$ et donc pour tout $x \in C^h$, $\sigma(x) = x$, i.e. $C^h \preccurlyeq B$. Mais cette extension est algébrique donc par le corollaire (**1.12**), B est Hensélien.

Soit maintenant x tel que $B \models P_n(x)$. Si $x = 0$ alors c'est évident, sinon il a donc une racine n-ième dans K, notée y. Soit $k \in \mathbb{N}^*$, par le corollaire (**2.21**), il existe $q \in \mathbb{Q}^*$ tel que $qy \in (K^*)^k$. Mais on a alors $\sigma(qy)/qy = q\sigma(y)/qy = \sigma(y)/y \in (K^*)^k$. De plus $\sigma(y)/y$ est une racine n-ième de $a/a = 1$. Il s'en suit que $\sigma(y)/y \in \mathrm{dcl}(\varnothing) \subseteq \mathbb{Q}_p$. Par le lemme (**2.23**), on a alors $\sigma(y)/y = 1$ et donc $y \in B$, i.e. $B \models \exists y\, x = y^n$. ■

Corollaire 2.29 :
Soit $A \subseteq K \models \mathrm{pCF}$ *alors* $\mathrm{dcl}(A) = \mathrm{acl}(A) = \overline{A}^{\mathrm{alg}} \cap K$.

Proof. Quitte à en prendre une extension élémentaire, on peut supposer que K est assez saturé et homogène. Il suffit alors de montrer que tout $\sigma \in \mathrm{Aut}(K/A)$ fixe $\overline{A}^{\mathrm{alg}} \cap K$. Mais comme σ fixe A alors σ fixe (globalement) $\mathrm{acl}(A) = \overline{A}^{\mathrm{alg}} \cap K$. Mais on a montré dans la proposition (**2.28**) que $\overline{A}^{\mathrm{alg}} \cap K$ est rigide au dessus de A, il est donc fixé point par point. ■

On peut alors en déduire, comme le fait van den Dries dans [Dri84] que pCF admet des fonctions de Skolem définissables. Pour cela on fait appel au critère suivant.

Lemme 2.30 (Critère pour les fonctions de Skolem) **:**
Soit T une théorie qui élimine les quantificateurs, alors T admet des fonctions de Skolem définissables si et seulement si tout $\mathcal{A} \models T_\forall$ se plonge dans un modèle $\overline{\mathcal{A}} \models T$ qui est algébrique et rigide au dessus de A.

Proof. Voir [Dri84, Théorème 2.1] ■

Corollaire 2.31 :
La théorie pCF *admet des fonctions de Skolem définissables.*

Proof. Soient $(K, v) \models \mathrm{pCF}$ et $A \subseteq K$. D'après la proposition (**2.24**), $\overline{A}^{\mathrm{alg}} \cap K$ est un modèle de pCF, algébrique au dessus de A. Mais par la proposition (**2.28**), il est rigide au dessus de A. On peut donc conclure par le lemme (**2.30**). ■

Remarque 2.32 :
Ces résultats seront utilisés dans la dernière section, mais il faut faire attention qu'on sera alors dans une extension définissable d'une partie de L^{eq}. Les résultats qu'on a démontré restent vrais dans ce langage, à condition de considérer des ensembles de paramètres et des variables du corps seulement.

2.3 Types dans pCF

La section qui suit est une reprise des résultats de la section 4 de [HM08], dans le cas particulier de la théorie pCF. Dans ce qui suit, on notera $\mathbb{B}$ l'ensemble des boules. En particulier, si K est un corps valué et $A \subseteq K$, on note $\mathbb{B}(A)$ l'ensemble des boules A-définissables. Si $b \in \mathbb{B}(A)$, on notera $x \in b$ pour $\varphi[x]$, où φ est une $\mathcal{L}_A$-formule qui définit b. De plus, si $\mathcal{M}^{\mathrm{eq}} \models \mathrm{pCF}^{\mathrm{eq}}$, on notera $K(M)$ la sorte du corps.

Définition 2.33 (Généricité) **:**
Soient (K, v) *un corps valué,* $A \subseteq K$, $(b_i)_{i\in I}$ *une famille de boules* A*-définissables et* $P = \bigcap_i b_i$*. On dit que* $x \in K$ *est générique dans* P *au dessus de* A *si* $x \in P$ *et* x *n'appartient à aucune sous-boule stricte* A*-définissable de* P*.*
On note $\alpha_P|A$ *le* A*-type partiel suivant :*

$$\alpha_P = \{x \in b_i : i \in I\} \cup \{\neg x \in b : b \in \mathbb{B}(A) \text{ et } b \subsetneq P\}.$$

Comme on l'a déjà fait remarquer précédemment, la notion de boule se comporte mal vis à vis des extensions de corps. Il faut donc faire attention qu'un point générique dans une intersection de boules dans un corps ne le sera pas forcément dans une extension. Mais pour les corps p-adiquement clos, cela cas ne peut pas se produire :

Lemme 2.34 :
Soient $(K, v) \models \mathrm{PCF}$, $(K, v) \leqslant (L, w)$ *une extension de corps valués,* $\gamma \in \Gamma_L$ *et* $a \in K$*. Si* $B_{\geqslant\gamma}(a) \cap K$ *et* $B_{>\gamma}(a) \cap K$ *sont définissables sur* K*, alors leurs traces sur* K *sont des boules de* K*.*

Proof. Considérons d'abord $b = B_{\geqslant\gamma}(a)$. Comme b est définissable sur K, son rayon (qui est la valuation maximal de la différence de deux points dans b) est aussi définissable sur K, il s'en suit qu'il est dans $\Gamma_{\overline{K}^{alg}} = \mathrm{div}\,\Gamma_K$. Il existe donc $n \in \mathbb{N}$ tel que $n\gamma \in \Gamma_K$. Comme K est un corps p-adiquement clos, Γ_K est un $\mathbb{Z}-$groupe et donc il existe $k \in [\![0 \dots n-1]\!]$ tel que $n\gamma + k \in n\Gamma_K$, i.e. $\gamma + \frac{k}{n} \in \Gamma_K$. En d'autres termes, il existe $\delta \in \Gamma_K$ tel que $\delta - v(p)\gamma \leqslant \delta$ et $b \cap M$ est donc la boule de centre de a est de rayon δ dans M.
De plus $B_{>\gamma}(a) \cap M = B_{\geqslant\gamma+v(p)}(a) \cap M$ qui est bien une boule de M par ce qu'on vient de démontrer. ∎

Il s'en suit donc que si $(K, v) \models \mathrm{pCF}$ et $(K, v) \leqslant (L, w)$ est une extension de corps valués (on considérera les deux corps munis de leur $\mathcal{L}_{\mathrm{div}}$-structure, car cela ne change rien aux boules définissables), P est une intersection de boules de K et $A \subseteq K$, alors si x est un point générique de P au dessus de A (dans K) si et seulement s'il l'est aussi dans L. En effet, si x est générique dans L, comme toutes les boules de K sont aussi des boules de L, x est générique dans K. Réciproquement, soit b une boule de L, A-définissable alors, comme on l'a démontré au lemme **(2.34)**, $b \cap K$ est une boule de K. Soit $\sigma \in \mathrm{Aut}(K/A)$, on peut (quitte à supposer L assez homogène) l'étendre en $\tilde{\sigma} \in \mathrm{Aut}(L/A)$ qui fixe globalement K. Comme b est A-définissable dans L, il est fixé par $\tilde{\sigma}$ et donc σ fixe $b \cap K$ qui est donc bien A-définissable. Comme cette dernière boule contient x, elle ne peut être strictement incluse dans P et donc b non plus.

Remarque 2.35 :
De même, si une boule b *de* K *est* A*-définissable où* $\mathrm{dcl}(A) \cap \mathbb{B} \subseteq A$*, alors* $\langle b \rangle \in A$ *et comme* $b(L)$ *est codé par le même point,* b *est aussi* A*-définissable dans* L*.*

On dira que P est une intersection stricte si ce n'est pas lui même une boule (qui serait alors immédiatement A-définissable) et que P est non vide.
D'après [HHMo6, lemme 2.3.3], le type générique sur une boule ou une intersection stricte de boules est complet dans le cas où l'ensemble de paramètres est algébriquement clos. De plus tous les types d'éléments du corps sont d'une de ces deux formes. Dans le cas de pCF, la situation est un peu plus compliquée.

Lemme 2.36 :
Soient $\mathcal{M} \models \mathrm{pCF}^{eq}$, $A \subseteq M$ *tel que* $\mathrm{acl}^{eq}(A) \cap \mathbb{B} \subseteq \mathrm{dcl}^{eq}(A)$ *et* $x \in K(M)$ *alors* x *est générique dans une intersection stricte de boules* A*-définissables au-dessus de* A.

Proof. Soit $P = \bigcap\{b \in \mathbb{B}(A) : x \in b\}$, il est alors évident que x est générique dans P au dessus de A. Supposons alors que l'intersection ne soit pas stricte, P est donc une boule A-définissable. Soit γ son rayon, d'après le lemme (**2.12**), la boule de centre x et de rayon $\gamma + 1$ est algébrique sur A. Elle est donc dans $\mathrm{acl}^{eq}(A) \cap \mathbb{B} \subseteq \mathrm{dcl}^{eq}(A)$ et est donc définissable sur A. De plus elle contient x et est strictement contenue dans P, ce qui est absurde. ■

Définition 2.37 ($f_\star p$) **:**
Soient $\mathcal{M}$ *une* $\mathcal{L}$*-structure,* $A \subseteq M$, p *un type sur* A *et* $f = (f_i : i \in I)$ *une famille de fonctions* A*-définissables telle que pour tout* i f_i *est défini sur les réalisations de* p. *Soit* $\varphi_i[\bar{x}, \bar{y}, \bar{a}_i]$ *qui définit* f_i, *on peut alors considérer le type*

$$f_\star p = \{\psi[\bar{y}_{i_1}, \dots, \bar{y}_{i_n}, \bar{a}'] : \forall \bar{y}_{i_1} \dots \bar{y}_{i_n} \bigwedge_{j=1}^{n} \varphi_{i_j}[\bar{x}, \bar{y}_{i_j}, \bar{a}_{i_j}] \wedge \psi[\bar{y}_{i_1} \dots \bar{y}_{i_n}, \bar{a}'] \in p\}.$$

Définition 2.38 (Relative complétude) **:**
Soient $\mathcal{M}$ *une* $\mathcal{L}$*-structure,* $A \subseteq M$ *et* $(f_i)_{i\in I}$ *une famille de fonctions* A*-définissables. Un* A*-type partiel* p *est complet au dessus de* A *relativement aux* f_i *si la fonction* $q \mapsto f_\star q$ *est injective de* $\{q \in S(A) : p \subseteq q\}$ *dans* $S(A)$.

En particulier, pour vérifier qu'un type est complet au dessus de A relativement à f, il suffit de de vérifier que, dans un modèle assez saturé, pour tous c et c' qui réalisent ce type, si $f(c) \equiv_A f(c')$ alors $c \equiv_A c'$.

Lemme 2.39 :
Soient $\mathcal{M}$ *une* $\mathcal{L}$*-structure,* $A \subseteq M$ *et* $(f_i)_{i\in I}$ *une famille de fonctions* A*-définissables. Un* A*-type partiel* $p[\bar{x}]$ *est complet au dessus de* A *relativement aux* f_i *si et seulement si pour toute* $\mathcal{L}_A$*-formule* $\varphi[\bar{x}]$, *il existe une* $\mathcal{L}_A$*-formule* $\theta[\bar{y}]$ *telle que* $p[\bar{x}] \Rightarrow (\varphi[\bar{x}] \iff \theta[f(\bar{x})])$, *où* $f(\bar{x})$ *représente le uplet des* $f_i(\bar{x})$.

Proof. Supposons, tout d'abord, que p est complet au dessus de A relativement à f. L'ensemble de formules $p[\bar{x}] \cup p[\bar{x}'] \cup \{\theta[f(\bar{x})] \iff \theta[f(\bar{x}') : \theta \in \mathcal{L}_A]\} \cup \{\neg(\varphi[\bar{x}] \iff \varphi[\bar{x}'])\}$ n'est pas satisfaisable (dans un extension $\mathcal{N}$ assez saturée de $\mathcal{M}$) sinon on aurait $f(\bar{x}) \equiv_A f(\bar{x}')$ mais pas $\bar{x} \equiv_A \bar{x}'$, ce qui contredit notre hypothèse. Il existe donc $(\theta_i)_{i=1\dots n}$ des A-formules telles que pour tout $\bar{x}$ et $\bar{x}'$ réalisations de p, on ait :

$$\bigwedge_i (\theta_i[f(\bar{x})] \iff \theta_i[f(\bar{x}')]) \Rightarrow (\varphi[\bar{x}] \iff \varphi[\bar{x}']).$$

Pour tout $\sigma : [\![1 \dots n]\!] \to \{0, 1\}$, on pose $\theta_\sigma[\bar{y}] = \bigwedge_{\sigma(i)=1} \theta_i[\bar{y}] \wedge \bigwedge_{\sigma(i)=0} \neg\theta_i[\bar{y}]$ et on définit $X = \{\sigma : \exists \bar{c} \in N\ \bar{c} \models p$ et $\mathcal{N} \models \varphi[\bar{c}] \wedge \theta_\sigma[f(\bar{c})]\}$ et $\theta[\bar{y}] = \bigvee_{\sigma\in X} \theta_\sigma[\bar{y}]$. Soit alors $\bar{c} \models p$ dans $\mathcal{N}$, si $\mathcal{N} \models \varphi[\bar{c}]$ alors, comme $\mathcal{N} \models \theta_\sigma[f(\bar{c})]$ pour σ tel que $\sigma(i) = 1$ si et seulement si $\mathcal{N} \models \theta_i[f(\bar{c})]$, on a bien $\sigma \in X$ et $\mathcal{N} \models \theta[f(\bar{c})]$. Réciproquement, si $\mathcal{N} \models \theta[f(\bar{c})]$, il existe $\sigma \in X$ tel que $\mathcal{N} \models \theta_\sigma[f(\bar{c})]$, et donc il existe $\bar{c}' \models p$ tel que $\mathcal{N} \models \theta_\sigma[f(\bar{c}')] \wedge \varphi[\bar{c}']$. On a

alors, pour tout i, $\theta_i[f(\bar{c})] \iff \theta_i[f(\bar{c}')]$ et donc, comme $\mathcal{N} \vDash \varphi[\bar{c}']$, on a aussi $\mathcal{N} \vDash \varphi[\bar{c}]$. Comme $\mathcal{N}$ est assez saturé, on a exactement montré que $p[\bar{x}] \Rightarrow (\varphi[\bar{x}] \iff \theta[f(\bar{x})])$.
Réciproquement, soient $\bar{c}$ et $\bar{c}'$ deux réalisations de p dans $\mathcal{N}$ telles que $f(\bar{c}) \equiv_A f(\bar{c}')$ et $\varphi[\bar{x}] \in \mathcal{L}_A$. Soit alors $\theta[\bar{y}]$ la formule qui existe par hypothèse. On a alors $\mathcal{N} \vDash \varphi[\bar{c}] \iff \theta[f(\bar{c})] \iff \theta[f(\bar{c}')] \iff \varphi[\bar{c}']$ car $f(\bar{c})$ et $f(\bar{c}')$ ont le même type. Il s'en suit donc que $\bar{c} \equiv_A \bar{c}'$. ∎

On a montré dans le corollaire (**2.21**) que pour tout corps p-adiquement clos K, le groupe $K^\star/(K^\star)^n$ est fini et a un système de représentants dans $\mathbb{Q}$. Soit alors (q_i^n) un tel système de représentants. La surjection canonique $K^\star \to K^\star/(K^\star)^n$ est alors définissable par la formule $r_n[x,y] = \bigvee_i y = q_i^n \wedge P_n((q_i^n)^{-1}x)$. On peut d'ailleurs remarquer que le lemme (**2.18**) implique que pour tout n, $1 + p^{1+2\nu(n)}\mathcal{O} \subseteq \ker(r_n)$. Il s'en suit donc que si $\nu(x-y) + 1 + 2\nu(n) \leqslant \nu(x-z)$ alors $r_n(y-x) = r_n(y-z)$, en effet $\frac{y-z}{y-x} = 1 + \frac{z-x}{y-x}$ et $\nu(x-z) - \nu(x-y) \geqslant 1 + 2\nu(n)$ et donc $\frac{y-z}{y-x} \in \ker r_n$.
Pour x et $y \in \Gamma$, on notera aussi dans la suite $x \ll y$ si pour tout $n \in \mathbb{N}$, $x + n \leqslant y$. Comme on vient de le remarquer, on a alors que $\nu(x-y) \ll \nu(x-z)$ implique que pour tout n, $r_n(y-x) = r_n(y-z)$. De plus soit b une boule, si $x \notin b$, alors pour tout $y \in b$, $\nu(x-y)$ est constant (c'est une conséquence immédiate du caractère ultramétrique), la notation $\nu(x-b)$ a donc un sens. De même, si $\nu(x-b) \ll \rho(b)$ (où $\rho(b)$ est le rayon de la boule) alors on vient de montrer que la notation $r_n(x-b)$ à un sens. Cela dit, il suffit d'avoir $\nu(x-b)+1+2\nu(n) \leqslant \rho(b)$, comme on l'a montré un peu plus haut. Enfin dans ce qui suit, on notera $r(x-b)$ pour le uplet des $r_n(x-b)$, sous réserve qu'il soit bien défini.
Rappelons enfin que si $\mathcal{M} \vDash pCF^{eq}$, ν est $\varnothing$-définissable (c'est même un symbole de $\mathcal{L}^{eq}$). En effet, le groupe de valeur n'est autre que $K^\star/(\mathcal{O}\setminus\mathfrak{M})$ qui est bien un quotient définissable, et ν est la projection canonique.

Lemme 2.40 :
Soient $\mathcal{M} \vDash pCF^{eq}$, $A \subseteq K(M)$, $P = \bigcap_{i\in I} b_i$ une intersection stricte de boules A-définissables et $a \in P(A)$, alors le type $(\alpha_P|A)[x]$ est complet relativement à $\nu(x-a)$ et aux $r_n(x-a)$.

Proof. Soit $L = \overline{K}^{alg}$ muni d'une valuation qui étend ν (et qu'on notera aussi ν). Dans un premier temps nous allons montrer que l'on peut étendre les r_n à $L^\star$. Soit $H = (K^\star)^n \cap (1 + p^{1+2\nu(n)}\mathcal{O}_L)$ un sous-groupe de $L^\star$. Si $ab \in H \cap K^\star$ avec $a \in (K^\star)^n$ et $b \in (1+p^{1+2\nu(n)}\mathcal{O}_L)$, on a alors $b \in K^\star$, or $b = 1 + p^{1+2\nu(n)}c$ où $\nu(c) \leqslant 0$. Mais on a alors $c \in K$ et donc $b \in (1+p^{1+2\nu(n)}\mathcal{O}_K) \subseteq (K^\star)^n$. Il s'en suit que $ab \in (K^\star)^n$. On a donc montré que $H \cap K^\star = (K^\star)^n$ et donc $K^\star/P_n$ s'identifie avec un sous groupe de $L^\star/H$, et la projection sur ce quotient étend r_n. De plus on a étendu r_n de façon à ce qu'il soit toujours vrai que si $\nu(x-y) \ll \nu(x-z)$ alors $r_n(x-z) = r_n(y-z)$.
Soient maintenant c et $c' \in K$ génériques dans P au dessus de A tels que $\nu(c-a) \equiv_A \nu(c'-a)$ et pour tout n, $r_n(c-a) \equiv_A r_n(c'-a)$, i.e. il existe $\sigma \in \mathrm{Aut}(M/A)$ tel que $\nu(c-a) = \sigma(\nu(c'-a)) = \nu(\sigma(c')-a)$ (quitte à supposer $\mathcal{M}$ assez homogène) et $r_n(c-a) = r_n(c'-a)$ (car les images des r_n sont dans $\mathrm{dcl}(\varnothing)$). Comme $\sigma(c') \equiv_A c'$, il suffit de démontrer que $\sigma(c') \equiv_A c$. On peut donc supposer $\nu(c-a) = \nu(c'-a)$.
Considérons maintenant $d \in \overline{A}^{alg}$. Si $d \notin P$, soit i tel que $d \notin b_i$. Pour tout $m \in \mathbb{N}$, il existe $j \in I$ tel que $\rho(b_j) \geqslant \rho(b_i) + m$ sinon $X = \{\rho(b_j) : j \in I\}$ aurait un minimum, (parmi $\rho(b_i), \rho(b_i)+$

$1, \dots, \rho(b_i) + m$) or comme les boules de même rayon sont soit égales soit disjointes et que $P \neq \emptyset$, l'ensemble des b_j aurait un minimum pour l'inclusion ce qui contredirait le fait que P soit une intersection stricte. Comme $d \notin b_i$, on a $v(d-a) < \rho(b_i)$ et donc, comme $a, c \in b_j$, $v(c-a) \geqslant \rho(b_j) \geqslant \rho(b_i) + m > v(d-a) + m$. On a donc montré que $v(d-a) \ll v(c-a)$. Le même résultat tient pour c' et donc $v(c-d) = v(d-a) = v(c'-d)$ et pour tout n, $r_n(c-d) = r_n(d-a) = r_n(c'-d)$.
Supposons maintenant que $d \in P$, comme $v(a-d) \in \Gamma_{\overline{A}^{alg}} = \mathrm{div}(\Gamma_A)$, il existe $m \in \mathbb{N}$ tel que $mv(a-d) = \gamma \in \Gamma_A$. Pour tout $l \in \mathbb{N}$, la boule $B_{\geqslant \gamma/m-l}(a)$ est une boule A-définissable incluse dans P (par le même raisonnement que précédemment mais en utilisant maintenant que $d \in P$) et donc c ne peut y appartenir, i.e. $v(c-a) < \gamma/m - l = v(d-a) - l$ et donc $v(c-a) \ll v(d-a)$. Par le même raisonnement, $v(c'-a) \ll v(d-a)$ et donc $v(c-d) = v(c-a) = v(c'-a) = v(c'-d)$ et pour tout n, $r_n(c-d) = r_n(c-a) = r_n(c'-a) = r_n(c-a)$.
Comme tout polynôme à coefficients dans A est scindé sur $\overline{A}^{alg}$, et que v et les r_n sont des morphismes pour la multiplication, on a démontré que pour tout $Q \in A[X]$, $v(Q(c)) = v(Q(c'))$ et pour tout n, $r_n(Q(c)) = r_n(Q(c'))$ i.e. $P_n(Q(c)) \iff P_n(Q(c'))$. Or comme $A \subseteq K(M)$ et que toute $\mathcal{L}^{eq}_{\mathbb{Q}_p}$-formule à paramètres et variables dans le corps est équivalente à une $\mathcal{L}_{\mathbb{Q}_p}$-formule (c'est un propriété de T^{eq} pour toute théorie T), le type de c sur A est entièrement déterminé par son type dans la $\mathcal{L}_{\mathbb{Q}_p}$-structure. Comme il y a élimination des quantificateurs et qu'on vient de démontrer que c et c' réalisent les même atomes, on a bien $c \equiv_A c'$. ∎

Proposition 2.41 :
Soient $M \vDash pCF^{eq}$, $A \subseteq M$, $(b_i)_{i\in I}$ *une famille de boules* A*-définissables d'intersection stricte* P *et* x *une variable de corps, alors pour toute* $\mathcal{L}^{eq}_{\mathbb{Q}_p}$*-formule à paramètres dans* A, $\varphi[x]$, *on a soit* $\alpha_P \Rightarrow \varphi$ *ou* $\alpha_P \Rightarrow \neg\varphi$, *ou il existe une* $\mathcal{L}^{eq}_{\mathbb{Q}_p A}$*-formule* $\theta(y,z)$ *et* $e \subseteq e' \subseteq P$ *dans* $\mathbb{B}(A)$, *tels que* $x \in P \wedge x \notin e' \Rightarrow (\varphi[x] \iff \theta[v(x-e), r(x-e)])$ *et que tous les* $r_n(x-e)$ *qui apparaissent dans* θ *soient bien définis en dehors de* e'.

Proof. Quitte à supposer $\mathcal{M}$ assez saturé, on peut supposer que $P(a) \neq \emptyset$. Soit alors $a \in P(A)$. D'après les lemmes (**2.40**) appliqué à $K(M)$ (ce qui est possible car on a bien $A \subseteq M = \mathrm{dcl}(K(M))$) et (**2.39**), il existe une $\mathcal{L}^{eq}_{\mathbb{Q}_p}$-formule $\theta[y, \bar{z}]$ à paramètres dans M telle que $\alpha_P|M[x] \Rightarrow (\varphi[x] \iff \theta[v(x-a), r(x-a)])$.
Montrons maintenant que θ peut être choisie A-définissable. Soient $\mathcal{N}$ une extension élémentaire de $\mathcal{M}$ assez saturée et homogène et $\sigma(\theta)$ un conjugué de θ au dessus de A (dans $\mathcal{M}$, i.e. $\sigma \in \mathrm{Aut}(\mathcal{M}/A)$). Alors, pour tout $x \in N$ tel que $x \vDash \alpha_P|M$, on a alors $v(x-a) \ll v(a-\sigma(a))$ car pour tout $m \in \mathbb{N}$, $B_{v(a-\sigma(a))-m}(a)$ est une sous-boule M-définissable de P. On a donc $v(x-a) = v(x-\sigma(a))$ et pour tout n, $r_n(x-a) = r_n(x-\sigma(a))$. Il s'en suit donc que $\theta[v(x-a), r(x-a)] \iff \varphi[x] \iff \sigma(\varphi[x]) \iff \sigma(\theta)[v(x-\sigma(a)), r(x-\sigma(a))]$ car φ est A-définissable, mais la dernière formule est équivalente à $\sigma(\theta[v(x-a), r(x-a)])$ par les égalités qu'on vient de montrer.
De plus supposons que seuls $r_1, \dots r_N$ apparaissent dans θ. Si q^n_i est le système de représentants rationnelles de $K^*/(K^*)^n$ utilisés pour définir r_n, pour tout $J = (q^i_{j_i})_{i=1\dots N}$, si on note $\theta_J[y] = \forall z_1 \dots z_N, \bigwedge_i z_i = q^i_{j_i} \wedge \theta[y, \bar{z}]$. On a $\sigma(\theta_J) = (\sigma(\theta))_J$ car les $q^i_{j_i}$ sont $\varnothing$-

définissables, et donc θ_J vérifie la même propriété que θ à savoir que pour tout conjugué $\sigma(\theta_J)$ au dessus de A (dans $\mathcal{M}$), $\alpha_P|M[x] \Rightarrow (\theta_J[v(x-a)] \iff \sigma(\theta_J)[v(x-a)])$. Comme $\theta[x,y] = \bigvee_J(\theta_J[x] \wedge \bigwedge y_i = q^i_{j_i})$, il suffit de montrer que tous les theta_J sont A-définissables (ou du moins qu'on peut les remplacer par une formule à paramètres dans A).
Considérons l'ensemble de formules suivant :

$$\Sigma[x,x'] = (\alpha_P|M)[x] \cup \{\theta_J[x], \neg\theta_J[x']\} \cup \{\psi[x,\bar{a}] \iff \psi[x'\bar{a}] : \psi \in \mathcal{L}^{eq}_{\mathbb{Q}_p}, \bar{a} \in A\}.$$

Supposons qu'il soit satisfait par c et c'. Ils ont alors le même type au dessus de A et donc il existe un automorphisme $\sigma \in \mathrm{Aut}(\mathcal{M}/A)$ tel que $\sigma(c') = c$. Mais comme $c \vDash \alpha_P|M$, et que $\mathcal{M} \vDash \theta_J[c]$, on a aussi $\mathcal{M} \vDash \sigma(\theta_J)[x]$, mais donc aussi $\mathcal{M} \vDash \theta_J[\sigma^{-1}(x)]$, i.e. $\mathcal{M} \vDash \theta_j[c']$ ce qui est absurde. Cet ensemble ne peut donc pas être satisfaisable et il existe $(\psi_i)_{i=1\ldots m}$ des $\mathcal{L}^{eq}_{\mathbb{Q}_p}$-formules à paramètres dans A, telles que $\alpha_P|M[x] \Rightarrow (\bigwedge_i \psi_i[x] \iff \psi_i[x']) \Rightarrow (\theta_J[x] \iff \theta_J[x'])$. Pour tout $\tau \in 2^m$, soit $\psi_\tau = \bigwedge_{\tau(i)=1} \psi_i \wedge \bigwedge_{\tau(i)=0} \neg\psi_i$. Notons $E = \{\tau \in 2^m : \exists x \in N, x \vDash \alpha_P|M, \mathcal{N} \vDash \theta_J[x] \text{ et } \mathcal{N} \vDash \psi_\tau[x]\}$ et $\psi_E = \bigvee_{\tau\in E} \psi_\tau$. Il est alors facile de voir que $\alpha_P|M[x] \Rightarrow (\theta_J[x] \iff \psi_E)$ et cette dernière formule est bien à paramètres dans A. On peut donc supposer que les θ_J, et donc aussi θ, sont à paramètres dans A.
Par compacité, il suffit d'être dans un nombre fini de b_i et d'éviter un nombre fini de sous-boules de P dans M pour avoir $\varphi[x] \iff \theta[v(x-a), r(x-a)]$. Mais ces sous-boules sont toutes incluse dans la plus petite boule qui les contient toutes (et a). On a donc $I_0 \subseteq I$ fini et une boule b de $\mathcal{M}$ tels que $b \subseteq P$, $a \in b$ et $\bigwedge_{i\in I_0} x \in b_i \wedge x \notin b \Rightarrow (\varphi[x] \iff \theta[v(x-a), r(x-a)])$. Soit b' la boule autour de b de rayon $\rho(b)-m$ tel que $m \in \mathbb{N}$ est suffisant pour qu'en dehors de b', $r_n(x-b)$ soit bien défini pour tous les r_n qui apparaissent dans θ (en reprenant les notation de ci- dessus, il suffit de prendre $m = \max(1+2v(n) : 1 \leqslant n \leqslant N)$). On a alors

$$\bigwedge_{i\in I_0} x \in b_i \wedge x \notin b' \Rightarrow (\varphi[x] \iff \theta[v(x-b), r(x-b)]). \tag{2.1}$$

Il suffit alors de montrer qu'on peut choisir b et b' A-définissables. Si $\alpha_P|A \Rightarrow \varphi$ ou $\alpha_P|A \Rightarrow \neg\varphi$ alors c'est fini. On peut donc supposer qu'on a a_1 et $a_2 \in M$ qui réalisent $\alpha_P|A$ tels que $\mathcal{M} \vDash \varphi[a_1]$ et $\mathcal{M} \vDash \neg\varphi[a_2]$. Soient alors $e = B_{\geqslant v(a_1-a_2)}(a_1)$ et e' la boule autour de e de rayon $\rho(e) - m$, alors aucune paire (b,b') qui satisfait (**2.1**) ne peut vérifier que b' et e' sont disjoints. En effet, si c'était le cas, comme b est disjoint de e', on aurait $\rho(e') = v(a_1-a_2) - m > v(a_1-b)$ et donc $v(a_1-b) = v(a_2-b)$ et pour tout n tel que r_n apparaît dans θ, $r_n(a_1-b) = r_n(a_2-b)$. De plus, comme $a_1, a_2 \notin b'$, on a $\varphi[a_1] \iff \theta[v(a_1-b), r(a_1-n)] \iff \theta[v(a_2-b), r(a_2-n)] \iff \varphi[a_2]$ ce qui est absurde. Quitte à agrandir b pour que son rayon soit supérieur à $v(a_1-a_2) \in \Gamma_M$, on peut supposer que $\rho(b') \geqslant \rho(e')$, on a donc forcément $e' \subseteq b'$. Comme tous les conjugués de (b,b') au dessus de A vérifient (**2.1**), un conjugué de b' au dessus de A ne pas être disjoints de e' et donc de b'. Cela implique aussi, quitte a appliquer un automorphisme, que deux conjugués de b ne peuvent pas être disjoints.
Soit $\psi[x,\bar{d}]$ une $\mathcal{L}^{eq}_{\mathbb{Q}_p}$-formule qui défini b'. Soit $p = \mathrm{tp}(\bar{d}/A\rho(b'))$. Si l'ensemble de formules

$$p[y] \cup \{\neg(\forall x\, \psi[x,\bar{d}] \iff \psi[x,\bar{y}])\}$$

était satisfaisable, on aurait $\sigma \in \mathrm{Aut}(\mathcal{M}/A\rho(b'))$ tel que $\psi[x, \bar{d}]$ et $\psi[x, \sigma(\bar{d})]$ ne définissent pas le même ensemble, i.e. $b' \neq \sigma(b')$. D'après ce qu'on vient de démontrer, on a soit $b' \subseteq \sigma(b')$, soit $\sigma(b') \subseteq b'$. Mais comme σ fixe $\rho(b')$, on a $\rho(\sigma(b')) = \sigma(\rho(b')) = \rho(b')$ et donc $b' = \sigma(b')$, ce qui est absurde. Il s'en suit donc qu'il existe $(\chi[\bar{y}, z])$ une $\mathcal{L}^{eq}_{\mathbb{Q}_p}$-formule à paramètres dans A, telle que $\mathcal{M} \vDash \forall \bar{d}' \chi[\bar{d}', \rho(b')] \Rightarrow (\forall x \psi[x, \bar{d}] \iff \psi[x, \bar{d}'])$ et on peut supposer que $\chi[y, \bar{z}]$ implique que $\psi[x, \bar{y}]$ est une boule de rayon z (car c'est exprimable par une formule qui est dans le type de $\bar{d}$). De plus, si on note $q = \mathrm{tp}(\bar{d}/A)$ et $\delta[x_1, x_2, \bar{y}_1, \bar{y}_2] = \psi[x_1, \bar{y}_1] \wedge \neg\psi[x_2, \bar{y}_1] \wedge \neg\psi[x_1, \bar{y}_2] \wedge \psi[x_2, \bar{y}_2]$, l'ensemble de formules

$$q[\bar{d}_1] \cup q[\bar{d}_2] \cup \delta[x_1, x_2, \bar{d}_1, \bar{d}_2]$$

n'est pas satisfaisable. En effet, il y aurait alors deux conjugués de b au dessus de A qui ne sont pas inclus l'un dans l'autre, i.e. sont disjoints, ce qui contredit ce que l'on a vu précédemment. Il s'en suit donc qu'il existe χ_1 et χ_2 deux formules de q telles que $\mathcal{M} \vDash \forall \bar{d}_1 \bar{d}_2 \chi_1[\bar{d}_1] \wedge \chi_2[\bar{d}_2] \Rightarrow (\forall x_1 x_2 \neg\delta[x_1, x_2, \bar{d}_1, \bar{d}_2])$. Posons alors $\zeta[x, z] = \exists \bar{d}' \chi[\bar{d}', z] \wedge \chi_1[\bar{d}'] \wedge \chi_2[\bar{d}'] \wedge \psi[x, \bar{d}']$ qui est à paramètres dans A. Cette formule permet alors de définir une fonction f A-définissable qui a un rayon γ associe une boule de rayon γ telle que $f(\rho(b')) = b'$. De plus les images par f forment une chaîne. En effet, si l'on a γ_1 et γ_2 tels que $f(\gamma_1)$ et $f(\gamma_2)$ ne sont pas inclus l'un dans l'autre, i.e. sont disjoints, alors il existe x_1, x_2, $\bar{d}_1$ et $\bar{d}_2$ dans $\mathcal{M}$ tels que $\mathcal{M} \vDash \delta[x_1, x_2, \bar{d}_1, \bar{d}_2] \wedge \chi_1[\bar{d}_1] \wedge \chi_2[\bar{d}_2]$, ce qui est absurde.
On note alors f' la fonction qui à γ associe la boule de rayon m de moins autour de $f(\gamma)$. L'ensemble G des $\gamma \in \Gamma_{\mathcal{M}}$ tels que $(f(\gamma), f'(\gamma))$ vérifie (**2.1**) est donc A-définissable et non vide car il contient $\rho(b')$ (en effet comme (b, b') vérifie (**2.1**) et que $f'(\rho(b'))$ contient b' qui contient b, $(b', f'(\rho(b')))$ vérifie aussi (**2.1**)).
Si cet ensemble est majoré il admet un maximum. En effet, le groupe de valeur de $\mathbb{Q}_p$ est $\mathbb{Z}$ où cette propriété est vérifiée et elle s'exprime au premier ordre. Soit donc γ_0 un majorant de G, il est donc A-définissable et $(f(\gamma_0), f'(\gamma_0))$ est une paire de boules A-définissables vérifiant (**2.1**). Si $f(\gamma_0) \subseteq P$ alors ce sont les boules recherchées, sinon $f'(\gamma_0)$ et P sont disjoints et donc comme a_1 et a_2 sont dans P, $v(a_1 - f(\gamma_0)) \ll v(a_1 - a_2)$. Il s'en suit alors que $\varphi[a_1] \iff \theta[v(a_1 - f(\gamma_0)), r(a_1 - f(\gamma_0))] \iff \theta[v(a_2 - f(\gamma_0)), r(a_2 - f(\gamma_0))] \iff \varphi[a_2]$ ce qui est absurde.
S'il n'est pas majoré, considérons l'ensemble $X = \bigcap_{\gamma \in G} f(\gamma)$ qui est A-définissable et ne peut contenir au plus qu'un point. De plus, comme la propriété que les intersections de chaînes définissables de boules sont non vides est vraie dans $\mathbb{Q}_p$ et s'exprime au premier ordre, il s'en suit que X est non vide et est donc réduit à un point a, qui est donc nécessairement A-définissable. Soient alors $x \in P$ distinct de a et $\gamma \in G$ tel que $\gamma - m > v(x - a)$, on a alors $\varphi[x] \iff \theta[v(x - f(\gamma)), r(x - f(\gamma))]$ mais comme $a \in f(\gamma)$, on a bien $\varphi[x] \iff \theta[v(x - a), r(x - a)]$. On peut alors choisir pour e et e' la boule de rayon ∞ autour de a. ■

Corollaire 2.42 :
Avec les même notations que dans le lemme précédent, s'il existe $b \in \mathbb{B}(A)$ *tel que* $b \subseteq P$ *alors* α_P *est complet relativement à* $v(x - b)$ *et aux* $r_n(x - b)$. *Si, par contre, il n'existe pas de tel* b *alors* α_P *est complet.*

Proof. Supposons qu'il existe $b \in \mathbb{B}(A)$ tel que $b \subseteq P$. Soit $\varphi[x]$ une $\mathcal{L}_A$-formule, si $\alpha_P[x] \Rightarrow \varphi[x]$, on a $\alpha_P[x] \Rightarrow (\varphi[x] \iff v(x) = v(x))$ et si $\alpha_P[x] \Rightarrow \neg\varphi[x]$, on a $\alpha_P[x] \Rightarrow$

$(\varphi[x] \iff \neg v(x) = v(x))$. Dans les autres cas, d'après la proposition (**2.41**), il existe une formule θ et $e \subseteq e' \subseteq P$ dans $\mathbb{B}(A)$ tels que $x \in P \wedge x \notin e' \Rightarrow (\varphi[x] \iff \theta[v(x-e), r(x-e)])$. Soit c la plus petite boule qui contient b et e, elle est bien A-définissable et donc toute réalisation x de α_P est à l'extérieure de cette boule (et même loin de cette boule). Il s'en suit donc que $v(x-b) = v(x-c) = v(x-e)$ et de même pour r. On a donc $\alpha_P[x] \Rightarrow (\varphi[x] \iff \theta[v(x-b), r(x-b)])$. Il suit alors du lemme (**2.39**), que α_P est complet au dessus de A relativement à v et r.
Par contre, si un tel b n'existe pas, si on n'a pas $\alpha_P \Rightarrow \varphi$ où $\alpha_P \Rightarrow \neg\varphi$ alors on devrait avoir un $e \in \mathbb{B}(A)$ qui sont inclus dans P, par la proposition (**2.41**), ce qui est absurde. ■

Corollaire 2.43 :
Soient $\mathcal{M}^{eq} \models pCF^{eq}$, $A \subseteq M^{eq}$ *tel que* $acl^{eq}(A) \cap \mathbb{B} \subseteq dcl^{eq}(A)$ *et* $B = \mathbb{B}(A)$ *alors pour tout* $c \in K(M)$, $tp(c/B) \Rightarrow tp(c/A)$.

Proof. Soient c et c' qui ont le même type au dessus de B et montrons qu'ils ont aussi le même type au dessus de A. Tout d'abord, d'après le lemme (**2.36**), comme A est algébriquement clos, c est générique dans une intersection stricte P de boules A-définissables. Comme $\alpha_p \subseteq tp(c/B)$, c' est aussi générique sur P. D'après le corollaire (**2.42**), si P ne contient pas de boule de B alors α_P est complet et comme c et c' en sont deux réalisations, on a bien $c \equiv_A c'$. Par contre s'il existe une boule $b \in B$ incluse dans P, toujours par ce corollaire, il suffit de vérifier que $v(c-b), r(c-b)$ a le même type au dessus de A que $v(c'-b), r(c'-b)$.
Tout d'abord comme les valeurs des différents r_i sont dans $\mathbb{Q} \subseteq dcl(\varnothing)$ et que $c \equiv_B c'$ et donc en particulier que $c - b \equiv_{\mathbb{Q}} c' - b$, $r(c-b)$ et $r(c'-b)$ ont bien le même type (ils sont en fait égaux). De plus comme Γ est plongé stablement et que tous ses points sont codés par une boule, le type de $v(c-b)$ sur B implique celui sur $\Gamma(A)$ et donc sur A. On a donc bien que $v(c-b) \equiv_A v(c'-b)$. ■

La proposition qui suit est une forme de réciproque à la proposition (**2.41**). On y avait démontré que pour rendre complet un α_P, il faut spécifier le type de $(v(x-a), r(x-a))$ pour un certain a. La proposition qui suit montre que réciproquement, quelque soit le type qu'on choisisse pour $(v(x-a), r(x-a))$, s'il est raisonnable alors il sera consistant avec α_P.

Définition 2.44 (P_Γ) **:**
Si $P = \bigcap_{b\in B} b$ *est une intersection de boules, on notera* $P_\Gamma = \{\gamma \in \Gamma : \forall b \in B,\ \gamma \geqslant \rho(b)\}$. *On notera aussi* P_Γ *l'ensemble de formules qui définit ce type partiel.*

On peut d'ailleurs remarquer que dans ACVF, P_Γ est un type total.

Proposition 2.45 :
Soient $\mathcal{M} \models pCF^{eq}$, $A \subseteq M$, $P = \bigcap_{b\in B} b$ *intersection stricte de boules* A*-définissables et* $q[y,z]$ *le type d'un certain* $(v(c), r(c))$ *au dessus de* A *tel que* $q[y,z]$ *implique* $P_\Gamma[y]$ *et* $y < \gamma$ *pour tout* $\gamma \in P_\gamma(A)$. *Alors* $(\alpha_P|M)[x] \cup \bigcup_{a\in P(M)} q[v(x-a), r(x-a)]$ *est consistant.*

Proof. On peut supposer $\mathcal{M}$ assez saturé pour que $P(M)$ soit non vide. Soit alors $a \in P(M)$. Montrons que $q[y,z] \cup \{y < \gamma : \gamma \in P_\Gamma(M)\}$ est consistant. En effet, s'il ne l'était pas, par compacité, il existerait $\gamma \in P_\Gamma(M)$ et $\psi \in q$ une $\mathcal{L}_A$-formule tels que $\psi[y,\bar{z}] \Rightarrow y \geqslant \gamma$. Comme $\bar{z}$ n'apparaît pas à droite de l'implication, quitte à remplacer ψ pas $\exists\bar{z}\psi[y,\bar{z}]$, on peut

supposer que sa seule variable est y. Comme $\psi[\mathcal{M}]$ a un minorant, elle admet une borne inférieure γ' (cette propriété est vraie dans $\mathbb{Z}$ et s'exprime au premier ordre). Comme $\psi[\mathcal{M}]$ a un minorant dans P_Γ, γ' est dans $P_\Gamma(A)$ et on a $q[y] \Rightarrow y \geqslant \gamma'$, ce qui est absurde.
Soit alors $(\gamma, s) \vDash q[y, \bar{z}] \cup \{y < \gamma : \gamma \in P_\Gamma(M)\}$ (dans une extension élémentaire de $\mathcal{M}$). Par hypothèse, la formule $\exists x,\ v(x) = y \wedge r(x) = z$ est dans q (à vrai dire comme r est un uplet infini, tout bout fini de cette formule est dans q). Par compacité, existe donc c tel que $(v(c), r(c)) \vDash q[y, z] \cup \{y < \gamma : \gamma \in P_\Gamma(M)\}$. On pose alors $d = a + c$. Tout d'abord, comme $v(d - a) = v(c) \in P_\Gamma$, et que $a \in P$, il s'en suit immédiatement que $d \in P$. De plus si d était dans une boule b M-définissable incluse dans P, quitte à la remplacer par la plus petite boule qui contient a et b, on pourrait supposer que b contient a. Mais alors $\rho(b) \in P_\Gamma(M)$ et $v(c) = v(d-a) \geqslant \rho(b)$, ce qui contredit la définition de c. On a donc bien $d \vDash \alpha_P|M$. De plus, soit $a' \in P(M)$, comme d est générique dans P au dessus de M, on a $v(d - a) \ll v(a - a')$. Il s'en suit donc qu'on a $v(d - a') = v(d - a) = v(c)$ et $r(d - a') = r(d - a) = r(c)$ et, comme $c \vDash q[v(c), r(c)]$, on a bien $(v(d - a'), r(d - a')) \vDash q$. ∎

Pour finir montrons l'existence d'extensions invariantes dans pCF. Avant de commencer rappelons cependant que dans un $\mathbb{Z}$-groupe, il existe des extension invariantes. Toute type p sur un ensemble de paramètres A est déterminé par l'ensemble des $n_k \in [\![0 \dots k-1]\!]$ tels que $x - n_k$ est un multiple de k et par la coupure réalisée par x dans A. Comme les n_k sont définissables sur le vide, une extension de p est juste une extension de la coupure, et elle peut être choisie de façon à être A-invariante (par exemple en mettant à gauche tout les nouveaux points qui réalisent la coupure sur A).

Proposition 2.46 :
Soient $\mathcal{M}^{eq} \vDash pCF^{eq}$, $A \subseteq M^{eq}$ *tel que* $\mathrm{acl}^{eq}(A) \cap \mathbb{B} \subseteq \mathrm{dcl}^{eq}(A)$ *et* $c \in K(M)$, $p = \mathrm{tp}(c/A)$ *a alors une extension* $\mathrm{Aut}(M^{eq}/A)$*-invariante.*

Proof. D'après le lemme (**2.36**), c est générique sur une intersection stricte P de boules A-définissables. Supposons qu'il existe une boule a A-définissable incluse dans P, on note alors $q = \mathrm{tp}(v(c-a), r(c-a)/A)$. D'après la proposition (**2.41**), on a alors $\alpha_P|A \cup q[v(x-a), r(x-a)] \Rightarrow p[x]$. On pose alors $s_i = r_i(x - a) \in \mathbb{Q}$ et soit q' une extension $\mathrm{Aut}(\Gamma(M)/\Gamma(A))$-invariante de $\mathrm{tp}(v(c - a)/\Gamma(A))$. Comme Γ est stablement plongé, q' est un type complet sur $\mathcal{M}^{eq}$ et il est bien $\mathrm{Aut}(\mathcal{M}^{eq}/A)$-invariant. De même le type $t[y, z] = q'[y] \cup \{z = s_i\}$ est un type complet sur $\mathcal{M}^{eq}$ qui est $\mathrm{Aut}(\mathcal{M}^{eq}/A)$-invariant (il est consistant car comme précédemment toute sous formule finie de $\exists x\ v(x) = y \wedge v(x) = \bar{y}$ est dans q dont q' est une extension). Par la proposition (**2.45**), $p^\star = \alpha_P|M^{eq} \cup \bigcup_{m \in P(M^{eq})} t[v(x - m), r(x - m)]$ est consistant. Il est évident qu'il est complet par le corollaire (**2.42**) et qu'il étend p. De plus, $\alpha_P|M^{eq}$ est clairement $\mathrm{Aut}(\mathcal{M}^{eq}/A)$-invariant et si $\sigma \in \mathrm{Aut}(\mathcal{M}^{eq}/A)$ et $m \in P(M^{eq})$ alors $\sigma(m) \in P(M^{eq})$ et $\sigma(t[v(x - m), r(x - m)]) = t[v(x - \sigma(m)), r(x - \sigma(m))]$ est aussi inclus dans $p^\star$, d'où $p^\star$ est $\mathrm{Aut}(M^{eq}/A)$-invariant. ∎

Remarque 2.47 :
Comme pour les résultats de la section précédente, les résultats de cette section ne seront pas utilisés exactement dans le cadre où on les a démontrés. Mais ici, on s'est déjà placé dans un modèle de pCF^{eq}*. Le passage à une extension définissable ne changeant rien aux types, on pourra les appliquer sans soucis.*

2.4 Extensions algébriques des corps $\mathfrak{p}$-adiquement clos

On va commencer dans cette partie par étudier les extensions finies de $\mathbb{Q}_p$, pour étendre ensuite cette étude aux corps p-adiquement clos. La partie algébrique de ce qui suit est inspiré de [Lan94, ch. II], [Lan02, ch. XII], [Nar74, ch. V §2] et [Ser68, ch. III §6].

Définition 2.48 (indice de ramification et d'inertie) **:**
Soit $(L,w)\geqslant(K,v)$ *une extension finie de corps valué. On note* $e(w|v)=[\Gamma_w:\Gamma_v]$ *(ou plus simplement* $e(L|K)$ *si les valuations sont évidentes) le degré de ramification et* $f(w|v)=[k_w|k_v]$ *l'indice d'inertie.*

Lemme 2.49 :
Soit $(L,w)\geqslant(K,v)$ *une extension finie, on a alors* $e(w|v)f(w|v)\leqslant[L:K]$ *(en particulier* $e(w|v)$ *et* $f(w|v)$ *sont finis).*

Proof. Soient $\overline{w(x_1)},\dots,\overline{w(x_r)}$ des éléments de classes distinctes de Γ_L/Γ_K (où $x_i\in L^\star$) et $\overline{y_1},\dots,\overline{y_s}$ une famille k_K-libre de k_L. Montrons alors que la famille $(x_iy_j)_{i,j}$ est libre sur K. Considérons donc $a_{i,j}\in K$ tels que $\sum_{i,j}a_{i,j}x_iy_j=0$. Quitte à retirer des termes, on peut supposer que pour tout i il existe j tel que $a_{i,j}$ est non nul. Fixons alors un i et soit j_i tel que $v(a_{i,j_i})$ est minimal. $\sum_j a_{i,j}/a_{i,j_i}y_j$ est alors une combinaison des y_j à coefficients dans $\mathcal{O}$ dont un des coefficients est de valuation nulle. Son résidu est une combinaison des $\overline{y_j}$ dont un des coefficients est non nul, elle ne peut donc pas être nulle et donc $v(\sum_j a_{i,j}/a_{i,j_i}y_j)=0$, i.e. $v(\sum_j a_{i,j}y_j)=v(a_{i,j_i})$, il s'en suit que $\infty=v(\sum_{i,j}a_{i,j}x_iy_j)=\sum_i v(a_{i,j_i})v(x_i)$. Il existe donc i_1 et i_2 tel que $v(a_{i_1,j_{i_1}})v(x_{i_1})=v(a_{i_2,j_{i_2}})v(x_{i_2})$. Mais alors $v(x_{i_1})-v(x_{i_2})=v(a_{i_2,j_{i_2}}/a_{i_1,j_{i_1}})\in\Gamma_K$ ce qui est absurde. Comme cette famille est libre, on doit donc avoir $rs\leqslant[L:K]$.
Supposons maintenant que $e(w|v)$ sont infini, on particulier on peut trouver une famille $x_1,\dots,x_r$ telle que précédemment avec $r>[L:K]$. Mais on a alors $[L:K]<r\leqslant[L:K]$, ce qui est absurde. Donc $e(w|v)$ est fini, et de même $f(w|v)$ est fini. On peut alors prendre $r=e(w|v)$ et $s=f(w|v)$ pour obtenir le résultat voulu. ∎

Proposition 2.50 :
Soient (K,v) *un corps valué complet de valuation discrète et* (L,w) *une extension finie, alors* $[L|K]=e(w|v)f(w|v)$. *De plus* L *est aussi à valuation discrète. Si l'extension* $k_L\geqslant k_K$ *est séparable, il existe* $a\in L$ *tels que* $L=K[a,\Pi]$ *(où* Π *est une uniformisante de* L *et le polynôme minimal annulateur de* a *est dans* $\mathcal{O}[X]$*) et* $\mathcal{O}_L=\mathcal{O}_K[a,\Pi]$, $K[a]\geqslant K$ *est purement inertielle,* $\mathrm{res}(K[a])=k_L$, $K[\Pi]\geqslant K$ *est purement ramifiée et* $v(K[\Pi])=\Gamma_L$ *(en fait* $K[a,\Pi]\geqslant K[a]$ *est aussi purement ramifiée).*

Proof. On notera dans cette preuve e pour $e(w|v)$ et de même pour f. Tout d'abord par le corollaire **(2.8)** L est un corps valué complet. De plus soit π une uniformisante de v, comme Γ_L/Γ_K est fini, entre 0 et π il y a au plus un nombre fini de points et donc Γ_L a un plus petit élément, i.e. L est à valuation discrète. Soit alors Π une uniformisante de L. Comme $[\Gamma_L:\Gamma_K]=e$, on a $ew(\Pi)\in\Gamma$. De plus, par la remarque **(2.11)**, Γ_L est monogène, il existe donc n tel que $v(\pi)=nw(\Pi)$. Si on prend ce n minimal, on a alors $n\leqslant e$, et $(iw(\Pi))_{i=0\dots n-1}$ sont dans des classes différentes modulo Γ_K (car leurs différences sont plus petites que π). De plus,

soit $\gamma \in \Gamma_L$, il existe m tel que $\gamma = mw(\Pi) = (qn + r)w(\Pi) = qv(\pi) + rw(\Pi)$ où $0 \leqslant r < n$ et donc $e = [\Gamma_L : \Gamma_K] = n$, i.e. $ew(\Pi) = v(\pi)$.
Soit de plus $(\overline{a_i})_{i=0\dots f-1}$ une base de $k_L \geqslant k_K$. Si R est un système de représentants de k_K alors $\{\sum_{i=0}^{f-1} r_i a_i \,:\, r_i \in R\}$ est un système de représentants de k_L. Comme la famille des $(\Pi^i\pi^j)_{i=0\dots e-1, j\in\mathbb{Z}}$ vérifie que $w(\Pi^i\pi^j) = i + ejw(\Pi)$, par le lemme (**2.13**), tout $x \in L$ s'écrit

$$\sum_{j=N}^{\infty}\sum_{i=0}^{e-1}\left(\sum_{l=0}^{f-1} r_{i,j,l}a_l\right)\Pi^i\pi^j = \sum_{i=0}^{e-1}\sum_{l=0}^{f-1}\left(\sum_{j=N}^{\infty} r_{i,j,l}\pi^j\right)a_l\Pi^i$$

or $\sum_{j=N}^{\infty} r_{i,j,l}\pi^j \in K$ et donc la famille à ef éléments $(a_l\Pi^i)$ est une famille génératrice de L au dessus de K et donc $[L : K] \leqslant ef$. Le lemme (**2.49**) permet alors de conclure qu'on a bien $[L : K] = ef$.
Supposons maintenant que $k_L \geqslant k_K$ est séparable. Soit alors α un élément primitif de cette extension et $P \in k_K[X]$ son polynôme minimal (que l'on choisit unitaire) qui est séparable. Soit $Q \in \mathcal{O}_K[X]$ unitaire tel que $\mathrm{res}(Q) = P$, comme K est complet et donc Hensélien (voir (**2.9**)), il existe $a \in \mathcal{O}_L$ tel que $Q(a) = 0$ et $\mathrm{res}(a) = \alpha$. On peut alors prendre $a_i = a^i$ dans la preuve précédente et on a alors bien $L = K[a, \Pi]$. De plus, on a $x \in \mathcal{O}_L$ si et seulement si $N \geqslant 0$ mais alors $\sum_{j=N}^{\infty} r_{i,j,l}\pi^j \in \mathcal{O}_K$ et on a donc bien $\mathcal{O}_L = \mathcal{O}_K[a, b]$.
Enfin, comme $w(\Pi) > 0$, on a $\mathrm{res}(\Pi) = 0$ et donc $\mathrm{res}(K[\Pi]) = \mathrm{res}(K) = k_K$ et donc l'extension est purement ramifiée. De plus $[K[a] : K] \leqslant \deg(Q) = \deg(P) = [k_L : k_K] \leqslant [K[a] : K]$ car $(\mathrm{res}(a)^i)_{i=0\dots f-1}$ est une famille génératrice de k_L au dessus de k_K. Il s'en suit que $[K[a] : K] = [k_L : k_K]$ et comme $\mathrm{res}(K[a]) = k_L$ c'est bien une extension purement inertielle. Pour finir, on peut remarquer que $[K[a, \Pi] : K[a]] = e = [\Gamma_L : \Gamma_K]$ et comme $v(K[a]) = \Gamma_K$ car l'extension est purement inertielle, on a bien que $K[a, \Pi] \geqslant K[a]$ est purement inertielle. ■

Remarque 2.51 :
On remarque que dans la preuve précédente on a démontré que si (K, v) *est un corps valué complet de valuation discrète,* (L, w) *une extension finie,* Π *une uniformisante de* L *et* a *tel que* $\mathrm{res}(a)$ *soit primitif de* k_L *au dessus de* k_K*, alors la famille* $(a^i\Pi^j)$ *pour* $0 \leqslant i < f(w|v)$ *et* $0 \leqslant j < e(w|v)$ *est une base du* K*-espace vectoriel* L *(et une base du* $\mathcal{O}_K$*-module* $\mathcal{O}_L$*). En effet, on démontré dans la preuve du lemme (**2.49**) qu'une telle famille est* K*-libre (et donc* $\mathcal{O}_K$*-libre) et on vient de démontrer qu'elle est aussi génératrice (de* L *si on prend les coefficients dans* K *et de* $\mathcal{O}_L$ *si on prends les coefficients dans* $\mathcal{O}_K$*).*

La proposition précédente permet donc de se ramener à l'étude des extensions purement inertielles et purement ramifiées.

Lemme 2.52 :
Soient (K, v) *un corps Hensélien et* $k \geqslant k_K$ *une extension finie séparable du corps résiduel. Il existe alors une unique extension purement ramifiée* (L, w) *à isomorphisme près telle que* $k_L \cong_{k_K} k$*. Si de plus l'extension* $k \geqslant k_K$ *est normale alors* $L \geqslant K$ *est aussi normale et elle est unique (pas seulement à isomorphisme près).*

Proof. Soient α un élément primitif de $k \geqslant k_K$ et $P \in k_K[X]$ son polynôme minimal (unitaire). Soit $Q \in \mathcal{O}_K[X]$ unitaire tel que $\mathrm{res}(Q) = P$ et soit $a \in \overline{K}^{\mathrm{alg}}$ tel que $Q(a) = 0$. On pose $L = K[a]$

et on muni L de la restriction de la valuation de $\overline{K}^{alg}$. Comme $P(res(a)) = res(Q(a)) = 0$, on a $k_L \supseteq k$ (ou du moins k s'injecte dans k_L au dessus de k_K), de plus k_L est engendré par les $res(a_i)_{i=1\dots[L:K]}$ au dessus de k_K et donc $[L : K] \leqslant \deg(Q) = \deg(P) = [k : k_K] \leqslant [k_L : k_K] \leqslant [L : K]$, i.e. $L \geqslant K$ est purement ramifié et $k_L \cong_{k_K} k_K$. On a donc montré l'existence.
Montrons maintenant l'unicité. Soit $L' \geqslant K$ une extension purement ramifiée telle que $k_{L'} \cong_{k_K} k$. Comme L' est Hensélien (c'est une extension finie d'un corps Hensélien), il existe $a' \in L'$ tel que $Q(a') = 0$. On a alors $K[a'] \cong_K K[a]$ (et ils sont isomorphe en temps que corps valués par unicité de l'extension de la valuation au dessus d'un corps Hensélien). Mais par les même considérations que précédemment, le corps résiduel de $K[a']$ est $k_{L'}$ et comme $L' \geqslant K$ est purement ramifiée, il s'en suit que $L' = K[a']$.
Supposons maintenant que $k \geqslant k_K$ soit normale. Le polynôme P est donc scindé dans k_L et par le lemme d'Hensel appliqué à chaque racine, Q est scindé sur L. Comme $Q \geqslant K$ est engendré par une des racines de Q, c'est le corps de décomposition de Q et il est donc normal et unique.
■

Corollaire 2.53 :
Soit (K, v) *un corps hensélien de corps résiduel fini, alors* K *n'a qu'une extension purement inertielle de degré donné.*

Proof. Comme un corps fini est parfait, n'a qu'une seule extension finie de degré donné et que cette extension est le corps de décomposition d'un polynôme de la forme $X^q - X$, i.e. est donc normale, le lemme (**2.52**) implique le résultat voulu. ■

Définition 2.54 (Polynôme d'Eisenstein) **:**
Soient (K, v) *un corps valué à valuation discrète d'uniformisante* π, $P \in \mathcal{O}[X]$ *unitiare et* (a_i) *tels que* $P = \sum_{i=0}^{n} a_i X^i$, *on dit que* P *est un polynôme d'Eisenstein si* $v(a_n) = 0$, *pour tout* $i \neq n$ $a_i \in \mathfrak{M}$ *et* $v(a_0) = v(\pi)$.

Lemme 2.55 :
Tout polynôme d'Eisenstein est irréductible.

Proof. Soit P un polynôme d'Eisenstein, supposons que $P = QR$ où Q et $R \in K[X]$. Soient (q_i) (respectivement (r_j)) les coefficients de Q (respectivement R) et q_{i_0} (respectivement R_{j_0}) le premier coefficient dont la valuation est minimale. On a alors $(q_{i_0} r_{j_0})^{-1} P = q_{i_0}^{-1} Q r_{j_0}^{-1} R$ et le polynôme à droite de l'égalité est dans $\mathcal{O}[X]$. Le coefficient dominant de ce polynome $(q_{i_0} r_{j_0})^{-1}$ est dans $\mathcal{O}$ et donc $v((q_{i_0} r_{j_0})^{-1}) \geqslant 0$, i.e. $v(q_{i_0}) + v(r_{i_0}) \leqslant 0$. Mais si on considère le $i_0 + j_0$-ième coefficient de P, on a $v(\sum_{i+j=i_0+j_0} q_i r_j) \geqslant 0$. Si $i < i_0$ alors $v(q_i r_j) < v(q_{i_0} r_{j_0})$ et de même si $j < j_0$ et donc $v(q_{i_0} r_{j_0}) = v(\sum_{i+j=i_0+j_0} q_i r_j) \geqslant 0$. On a donc montré que $v(q_{i_0}) = -v(r_{i_0})$ et donc $q_{i_0} R \in \mathcal{O}[X]$. Comme $P = q_{i_0}^{-1} Q q_{i_0} R$, on peut supposer que Q et R sont dans $\mathcal{O}[X]$.
Mais comme $res(P) = cX^n$ pour un certain $c \in k^\star$, $res(Q)$ et $res(R)$ qui le divisent sont aussi de cette forme et donc $res(q_0) = res(Q)(0) = 0$ et de même $res(r_0) = 0$, il s'en suit donc que le coefficient constant de P qui est $q_0 r_0$ a une valuation d'au moins $2v(\pi)$ ce qui est absurde.
■

Lemme 2.56 :
Soient (K, v) *un corps complet de valuation discrète. Les extensions purement ramifiées de* K *sont exactement les corps de rutpures de polynomes d'Eisenstein.*

Proof. Soit $(K, v) \leqslant (L, w)$ une extension purement ramifiée. Comme dans la preuve de la proposition **(2.50)**, on montre que L est à valuation discrète et que si Π est une uniformisante de L et π une uniformisante de K et que $[L : K] = e$ alors $ew(\Pi) = v(\pi)$ et $L = K[\Pi]$. Soit alors $P \in K[X]$ le polynôme minimal unitaire de Π. Montrons qu'il est d'Eisenstein. Tout d'abord, remarquons que si $\sigma \in \mathrm{Aut}(\overline{K}^{alg}/K)$, $\sigma(\Pi)$ engendre une extension isomorphe à L et donc par unicité de l'extension de v (car K est hensélien), l'anneau de valuation de $K[\sigma(\Pi)]$ muni d'une extension w' de w à $\overline{K}^{alg}$ est $\sigma(\mathcal{O}_L)$ et son idéal maximal est $\sigma(\Pi\,\mathcal{O}_L) = \sigma(\Pi)\sigma(\mathcal{O}_L)$. Il s'en suit donc que $\sigma(\Pi)$ est une uniformisante de $K[\sigma(\Pi)]$ muni de w' et donc que $ew'(\sigma(\Pi)) = v(\pi) = ew(\Pi)$. Comme un groupe abélien totalement ordonné est sans torsion, on doit avoir $w'(\sigma(\Pi)) = w(\Pi)$.
Comme tous les coefficients de P peuvent s'exprimer comme des polynômes symétriques des racines dont les seuls coefficients sont des 1, il s'en suit tous les coefficients de P sauf le coefficient dominant sont dans $\mathfrak{M}_L$ or $\mathfrak{M}_L \cap K = \mathfrak{M}_K$ et donc tous les coefficients de P sauf le coefficient dominant, sont dans $\mathfrak{M}_K$. De plus a_0 est le produit des e conjugués de Π et donc $v(a_0) = ew(\Pi) = v(\pi)$. On a donc bien montré que P est un polynôme d'Eisenstein.
Supposons maintenant que L soit engendré au dessus de K par une racine b d'un polynôme d'Eisenstein P de degré n. Comme les polynômes d'Eisenstein sont irréductibles (voir lemme **(2.55)**), $[L : K] = n$. De plus par le même argument que précédemment, les conjugués de b ont la même valuation et si a_0 est le coefficient constant de P, alors $nw(b) = v(a_0) = v(\pi)$ et donc $[\Gamma_L : \Gamma_K] \geqslant n$ or c'est aussi au plus n et donc l'extension est purement ramifiée. ∎

Lemme 2.57 (Lemme de Krasner) **:**
Soient (K, v) *un corps complet et* a *et* $b \in \overline{K}^{alg}$ *(muni d'une valuation* w *qui étend* v*) tel que* a *soit séparable au dessus de* $K[b]$*. Supposons que pour tout* a' *conjugué de* a *au dessus de* K*, on ait* $w(b - a) > w(a' - a)$*, alors* $K[a] \subseteq K[b]$.

Proof. Soit L une extension normale de K contenant a et b. Si $a \notin K[b]$, il a un conjugué au dessus de $K[b]$ et donc comme l'extension est normale il existe $\sigma \in \mathrm{Aut}(L/K[b])$ qui ne fixe pas a. Par unicité de l'extension de la valuation, on a $v(\sigma(a) - b) = v(\sigma(a - b)) = v(a - b)$ et donc $v(b - a) > v(\sigma(a) - a) = v(\sigma(a) - b + b - a) \geqslant v(b - a)$, ce qui est absurde. On a donc $a \in K[b]$. ∎

Soit (K, v) un corps valué, on munit $K[X]$ de la norme $|\sum a_i X^i| = \max_i(v(a_i))$.

Corollaire 2.58 :
Soient (K, v) *un corps complet et* $P \in K[X]$ *un polynôme unitaire irréductible et séparable. Si* $G \in K[X]$ *est un polynôme unitaire de même degré tel que* $|P - Q|$ *est assez grand, alors* G *est aussi irréductible et pour toute racine* α *de* P *(dans une clôture algébrique fixée de* K*) il existe une racine* β *de* Q *tel que* $K[\alpha] = K[\beta]$.

Proof. Montrons tout d'abord que pour tout $M \neq \infty$ il existe $N \neq \infty$ tel que si $|P - Q| > N$ alors pour toute racine α de P il existe une racine β de Q telle que $v(\alpha - \beta) > M$. Soient β_i

les racines de Q, supposons que pour tout i, $v(\alpha - \beta_i) \leqslant M$. On a alors $v(P(\alpha) - Q(\alpha)) = v(Q(\alpha)) = v(\prod_i \alpha - \beta_i) \leqslant nM$ où n est le degré de P. Mais on a aussi, si on note a_j les coefficients de P et b_j ceux de Q, $v(P(\alpha) - Q(\alpha)) = v(\sum_j (a_j - b_j)\alpha^j) \geqslant \min_j(v(a_j - b_j) j v(\alpha)) \geqslant |P - Q| + \min_j(j v(\alpha))$. On a donc $|P - Q| \leqslant nM - \min_j(j v(\alpha))$ ce qui est absurde si on pose $N = nM - \min_j(j v(\alpha))$.
Notons alors α_i les racines de P et posons $M = \max_{i \neq j}(v(\alpha_i - \alpha_j))$ qui est bien différent de ∞ car P est séparable. Soit alors N tel que dans le paragraphe précédent, si $|Q - P| > N$, pour tout i, il existe β_{j_i} tel que $v(\alpha_i - \beta_{j_i}) > M \geqslant v(\alpha_i - \alpha_k)$ pour tout $k \neq i$. Par le lemme de Krasner (**2.57**), on a alors $K[\alpha_i] \subseteq K[\beta_{j_i}]$, mais comme $[K[\beta_{j_i}] : K] \leqslant \deg(Q) = n = [K[\alpha_i] : K]$, on a $K[\alpha_i] = K[\beta_{j_i}]$ et donc Q est le polynôme minimal annulateur de β_{j_i}, i.e. il est irréductible. ■

Lemme 2.59 :
Soit (K, v) un corps complet de valuation discrète et de corps résiduel fini, alors $\mathcal{O}$ est compact.

Proof. Soient π une uniformisante de K et $(a_n)_{n \in \mathbb{N}}$ une suite d'éléments de $\mathcal{O} = B_{\geqslant 0}(0)$, il suffit de montrer qu'on peut en extraire une suite convergente. On construit b_i par récurrence de telle façon que la boule $B_{\geqslant i v(\pi)}(b_i)$ contienne une infinité d'éléments de la suite (a_n) et que ces boules forment une suite décroissante. On peut poser $b_0 = a_0$. Supposons que b_i soit construit, par le lemme (**2.12**), la boule $B_{\geqslant i v(\pi)}(b_i)$ est recouverte par une union finie des boules de rayon $i + 1$. Comme $B_{\geqslant i v(\pi)}(b_i)$ contient une infinité d'éléments de (a_n) c'est aussi le cas d'un de ces sous-boules. On pose b_{i+1} le premier élément de la suite après b_i à être dans cette sous-boule.
Cette suite vérifie que pour tout N, si i et j sont supérieurs à N alors b_i et b_j sont tous les deux dans la boule $B_{\geqslant N v(\pi)}(b_N)$ et donc $v(b_i - b_j) \leqslant N$. C'est donc une suite de Cauchy car le groupe de valeurs de K est Archimédien. Comme le corps est complet, elle converge. ■

Lemme 2.60 :
Soit (K, v) un corps complet de valuation discrète et de corps résiduel fini, alors K a un nombre fini d'extension purement ramifiées d'un degré donné.

Proof. Soit E_d l'ensemble des polynômes d'Eisenstein de degré d, par définition des polynômes d'Eisenstein, on a $E_d = \mathcal{O}^\star \times \mathfrak{M}^{d-1} \times (\mathfrak{M} \setminus \mathfrak{M}^2)$. Comme la valuation est discrète toutes les boules sont ouvertes et fermées et donc tous les ensembles qui apparaissent dans ce produit sont fermés, inclus dans $\mathcal{O}$, or par le lemme (**2.59**) $\mathcal{O}$ est compact, donc ils le sont tous. Il s'en suit que E_d est compact pour la topologie produit. Soit $L \geqslant K$ une extension purement ramifiée de degré d, on pose $U_L = \{P \in E : L \text{ est un corps de rupture pour } P\}$. D'après le lemme (**2.56**), et comme les polynômes d'Eisenstein sont irréductibles, les U_L recouvrent E_d. Mais par le corollaire (**2.58**) ces ensembles sont ouverts pour la topologie produit. Comme E_d est compact, il est recouvert par un nombre fini de U_L, i.e. il existe n extensions $L_1, \dots L_n$ telles que tout polynôme d'Eisenstein sur K de degré d admet l'un des L_i comme corps de rupture. Quitte à agrandir un peu n on peut supposer que tous les conjugués (qui sont en nombre finis) des L_i au dessus de K sont parmi les L_i. Soit alors $L \geqslant K$ une extension purement ramifiée de degré d, par le lemme (**2.56**), c'est le corps de rupture d'un polynôme d'Eisenstein qui admet donc un des L_i comme corps de rupture. Il s'en suit que L est conjugué à ce L_i au dessus de K et donc est lui même l'un des L_i. ■

Proposition 2.61 :
Soit (K, v) *un corps complet de corps résiduel fini et à valuation discrète, alors* K *a un nombre fini d'extensions de degré donné.*

Proof. Comme on l'a montré dans la proposition (**2.50**), toute extension finie de K est la composée d'une extension purement inertielle et d'une extension purement ramifiée. Soit alors $n \in \mathbb{N}^*$. Il existe un nombre fini de façon d'écrire n sous la forme ef avec e et $f \in \mathbb{N}^*$. D'après le corollaire (**2.53**), il existe une unique extension purement inertielle de K de degré f. Cette extension finie est aussi complète par le corollaire (**2.8**) et, comme le groupe de valeur ne change pas, évidemment aussi à valuation discrète. Par le lemme (**2.60**), ce corps a donc un nombre fini d'extensions purement ramifiées de degré e. ■

Proposition 2.62 :
Soit $(\mathbb{Q}_p, v_p) \leqslant (K, v)$ *une extension finie, il existe alors* $\alpha \in \overline{\mathbb{Q}}^{alg}$ *tel que* $K = \mathbb{Q}_p[\alpha]$, *que* $\mathcal{O}_K = \mathbb{Z}_p[\alpha]$ *et que le polynôme minimal annulateur de* α *au dessus de* $\mathbb{Q}_p$ *soit dans* $\mathbb{Q}$.

Proof. Soient a et Π tels que $K = \mathbb{Q}_p[a, \Pi]$, $\mathcal{O}_K = \mathbb{Z}_p[a, \Pi]$, $\mathbb{Q}_p \leqslant \mathbb{Q}_p[a]$ est purement inertielle, le polynôme minimal de a est dans $\mathbb{Z}_p[X]$ et $\mathbb{Q}_p \leqslant \mathbb{Q}_p[\Pi]$ est purement ramifiée (cette décomposition est donnée à la proposition (**2.50**)). Comme $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$ est que $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$, quitte à remplacer a et Π par des racines de polynômes assez proches de leurs polynômes minimaux, on peut supposer que le polynôme minimal de Π est dans $\mathbb{Q}[X]$ et que celui de a est dans $\mathbb{Z}[X]$. Il est alors facile de vérifier que Π est alors toujours une uniformisante.
Posons alors $\alpha = a + \Pi$. On sait alors qu'il existe un polynôme P dans $\mathbb{Q}[X]$ de degré n qui annule α. Soit Q le polynôme minimal de a, d'après la formule de Taylor, $Q(\alpha) = Q(a) + \Pi Q'(a) + \sum_i \frac{Q^{(i)}(a)}{i!}\Pi^i = Q(a) + \Pi Q'(a) + \Pi^2 b$ où $b \in \mathcal{O}_K$. Comme $\mathrm{res}(a)$ engendre k_K au dessus de $\mathbb{F}_p$, que $[k_K : \mathbb{F}_p] = \deg(Q) = \deg(\mathrm{res}(Q))$ et que $\mathrm{res}(Q)(\mathrm{res}(a)) = \mathrm{res}(Q(a)) = 0$, il s'en suit que Q est $\mathrm{res}(Q)$ est irréductible et donc, comme $\mathbb{F}_p$ est parfait, que $\mathrm{res}(Q'(a)) \neq 0$, i.e. $v(Q'(a)) = 0$. Il s'en suit donc que $v(Q(\alpha)) = v(\Pi)$, i.e. $Q(\alpha)$ est une uniformisante. Comme $\mathrm{res}(\alpha) = \mathrm{res}(a)$ est un élément primitif de $k_K \leqslant \mathbb{F}_p$, d'après la remarque (**2.51**), la famille $\alpha^i Q(\alpha)^j$, et donc la famille (α^i), génère K au dessus de $\mathbb{Q}_p$ et $\mathcal{O}_K$ au dessus de $\mathbb{Z}_p$. Le polynôme P est donc bein irréductible et est donc bien le polynôme minimal annulateur de α. ■

Théorème 2.63 :

> *Soit* $(K, v) \models \mathrm{pCF}$, *alors* K *a un nombre fini d'extensions d'un degré donné et elles sont toutes engendrées par un élément algébrique sur* $\mathbb{Q}$ *qui engendre aussi l'anneau de valuation et dont le polynôme minimal annulateur au dessus de* K *est dans* $\mathbb{Q}$.

Proof. On a montré aux propositions (**2.61**) et (**2.62**) que ces propriétés sont vraies pour $\mathbb{Q}_p$, il suffit donc de montrer qu'elles sont exprimables au premier ordre. Fixons alors un degré n et $P_1, \dots P_k$ des polynômes de degré n à coefficients dans $\mathbb{Q}$ tels que leurs corps de rupture sont les extensions de degré n de $\mathbb{Q}_p$ et qu'une de leur racine dans un corps de rupture engendre l'anneau de valuation.
Mais les extensions finies de degré n d'un corps sont définissables de façon uniforme avec pour paramètres les coefficients du polynôme minimal d'un élément primitif. On peut donc

exprimer au premier ordre que dans toute extension L de degré donné il y a un élément α qui annule un des P_i. De plus on peut exprimer au premier ordre que l'anneau engendré par α au dessus de $\mathcal{O}_K$ est un anneau de valuation. Comme K est hensélien, c'est donc l'unique anneau de valuation au dessus de $\mathcal{O}_K$ et c'est donc forcément $\mathcal{O}_L$. ■

2.5 Élimination des imaginaires dans pCF

Dans cette section, on reprendra les notations de la proposition (**1.53**) avec $\mathcal{L} = \mathcal{L}^{\mathcal{G}}_{\mathbb{Q}_p}$, $T = \mathrm{pCF}^{\mathcal{G}}$, $\widetilde{\mathcal{L}} = \mathcal{L}^{\mathcal{G}}_{\mathrm{div}}$ et $\widetilde{T} = \mathrm{ACVF}^{\mathcal{G}}_{0,p}$. On rappelle que $\mathcal{M}$ est un modèle de $\mathrm{pCF}^{\mathcal{G}}$ assez saturé et homogène et que $\widetilde{\mathcal{M}}$ est un modèle de $\mathrm{ACVF}^{\mathcal{G}}_{0,p}$ qui contient M et qui est lui même assez saturé et homogène.
Montrons maintenant que les hypothèses de la proposition (**1.53**) sont vérifiées.

Proposition 2.64 ((i) dans pCF) **:**
Soient $M' \preccurlyeq M$ *deux modèles de* T *et* $c \in \mathrm{dom}(M)$*, on a alors* $\mathrm{dcl}_{\mathcal{L}}(M'c) \cap M \subseteq \mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c)$.

Proof. Comme $\mathrm{acl}_{\widetilde{\mathcal{L}}}(\mathrm{dom}(M')c) = \overline{\mathrm{dom}(M')c}^{\mathrm{alg}}$ d'après la remarque (**1.32.i**), on a montré à la proposition (**2.24**) que $\mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap \mathrm{dom}(M) = \mathrm{acl}_{\widetilde{\mathcal{L}}}(\mathrm{dom}(M')c) \cap \mathrm{dom}(M)$ est un modèle de pCF. Par modèle complétude, on a $\mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap \mathrm{dom}(M) \preccurlyeq \mathrm{dom}(M)$ et donc $\mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap M^{\mathrm{eq}} = (\mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap \mathrm{dom}(M))^{\mathrm{eq}} \preccurlyeq M^{\mathrm{eq}}$. Comme $\mathcal{L}^{\mathcal{G}}_{\mathbb{Q}_p}$ est une extension définissable de $\mathcal{L}^{\mathrm{eq}}_{\mathbb{Q}_p}$, on a donc aussi $\mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap M \preccurlyeq M$. Enfin, comme la clôture définissable ne dépend pas du modèle dans une extension élémentaire, on a bien que $\mathrm{dcl}_{\mathcal{L}}(M'c) \cap M \subseteq \mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap M \subseteq \mathrm{acl}_{\widetilde{\mathcal{L}}}(M'c)$. ■

Proposition 2.65 ((ii) dans pCF) **:**
Pour tout $A = \mathrm{acl}_{\mathcal{L}}(A) \cap M$ *et* $c \in \mathrm{dom}(M)$*, on a* $\mathrm{acl}_{\mathcal{L}}(Ac) = \mathrm{dcl}_{\mathcal{L}}(Ac)$ *et donc, en particulier,* $\mathrm{acl}_{\mathcal{L}}(Ac) \cap M \subseteq \mathrm{dcl}_{\mathcal{L}}(Ac) \cap M$.

Proof. D'après le corollaire (**2.29**), on a, pour tout $A \subseteq K(M)$, $\mathrm{acl}_{\mathcal{L}}(Ac) \cap K(M) = \mathrm{dcl}_{\mathcal{L}}(Ac) \cap K(M)$. Or cet ensemble est un modèle de pCF et donc $\mathrm{acl}_{\mathcal{L}}(Ac) \subseteq (\mathrm{acl}_{\mathcal{L}}(Ac) \cap K(M))^{\mathrm{eq}} = \mathrm{dcl}_{\mathcal{L}}((\mathrm{acl}_{\mathcal{L}}(Ac) \cap K(M))) = \mathrm{dcl}_{\mathcal{L}}((\mathrm{dcl}_{\mathcal{L}}(Ac) \cap K(M))) = \mathrm{dcl}_{\mathcal{L}}(Ac)$. Il faut cependant étendre ce résultat à des ensembles de paramètres imaginaires (et pas uniquement dans la sorte du corps).
Soit $A = \{a_i : i \in \kappa\}$ une énumération de A. Pour tout i, soit $c_i \in \mathrm{dom}(M)$ tel que $a_i \in \mathrm{dcl}_{\mathcal{L}}(c_i)$ (qui existe par définition des sortes dominantes) et $p_i \in S_{\mathcal{L}}(M)$ une extension $\mathrm{Aut}_{\mathcal{L}}(\mathcal{M}/A)$-invariante de $\mathrm{tp}_{\mathcal{L}}(c_i/A)$ (qui existe par la proposition (**2.46**)). On construit alors $(A_i)_{i \in \kappa}$ par induction. On pose $A_0 = A$, $A_{i+1} = A_i \cup \{b_i\}$ où $b_i \models p_i | \mathrm{acl}_{\mathcal{L}}(A_i c)$ et $A_\lambda = \bigcup_{i<\lambda} A_i$ pour tout i et $\lambda < \kappa$. Montrons alors, par induction, que $\mathrm{acl}_{\mathcal{L}}(Ac) \cap \mathrm{dcl}_{\mathcal{L}}(A_i c) \subseteq \mathrm{dcl}_{\mathcal{L}}(Ac)$. Le cas $i = 0$ est évident et pour λ limite, $\mathrm{acl}_{\mathcal{L}}(Ac) \cap \mathrm{dcl}_{\mathcal{L}}(A_\lambda c) = \bigcup_{i<\lambda} \mathrm{acl}_{\mathcal{L}}(Ac) \cap \mathrm{dcl}_{\mathcal{L}}(A_i c) \subseteq \mathrm{dcl}_{\mathcal{L}}(Ac)$. Reste alors le cas successeur. Soient $a \in \mathrm{acl}_{\mathcal{L}}(Ac) \cap \mathrm{dcl}_{\mathcal{L}}(A_{i+1} c)$ et $\sigma \in \mathrm{Aut}_{\mathcal{L}}(\mathcal{M}/A_i c)$. Comme $a \in \mathrm{dcl}_{\mathcal{L}}(A_{i+1} c)$, il existe $\varphi[x, y, z] \in \mathcal{L}_{A_i}$ telle que a est définit pas $\varphi[x, c, b_{i+1}]$. Comme $a \in \mathrm{acl}_{\mathcal{L}}(Ac) \subseteq \mathrm{acl}_{\mathcal{L}}(A_i c)$, il s'en suit que $\varphi[a, c, z] \in p_{i+1} | \mathrm{acl}_{\mathcal{L}}(A_i c)$ et comme p_{i+1} est $\mathrm{Aut}_{\mathcal{L}}(\mathcal{M}/A)$-invariant et que $\sigma(a) \in \mathrm{acl}_{\mathcal{L}}(Ac)$, on a aussi $\varphi[\sigma(a), c, z] \in$

$p_{i+1} | \mathrm{acl}_{\mathcal{L}}(A_i c)$ et donc $\mathcal{M} \vDash \varphi[\sigma(a), c, b_{i+1}]$. Il s'en suit donc que $\sigma(a) = a$ et donc que $a \in \mathrm{dcl}_{\mathcal{L}}(A_i c)$. On a donc $\mathrm{acl}_{\mathcal{L}}(Ac) \cap \mathrm{dcl}_{\mathcal{L}}(A_{i+1} c) \subseteq \mathrm{acl}_{\mathcal{L}}(Ac) \cap \mathrm{dcl}_{\mathcal{L}}(A_i c) \subseteq \mathrm{dcl}_{\mathcal{L}}(Ac)$.
Pour tout i, $a_i \in \mathrm{dcl}_{\mathcal{L}}(b_i)$ et donc, comme $b_i \in \mathrm{dom}(M)$, $A \subseteq \mathrm{dcl}(A_k \cap \mathrm{dom}(M))$. On a alors $\mathrm{acl}_{\mathcal{L}}(Ac) \subseteq \mathrm{acl}_{\mathcal{L}}(A_\kappa \cap \mathrm{dom}(M) c) \subseteq \mathrm{dcl}_{\mathcal{L}}(A_\kappa \cap \mathrm{dom}(M) c) \subseteq \mathrm{dcl}_{\mathcal{L}}(A_\kappa c)$. Il s'en suit donc que $\mathrm{acl}_{\mathcal{L}}(Ac) = \mathrm{acl}_{\mathcal{L}}(Ac) \cap \mathrm{dcl}_{\mathcal{L}}(A_\kappa c) \subseteq \mathrm{dcl}_{\mathcal{L}}(Ac)$. ■

Pour ce qui est du (iii), on peut même en montrer une version un petit peu plus forte.

Proposition 2.66 ((iii′) dans pCF) **:**
Soit $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M) \subseteq \widetilde{\mathcal{M}}$, il existe alors $e' \in M$ tel que tout automorphisme de $\widetilde{\mathcal{M}}$ qui laisse M globalement fixe, fixe e si et seulement si il fixe e', et $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(e')$.

Proof. Supposons tout d'abord que $e \in K(\widetilde{\mathcal{M}})$. D'après la remarque (**1.32.ii**), comme $K(M)$ est Hensélien et qu'on est en caractéristique nulle, $K(M)$ est $\mathrm{dcl}_{\widetilde{\mathcal{L}}}$-clos. On a donc $e \in K(M)$.
Si maintenant, $e \in K(\widetilde{\mathcal{M}})$, comme $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M) \subseteq \mathrm{acl}_{\widetilde{\mathcal{L}}}(M)$ et que $\mathrm{acl}_{\widetilde{\mathcal{L}}}(M) \vDash \mathrm{ACVF}^{\mathcal{G}}_{0,p}$ (la preuve est similaire à celle de la proposition (**2.64**) dans le cas de $\mathrm{pCF}^{\mathcal{G}}$), il s'en suit que e a une base dans $\mathrm{acl}_{\widetilde{\mathcal{L}}}(M)$. Il existe donc une extension finie $K(\mathcal{M}) \leqslant L$, telle que e ait une base dans L. Soit $m = [L : K(\mathcal{M})]$. On sait par le théorème (**2.63**), qu'il y a un nombre fini d'extensions de degré m au dessus de $K(\mathcal{M})$. Soit alors L' l'union de toutes ces extensions. L'extension $K(\mathcal{M}) \leqslant L'$ est toujours finie et si σ est un automorphisme de $K(\widetilde{\mathcal{M}})$ qui fixe globalement $K(\mathcal{M})$ alors il fixe globalement L. En effet, si a est algébrique de degré m au dessus de $K(\mathcal{M})$, alors $\sigma(a)$ aussi et donc $\sigma(a) \in L'$. On a donc $\sigma(L') \subseteq L'$ et comme ces deux extensions sont de même degré, elles sont égales. Quitte à remplacer L par L', on peut donc supposer que L vérifie cette même propriété que tout automorphisme de $K(\widetilde{\mathcal{M}})$ qui fixe globalement M fixe globalement L.
Soit alors $a \in \overline{\mathbb{Q}}^{\mathrm{alg}}$ tel que $L = K(\mathcal{M})[a]$, que $\mathcal{O}_L = \mathcal{O}_{\mathcal{M}}[a]$ et dont le polynôme minimal annulateur est dans $\mathbb{Q}$. On connaît l'existence d'un tel a par le théorème (**2.63**). Ce a permet donc de définir une bijection $f_a : L \to K(\mathcal{M})^m$ qui induit une bijection $f_a^n : L^n \to K(\mathcal{M})^{mn}$. On pose alors $e' = f_a^n(e)$. Comme $\mathcal{O}_L$ est un $\mathcal{O}_{\mathcal{M}}$-module libre de rang m (la famille des a^i en est une base), s est un $\mathcal{O}_{\mathcal{M}}$ module libre de rang mn. Il est facile de voir que f_a^n est un isomorphisme de $\mathcal{O}_{\mathcal{M}}$-modules et il s'en suit donc que e' est bien dans $\mathcal{S}_{mn}(\mathcal{M})$.
Si a' est un conjugué de A au dessus de $\mathbb{Q}$, comme le polynôme minimal annulateur de a au dessus de $K(\mathcal{M})$ est dans $\mathbb{Q}$, c'est aussi le polynôme minimal annulateur au dessus de $\mathbb{Q}$ et donc a et a' sont conjugués au dessus de $K(\mathcal{M})$. Il existe donc $\sigma \in \mathrm{Aut}(L/K(\mathcal{M}))$ un automorphisme de corps, qui envoie a sur a'. De plus, comme e et $e' \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$ (à vrai dire on a même $e' \in M$), ces deux points sont fixés par σ et donc $f^n_{\sigma(a)}(e) = e'$. Il s'en suit donc que tout automorphisme de $\widetilde{\mathcal{M}}$ qui fixe globalement M fixe globalement f_a et donc fixe e si et seulement s'il fixe e'.
Il reste alors à démontrer que $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(e')$. Mais l'inverse de $g_a : (x_0 \dots x_{m-1}) \mapsto \sum_i x_i a^i$ peut être étendue par la même formule en un $\mathcal{O}_{\widetilde{\mathcal{M}}}$-module $\widetilde{g}_a : K(\widetilde{\mathcal{M}})^m \to K(\widetilde{\mathcal{M}})$, qui induit donc un morphisme de $\mathcal{O}_{\widetilde{\mathcal{M}}}$-module $\widetilde{g}_a^n : K(\widetilde{\mathcal{M}})^{mn} \to K(\widetilde{\mathcal{M}})^n$. Ce morphisme envoie une base de e' sur une base de e, on a donc $\widetilde{g}_a^n(e') = e$. Comme précédemment $\widetilde{g}_a = \widetilde{g}_{a'}$ pour tout conjugué de a au dessus de $\mathbb{Q}$ et donc tout automorphisme de $\widetilde{\mathcal{M}}$ qui fixe e' fixe bien e, i.e. $e \in \mathrm{dcl}(e')$.

Pour ce qui est des $e \in \mathcal{T}_n(\widetilde{\mathcal{M}})$, on peut procéder de la même manière ou remarquer que si L est un extension finie de $K(\mathcal{M})$ telle que $s = \tau_n(e)$ a une base dans L alors comme la valuation de $K(\mathcal{M})$ est discrète, celle de L aussi et donc, si Π est une uniformisante de L, $\mathfrak{M}_L\, s = \Pi s$ est toujours un réseau de L. Par le lemme (**1.58**), ses translatés (dont e) codés dans $\mathcal{S}_{n+1}(L)$. Soit alors $s \in \mathcal{S}_{n+1}(L)$ qui code e. Comme on a déjà traité le cas des réseaux, on peut trouver e' tel que tout automorphisme de $\widetilde{\mathcal{M}}$ qui fixe globalement M fixe s si et seulement si il fixe e'. Mais comme il fixe s si et seulement si il fixe e, on a bien le résultat voulu. De plus, comme s est un code de e, on a $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(s)$ et, comme on l'a montré précédemment, $s \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(e')$. Il s'en suit donc que $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(e')$ ■

Corollaire 2.67 :
Soient X un ensemble $\widetilde{\mathcal{L}}_M$-définissable sans quantificateurs et $A' \subseteq M^{eq}$ tel que $A' = \mathrm{dcl}_{\mathcal{L}}(A')$. Si $\langle X\rangle \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$ est $\mathrm{Aut}(\ \mathrm{mod}^{eq}/A')$-invariant (on rappel que l'action de $\mathrm{Aut}(\mathcal{M}^{eq}/A')$ sur $\langle X\rangle$ est bien définie car toute les extension d'un même morphisme de $\mathcal{M}$ à $\widetilde{\mathcal{M}}$ sont égales sur $\mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$), alors X est $\widetilde{\mathcal{L}}_A$-définissable sans quantificateurs, où $A = A' \cap M$.

Proof. Comme X un ensemble $\widetilde{\mathcal{L}}_M$-définissable sans quantificateurs, il a un code $\langle X\rangle \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$. D'après la proposition (**2.66**), il existe $\bar{e}' \in M$ tel que tout automorphisme de $\widetilde{\mathcal{M}}$ qui fixe globalement M fixe $\langle X\rangle$ si et seulement si il fixe $\bar{e}'$ et que $\langle X\rangle \in \mathrm{dcl}(\bar{e}')$. Il suffit donc de montrer que $\bar{e}' \in A$. Soit $\sigma \in \mathrm{Aut}(\mathcal{M}^{eq}/A')$ et $\widetilde{\sigma}$ une extension de σ à $\widetilde{\mathcal{M}}$ (qui laisse bien M globalement invariant). Par hypothèse, $\widetilde{\sigma}(\langle X\rangle) = \langle X\rangle$ et donc $\widetilde{\sigma}(\bar{e}') = \bar{e}'$. Il s'en suit donc que $\bar{e}' \in \mathrm{dcl}_{\mathcal{L}}(A') = A'$ et comme $\bar{e}' \in M$, on a bien $\bar{e}' \in A$. ■

Proposition 2.68 ((iv) dans pCF) **:**
Tout sous-ensemble X M-définissable inclus dans $\mathrm{dom}(M)$ a un code dans M.

Proof. Soit x un code de X dans $\mathcal{M}^{eq}$. On pose $A = \mathrm{acl}_{\mathcal{L}}(x)$ et $B = \mathbb{B}(A)$. D'après le corollaire (**2.43**), pour tout $c \in \mathrm{dom}(M)$, on a $\mathrm{tp}(c/B) \Rightarrow \mathrm{tp}(c/A)$, en particulier, tous les types sur B impliquent soit X soit $\neg X$. Il s'ensuit que X est laissé invariant par les automorphismes de M^{eq} qui fixent B et donc, par compacité, X est B-définissable. On a donc montré que X a un code faible, mais on sait que les ensembles finis sont codés par le lemme (**1.54**) (et la proposition (**2.66**)) et donc le lemme (**1.47**) permet de conclure. ■

Avant de traiter le cas de l'hypothèse (v), il nous faut définir quelques notions et montrer quelques lemmes.

Définition 2.69 (Boule générique) **:**
Soient $A \subseteq \widetilde{M}$ et P une intersection stricte de boules A-définissables. Une boule générique dans P au dessus de A, est une sous-boule fermée de P qui contiennent strictement toutes les sous-boules strictes de P qui sont A-définissables et dont le rayon est strictement inférieur à tous les $\gamma \in P_\Gamma(A)$. On note $\beta_P|A$ le A-type partiel suivant (dont la variable parcourt l'ensemble des boules fermées) :

$$\beta_P = \{x \subseteq b_i : i \in I\} \cup \{x \not\supseteq b : b \in \mathbb{B}(A) \text{ et } b \not\subseteq P\} \cup \{\rho(x) < \gamma : \gamma \in P_\Gamma(A)\}.$$

Comme Γ est o-minimal et que les conditions $\rho(b) > \rho(b_i)$ pour $i \in I$ et $\mathrm{rad}b < \gamma$ pour $\gamma \in P_\Gamma(A)$ définissent une coupure de Γ_A, il s'en suit que si b et $b' \vDash \beta_P|A$, alors $\rho(b) \equiv_A \rho(b')$.

Proposition 2.70 :
Soient $A \subseteq \widetilde{M}$ *et* P *une intersection (pas forcément stricte) de boules* A*-définissables,* $\gamma \in \Gamma_{\widetilde{M}}$ *et* b *une sous-boule de* P *telle que* $b \in \mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma) \setminus \mathrm{acl}_{\widetilde{\mathcal{L}}}(A)$*. Alors* $\rho(b) \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(A\gamma)$ *et il existe* $a \in \mathrm{acl}_{\widetilde{\mathcal{L}}}(A)$ *une sous-boule de* P *telle que* $\rho(a) > \rho(b)$ *et* $b \in \{B_{\geqslant\gamma}(a), B_{>\gamma}(a)\}$*.*

Proof. TO DO [HHM06, Proposition 2.4.4] ∎

Corollaire 2.71 :
Soient $A \subseteq \widetilde{M}$ *tel que* $A = \mathrm{acl}_{\widetilde{\mathcal{L}}}(A)$ *et* P *une intersection de boules* $\widetilde{\mathcal{L}}_A$*-définissables, si* P *ne contient aucune boule stricte* $\widetilde{\mathcal{L}}_A$*-définissable, alors le type d'une chaîne de* n *boules au dessus de* A *est déterminé par le type de leurs rayons au dessus de* A*.*

Proof. Tout d'abord, soient $(\gamma_i)_{1\leqslant i\leqslant n} \in \Gamma_{\widetilde{M}}$, montrons par récurence sur n que P ne contient aucune boule stricte $\widetilde{\mathcal{L}}_{\mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma_1\dots\gamma_n)}$-définissable. Pour $n = 0$ c'est une trivialité. Supposons maintenant que l'on ait montré que c'est vrai pour n et soit b une boule $\widetilde{\mathcal{L}}_{\mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma_1\dots\gamma_{n+1})}$-définissable strictement incluse dans P. Par hypothèse de récurrence, elle ne peut pas être $\widetilde{\mathcal{L}}_{\mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma_1\dots\gamma_n)}$-définissable, et donc la proposition (**2.70**) implique qu'il existe une boule b' $\widetilde{\mathcal{L}}_{\mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma_1\dots\gamma_n)}$-définissable incluse dans b et donc strictement incluse dans P, ce qui est absurde.
Soit alors $(b_i)_{1\leqslant i\leqslant n}$ et $(b'_i)_{1\leqslant i\leqslant n}$ deux chaînes de n boules telles que $\rho(b_1)\dots\rho(b_n) \equiv_A \rho(b'_1)\dots\rho(b'_n)$. Quitte à appliquer un isomorphisme de $\widetilde{\mathcal{M}}$ qui fixe A, on peut supposer que pour tout i, $\rho(b_i) = \rho(b'_i) = \gamma_i$. De plus on vient de montrer que P ne contient pas de sous-boule stricte $\widetilde{\mathcal{L}}_{\mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma_1\dots\gamma_n)}$-définissable. Soit alors $x \in b_1$ et $x' \in b'_1$, ils sont tous les deux génériques dans P au dessus de $\mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma_1\dots\gamma_n)$. Comme $\alpha_P|\mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma_1\dots\gamma_n)$ est complet, il existe $\sigma \in \mathrm{Aut}(\widetilde{\mathcal{M}}/A\gamma_1\dots\gamma_n)$ qui envoit x sur x'. Mais alors pour tout i, $\sigma(b_i)$ et b'_i contiennent toutes deux x' et sont toutes deux de rayon γ_i, i.e. elles sotn égales. ∎

Corollaire 2.72 (Complétude de β_P) **:**
Soient $A \subseteq \widetilde{M}$ *tel que* $A = \mathrm{acl}_{\widetilde{\mathcal{L}}}(A)$ *et* P *une intersection stricte de boules* $\widetilde{\mathcal{L}}_A$*-définissables, alors* $\beta_P|A$ *est complet.*

Proof. Soient b et $b' \vDash \beta_P|A$, comme on a remarqué précédemment, il s'en suit que $\rho(b) \equiv_A \rho(b')$. D'une part, si P ne contient aucune boule $\widetilde{\mathcal{L}}_A$-définissable, alors par le corollaire (**2.71**), $b \equiv_A b'$. D'autre part, si il existe $a \in \mathbb{B}(A)$, alors $a \subseteq b$ et $a \subseteq b'$. De plus, comme $\rho(b) \equiv_A \rho(b')$, il existe $\sigma \in \mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A)$ tel que $\sigma(\rho(b)) = \rho(b')$. Comme a est fixé par σ, on a $a \subseteq (\sigma(b))$. Les boules $\sigma(b)$ et $\sigma(b')$ ont alors le même rayon et ne sont pas disjointes, elles sont donc égales. ∎

Le lemme qui suit est le lemme 5.4 de [HM08].

Lemme 2.73 :
Soient $A \subseteq \widetilde{\mathcal{M}}$ *tel que* $A = \mathrm{acl}_{\widetilde{\mathcal{L}}}(A)$ *et* $(s_b)_{b\vDash\beta_P|A}$ *une famille de fonctions de* $\mathrm{dom}(\widetilde{M})$ *dans* $\widetilde{M}^n$ $\widetilde{\mathcal{L}}_A$*-définissable uniformément en* b*. Supposons de plus qu'il existe une fonction* r $\widetilde{\mathcal{L}}_{\widetilde{M}}$*-définissable telle que pour tout* $b \vDash \beta_P|A$*, on ait* $\partial_{\alpha_b} r = \partial_{\alpha_b} s_b$*. Il existe alors une fonction* s $\widetilde{\mathcal{L}}_A$*-définissable telle que* $\partial_{\alpha_P} s = \partial_{\alpha_P} r$*.*

Proof. Supposons tout d'abord que P a une sous-boule $a \in \mathbb{B}(A)$. On pose alors $s(x) = s_{B_{\geqslant v(x-a)}(a)}(x)$ qui est bien une fonction $\widetilde{\mathcal{L}}_A$-définissable. Soient alors $b \models \beta_P|A$ et $x \models \alpha_b|\operatorname{acl}_{\widetilde{\mathcal{L}}}(Ab)$. Comme $x \in b$ et $a \subseteq b$ car b est générique au dessus A, il s'en suit que $v(x-a) \geqslant \rho(b)$. De plus $x \notin B_{>\rho(b)}(a)$ car c'est une sous-boule stricte de b, et donc $v(x-a) = \rho(b)$. On a donc $s(x) = s_{B_{\geqslant\rho(b)}(a)}(x) = s_b(x)$, i.e. $\partial_{\alpha_b} s = \partial_{\alpha_b} s_b$. Montrons maintenant que $\partial_{\alpha_P} s = \partial_{\alpha_P} r$. Si ce n'était pas le cas r et s ne seraient égaux au plus sur b une sous-boule de P. Soit alors b' un sous-boule de P qui contient b et qui est générique au dessus de A. Par hypothèse, pour tout $t \models \alpha_b|\operatorname{acl}_{\widetilde{\mathcal{L}}}(A\langle r\rangle)$, on a $r(t) = s_b(t)$, or comme $s(t) \neq r(t)$, cela contredit le fait que $\partial_{\alpha_b} s = \partial_{\alpha_b} s_b$.
Supposons maintenant que P ne contient aucune sous-boule $a \in \mathbb{B}(A)$. Soient alors $b_1 \models \beta_P|A$ et $b_2 \models \beta_P|\operatorname{acl}_{\widetilde{\mathcal{L}}}(Ab_1)$. Comme, par hypothèse, $\partial_{\alpha_{b_2}} r = \partial_{\alpha_{b_2}} s_{b_2}$, r et s_{b_2} sont égaux sur $b_2 \backslash e$, où e est une union finie de sous-boules strictes de b. Soit alors b_1' une sous-boule de b_2 qui est disjoint de e et de même rayon que b_1 (une telle boule existe car sinon b serait recouverte par un nombre fini de boules de rayon $\rho(b_1)$, ce qui est absurde car le corps résiduel est infini). On a alors $r_{|b_1'} = s_{b_2|b_1'}$. De plus, comme $\rho(b_1') = \rho(b_1)$, par le corollaire (**2.71**), $b_1' \models s\beta_P|A$ et donc $\partial_{\alpha_{b_1'}} r = \partial_{\alpha_{b_1'}} s_{b_1'}$. Il s'en suit donc que $\partial_{\alpha_{b_1'}} s_{b_2} = \partial_{\alpha_{b_1'}} s_{b_1'}$. Mais, comme b_1' ne contient aucune sous-boule $\operatorname{acl}(A, b_1', b_2)$-définissable (en effet b_1' contient une infinité de boules d'un rayon donné qui ont toutes le même type au dessus de A, b_1', b_2 par le corollaire (**2.71**)), les fonctions s_{b_2} et $s_{b_1'}$ coïncident sur tout b_1'. Comme le fait que $b_1' \models \beta_P|A$ et $b_2' \models \beta_P|\operatorname{acl}_{\widetilde{\mathcal{L}}}(Ab_1')$ définit un type complet au dessus de A, l'égalité que l'on vient de montrer est vraie pour toute paire de boules qui vérifient les même hypothèses.
Soient alors $b_1 \subseteq b_2$ deux sous-boules de P et $b_3 \models \beta_P|\operatorname{acl}_{\widetilde{\mathcal{L}}}(Ab_1b_2)$. On a alors pour $i = 1, 2$, $s_{b_i|b_i} = s_{b_3|b_i}$ et donc s_{b_1} et s_{b_2} coïncident sur b_1. On pose donc $s = \bigcup_{b\subseteq P} s_b$ qui est bien une fonction. Il est alors évident que pour tout boule $b \subseteq P$, $\partial_{\alpha_b} s = \partial_{\alpha_b} s_b$ et donc pas la même preuve que précédemment, $\operatorname{germs}\alpha_P = \partial_{\alpha_P} r$. ∎

Définition 2.74 (Irréductibilité sur un type) **:**
Soient $A \subseteq \widetilde{M}$ *tel que* $A = \operatorname{acl}_{\widetilde{\mathcal{L}}}(A)$, q *un type* $\operatorname{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A)$*-invariant et* $R[x, y]$ *une relation* $\widetilde{\mathcal{L}}_A$*-définissable telle que pour tout* $c \in \widetilde{M}$, $R(c) = R[c, \widetilde{\mathcal{M}}]$ *soit un ensemble fini (on dit que* R *est une pseudo-fonction). On dit que* R *est irréductible sur* q *au dessus de* A *s'il n'existe pas de* $R'[x, y]$ A*-définissable tel que pour* $c \models q|A$, $R'(c)$ *est un sous-ensemble strict non vide de* $R(c)$ *(comme cette propriété s'exprime avec un* $\widetilde{\mathcal{L}}_A$*-formule, il suffit de le vérifier pour un unique* $c \models q|A$*).*

Remarque 2.75 :
Si R *est irréductible sur* q *au dessus de* A *alors pour* $c \models q|A$, $R[c, y]$ *est une formule algébrique complète, i.e. tous les éléments de* $R(c)$ *sont* $\operatorname{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/Ac)$*-conjugués.*

Lemme 2.76 :
Soit $A \subseteq \widetilde{M}$ *tel que* $\operatorname{acl}_{\widetilde{\mathcal{L}}}(A) = A$ *et* P *une intersection de boules* A*-définissables. Soit* f *une fonction* $\widetilde{\mathcal{L}}_{\widetilde{M}}$*-définissable tel que pour tout* $x \in P$, $f(x) \in \operatorname{acl}_{\widetilde{\mathcal{L}}}(Ax)$*. Il existe alors* g *une fonction* A*-définissable qui a le même germe que* f *sur* α_P*.*

Proof. TO DO Voir [HHM06, Lemme 3.4.13]. ∎

Corollaire 2.77 :
Soient $A \subseteq \widetilde{M}$, q *un type* $\mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A)$*-invariant et* R *une pseudo-fonction* $\widetilde{\mathcal{L}}_A$*-définissable et* $B \subseteq \widetilde{M}$ *tel que* $A \subseteq B = \mathrm{acl}_{\widetilde{\mathcal{L}}}(B)$ *et* R *est irréductible sur* q *au dessus de* B*. Alors pour tout* $B' \subseteq \widetilde{M}$ *tel que* $A \subseteq B = \mathrm{acl}_{\widetilde{\mathcal{L}}}(B)$*,* R *est irréductible sur* q *au dessus de* B'*.*

Il est donc inutile de préciser au dessus de quel ensemble un tel R est irréductible sur q.
Proof. Supposons tout d'abord que $B' \subseteq B$. Supposons qu'il existe R' B'-définissable et $c \vDash q|B'$, tel que $\varnothing \neq R'(c) \subsetneq R(c)$. Mais ceci s'exprime avec une formule à paramètres dans B' et est donc vérifiée pour toute réalisation de $q|B'$, en particulier celles de $q|B$, ce qui contredit le fait que R est irréductible sur q au dessus de B.
Supposons maintenant que $B \subseteq B'$. Tout d'abord, comme on l'a déjà fait remarqué, q est le type générique d'une intersection P de boules A-définissables. Supposons qu'il existe R' B'-définissable telle que pour un $c \vDash q|B'$ (et donc pour tous) $\varnothing \neq R'(c) \subsetneq R(c)$. C'est donc aussi vérifié sur un ouvert autour de $q|B'$, et donc quitte à étendre R en dehors de cet ouvert par $R(x) = \varnothing$, on peut supposer que pour tout $c \in P$, $R'(c) \subseteq R(c)$. Comme tout automorphisme qui fixe Bc fixe $R(c)$ qui est un ensemble fini et donc qui a un nombre fini de parties, $R'(c)$ a au plus un nombre fini de conjugués au dessus de Bc. Il s'en suit donc que, si on note $r' : x \mapsto \langle R'(x) \rangle$, pour tout $c \in P$, $r'(c) \in \mathrm{acl}_{\widetilde{\mathcal{L}}}(Bc)$. Par le lemme **(2.76)**, il existe donc une fontion s B-définissable qui a le même germe que r' au dessus de q, i.e. il existe une pseudo-fonction S B-définissable telle que pour tout $c \vDash q|B'$, $S(c) = R'(c)$ et donc $\varnothing \neq S(c) \subsetneq R(c)$. Mais cette dernière affirmation s'exprime avec une formule à paramètres dans B et donc est vérifiée de tout $c \vDash q|B$, ce qui contredit notre hypothèse d'irréductibilité de R sur q au dessus de B. ■

Démontrons maintenant un lemme qui permet de « descendre » l'irréductibilité sur une intersection stricte à des sous-boules génériques (c'est le lemme 5.3 de [HM08]). Mais pour cela il nous faut un autre lemme de [HHM06].

Lemme 2.78 :
Soient $A \subseteq \widetilde{M}$ *tel que* $A = \mathrm{acl}_{\widetilde{\mathcal{L}}}(A)$ *et* $\gamma \in \Gamma_{\widetilde{M}}$*. On alors* $\mathrm{acl}_{\widetilde{\mathcal{L}}}(A\gamma) = \mathrm{dcl}_{\widetilde{\mathcal{L}}}(A\gamma)$*.*

Proof. TO DO voir [HHM06, Lemme 3.4.12] ■

Lemme 2.79 :
Soient $A \subseteq \widetilde{M}$ *tel que* $A = \mathrm{acl}_{\widetilde{\mathcal{L}}}(A)$*,* P *une intersection stricte de boules* $\widetilde{\mathcal{L}}_A$*-définissables et* R *une pseudo-fonction* $\widetilde{\mathcal{L}}_A$*-définissable qui est irréductible sur* α_P*. Alors pour tout* $b \vDash \beta_P|A$*,* r *est irréductible sur* α_b*.*

Proof. Soit $B \subseteq \widetilde{M}$ tel que $\mathrm{acl}_{\widetilde{\mathcal{L}}}(B) = B$, $A \subseteq B$ et B contient un point d de P. Soit $b \vDash \beta_P|B$. On a alors $d \in b$ et b est $\widetilde{\mathcal{L}}_{B\rho(b)}$-définissable. Soit $c \vDash \alpha_b|\mathrm{acl}_{\widetilde{\mathcal{L}}}(B\rho(b))$. Il est aussi générique dans P au dessus de B et donc, par hypothèse, les éléments de $R(c)$ sont $\mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/Bc)$-conjugués. Mais $\rho(b) = v(c - d) \in \mathrm{dcl}(Bc)$ et donc les éléments de $R(c)$ sont $\mathrm{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/\mathrm{dcl}_{\widetilde{\mathcal{L}}}(B\rho(b))c)$-conjugués. Or par le lemme **(2.78)**, $\mathrm{acl}_{\widetilde{\mathcal{L}}}(B\rho(b)) = \mathrm{dcl}_{\widetilde{\mathcal{L}}}(B\rho(b))$. On a dont bien montré que R est irréductible sur α_b.
Soit R' une pseudo-fonction $\widetilde{\mathcal{L}}_A$-définissable. On vient de montrer que pour tout $b \vDash \beta_P|A$, $(\neg(\varnothing \neq R'(x) \subsetneq R(x))) \in \alpha_b$. Comme α_b est b-définissable uniformément en b, il s'en suit

qu'il existe une $\widetilde{\mathcal{L}}_A$-formule $\varphi[b]$ qui exprime exactement ce fait, et comme $\alpha_b|A$ est complet, il suffit que b soit générique au dessus de A pour que pour tout $c \vDash \alpha_b$, $R'(c)$ ne peut pas être un sous-ensemble strict de $R(c)$, i.e. r est irréductible sur α_b. ■

On aura aussi besoin du lemme combinatoire suivant :

Lemme 2.80 :
Soit $M = (P, Q, R)$ *un structure avec* $R \subseteq P^2 \times Q$. *Supposons que :*

(i) *Pour tout* $a \in P$, $\mathrm{acl}(a) \cap Q = \varnothing$.

(ii) *Pour tout* $a \neq b \in P$, $R(a,b) = \{c \in Q : R(a,b,c)\}$ *est fini, de taille bornée et que* $R(a,b) = R(b,a)$.

(iii) *Pour* a, b *et* $c \in P$ *distincts, on a* $R(a,c) \subseteq R(a,b) \cup R(b,c)$.

Alors pour tous a *et* b *distincts,* $R(a,b) = \varnothing$.

Proof. Quitte à prendre une extension élémentaire, on peut supposer la structure assez saturée et homogène. Soient a et $b \in P$ distincts tel que $R(a,b)$ soit de cardinal maximal n. Montrons alors que pour tout $b' \in P$, si $b' \neq b$ et $R(b,b') \neq \varnothing$ alors $R(b,b') \cap R(a,b) \neq \varnothing$. En effet, si $b' = a$ ceci est clair (à moins que $n = 0$ dans quel cas c'est fini). On peut donc supposer $b' \neq a$. Supposons que $R(b,b') \cap R(a,b) = \varnothing$. Comme $R(b,b') \subseteq R(b,a) \cup R(a,b')$ on a $R(b,b') \subseteq R(a,b')$ et de même $R(a,b) \subseteq R(a,b')$. Mais par maximalité du cardinal de $R(a,b)$, on a $R(a,b) = R(a,b')$ et donc $R(b,b') = R(a,b') \cap R(b,b') = R(a,b) \cap R(b,b') = \varnothing$.
Cependant, par (i), $R(a,b) \cap \mathrm{acl}(b) = \varnothing$, i.e. Pour tout $x \in R(a,b)$, son stabilisateur est d'indice infini dans $\mathrm{Aut}(M/b)$. Par le lemme de Neumann, il existe un automorphisme σ qui envoit chacun des points de $R(a,b)$ en dehors de cet ensemble, c'est à dire que $R(a,b)$ et $\sigma(R(a,b)) = R(\sigma(a),b)$ sont disjoints. En itérant cette construction, on obtient des points $(a_i)_{0 \leqslant i \leqslant n}$ conjugués au dessus de b tels que pour tout $i \neq j$, $R(a_i,b) \cap R(a_j,b) = \varnothing$. Comme $R(a_i,b)$ est aussi de cardinal maximal, on a aussi que pour tout $b' \in P$, si $b' \neq b$ et $R(b,b') \neq \varnothing$ alors $R(b,b') \cap R(a_i,b) \neq \varnothing$. En particulier, $R(b,a) \cap R(a_i,b) \neq \varnothing$. Comme les $R(a_i,b)$ sont disjoints, on a donc trouvés $n+1$ éléments distincts de $R(a,b)$ ce qui est contradictoire.
■

Théorème 2.81 :

La théorie $\mathrm{pCF}^{\mathcal{G}}$ *élimine les imaginaires.*

Proof. Le théorème suit (presque) de la proposition (**1.53**). Les hypothèses (i) à (iv) de la proposition sont démontrés dans les propositions (**2.64**),(**2.65**),(**2.66**) et (**2.68**). On ne sait pas démontrer le (v) en général, mais cette hypothèse ne sert que dans la preuve du lemme (**1.56**), il suffirait donc de montrer ce lemme dans le cas précis de pCF.

■

Remarque 2.82 :
*Les torseurs ne sont pas nécessaires dans les corps p-adiquement clos. Comme on a vu dans la preuve du lemme (**2.66**), pour tout* $s \in \mathcal{S}_n(M)$, $\mathfrak{M}$ *s est en fait un réseau et ses translatés sont donc codés par des éléments de* $\mathcal{S}_{n+1}(M)$, *par le lemme (**1.58**).*

Bibliographie

Algèbre

[EP05] A.J. Engler et A. Prestel. *Valued Fields*. Springer Monographs in Mathematics. Springer-Verlag, 2005.

[GSS88] F. J. Grunewald, D. Segal et G. C. Smith. « Subgroups of Finite Index in Nilpotents Groups ». Dans : *Inventiones Mathematicae* 93.1 (1988), p. 185–223.

[Lan02] Serge Lang. *Algebra*. 3rd edition. Graduate Texts in Mathematics 211. Springer-Verlag, 2002.

[Lan94] Serge Lang. *Algebraic Number Theory*. 2nd edition. Graduate texts in Mathematics. Springer-Verlag, 1994.

[Nar74] Wladislaw Narkiewicz. *Elementary and Analytic Theory of Alebraic Numbers*. Polish Scientific Publishers, 1974.

[Rib64] Paulo Ribenboim. *Théorie des valuations*. Les presse de l'université de Montréal, 1964.

[Rib99] Paulo Ribenboim. *The Theory of Classical Valuations*. Springer Monographs in Mathematics. Springer-Verlag, 1999.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, 1968.

Théorie des modèles

[AK65] James Ax et Simon Kochen. « Diophantine Problems Over Local Fields I ». Dans : *American Journal of Mathematics* 87.3 (1965), p. 605–630.

[Cha08] Zoé Chatzidakis. « Théorie des modèles des corps valués ». cours de M2. 2008.

[Den84] Jan Denef. « The rationality of the Poincaré series associated to the p-adic points on a variety ». Dans : *Inventiones Mathematicae* 77 (1984), p. 1–23.

[Dri84] Lou van den Dries. « Algebraic Theories with Definable Skolem Functions ». Dans : *The Journal of Symbolic Logic* 49.2 (1984), p. 625–629.

[HHM06] Deirdre Haskell, Ehud Hrushovski et Dugald Macpherson. « Definable Sets in Algebraically Closed Valued Fields : Elimination of Imaginaries ». Dans : *Journal für die Reine und Angewandte Mathematik* 597 (2006), p. 175–236.

[HM08] Ehud Hrushovski et Ben Martin. « Zeta Functions from Definable Equivalence Relations ». arXiv : math/0701011. 2008.

[Hod93] Wilfrid Hodges. *Model Theory*. Encyclopedia of Mathematics and its Applications 42. Cambridge University Press, 1993.

[Hol95] Jan E. Holly. « Canonical forms for definable subsets of algebraically closed and real closed valued fields ». Dans : *The Journal of Symbolic Logic* 60.3 (1995), p. 843–860.

[Mac76] Angus Macintyre. « On Definable Subsets of p-Adic Fields ». Dans : *The Journal of Symbolic Logic* 41.3 (1976), p. 605–610.

[Poi83] Bruno Poizat. « Une théorie de Galois imaginaire ». Dans : *The Journal of Symbolic Logic* 48.4 (1983), p. 1151–1170.

[Rob56] Abraham Robinson. *Complete Theories*. Studies in Logic 7. North-Holland Publishing Company, 1956.

[She78] Saharon Shelah. *Classification Theory and the Number of Non-Isomorphic Models*. Studies in Logic 92. North-Holland Publishing Company, 1978.

Table des matières