

Élimination des imaginaires
dans les
extensions finies de \mathbb{Q}_p

Silvain Rideau
École Normale Supérieure,
Paris XI

26 février 2012

Table des matières

Introduction	I
1 Élimination des imaginaires dans un cadre abstrait	3
2 Élimination des imaginaires dans ACVF	II
3 Corps p -adiquement clos	16
4 Cloture algébrique et définissable dans $p\text{CF}_{P,f}$	22
5 Les Types unaires dans $p\text{CF}_{P,f}$	24
6 Élimination des imaginaires dans $p\text{CF}_{P,f}$	32
Références	36

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 $\mathbb{Q}_p[X_1, \dots, X_n]$, on note $a_n := \#\{x \bmod p^n : x \in \mathbb{Z}_p^n \wedge \forall i P_i(x) \equiv 0 \bmod p^n\}$ et $\tilde{a}_n := \#\{x \bmod p^n : x \in \mathbb{Z}_p^n \wedge \forall i P_i(x) = 0\}$. Le résultat que Denef démontre est que la série des $\sum_i \tilde{a}_i T^i$ 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 $f : D \rightarrow \mathbb{Q}_p$ telle que pour tout $x \in D$, la mesure de la E -classe de x est égale à $v_p(f(x))$, où v_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 [HHMo6] 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 [HMo8], utilisent ce résultat pour montrer l'élimination des imaginaires pour \mathbb{Q}_p avec les mêmes sortes additionnelles et en déduisent la rationalité des séries de comptage des représentations des groupes finiment engendrés nilpotents.

Le but de ce texte est donc de démontrer le principal résultat de théorie des modèles

de [HMo8] : l'élimination des imaginaires pour la théorie de K extension finie de \mathbb{Q}_p avec les sortes géométriques et d'en profiter pour rappeler, ou 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 d'une extension finie de \mathbb{Q}_p .

Ce texte s'organise en six sections. La première section introduit les notions d'élimination des imaginaires et démontre l'équivalence d'un certain nombre de définitions classiques avant de démontrer le critère abstrait démontré dans [HMo8]. La seconde rappelle le résultat d'élimination des imaginaires pour ACVF démontré dans [HHMo6], en particulier en introduisant le langage géométrique. La troisième section contient les rappels sur les corps p -adiquement clos. Les deux sections suivantes démontrent les préliminaires nécessaires à la démonstration de l'élimination des imaginaires, en premier lieu l'étude des clôtures algébriques et définissables et en second lieu celle des types unaires d'éléments du corps. Pour finir, tout cela est utilisé pour donner 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 $c \equiv_{\mathcal{L}_A} c'$ pour c et c' ont le même \mathcal{L} -type au dessus de A , dans le cas où il n'y a pas d'ambiguïté sur le langage, on notera simplement $c \equiv_A c'$;
- pour tout ensemble définissable (ou infiniment définissable) X et tout ensemble de paramètres A dans un modèle \mathcal{M} , on notera $X(A) := \{a \in \text{dcl}(A) : \mathcal{M} \models X(a)\}$.

I *Élimination des imaginaires dans un cadre abstrait*

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 1.1 (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 $\bar{b}' \in A$ (de la bonne sorte), 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 \emptyset -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 1.2 :

Soit \mathcal{M} une \mathcal{L} -structure telle que $\text{dcl}(\emptyset)$ 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 $\bar{m} \in M$ (de la bonne sorte), $\theta[\mathcal{M}, \bar{m}]$ ait un code, alors ce codage peut être choisi uniformément.

Démonstration. Pour tout $\bar{m} \in M$, on a $\varphi_{\bar{m}}[\bar{x}, \bar{z}]$ une \mathcal{L} -formule 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 $\varphi[\bar{x}, \bar{z}] \wedge (\bigwedge_{j < i} \neg(\exists \bar{z}' \forall \bar{x} \varphi_j[\bar{x}, \bar{z}'] \iff \varphi_i[\bar{x}, \bar{z}]))$, 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 $\varphi_{i_{\bar{m}}}$. Soient c_1 et c_2 les deux constantes de même sorte, on pose alors $\psi[\bar{x}, \bar{z}, \bar{t}] = \bigvee_i (\bigwedge_{j \neq i} t_j = c_2 \wedge t_i = c_1) \wedge \varphi_{i_{\bar{m}}}[\bar{x}, \bar{z}]$, \bar{c}^i le n -uplet $(c_2 \dots c_1 \dots c_2)$ où le c_1 est 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'une 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 (I.II)), les ensembles définissables ne sont pas exactement codés, mais c'est presque le cas (voir lemme (I.IO)). Il existe donc une notion un peu plus large de codage, celui de codage faible.

Définition 1.3 (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 1.4 :

Soient \mathcal{M} une \mathcal{L} -structure, X un ensemble M -définissable et $\bar{a} \in M$. Alors \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 .

Démonstration. Supposons que \bar{a} soit un code de X . Comme X est \bar{a} -définissable, 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 $\text{Aut}(\mathcal{N}/\bar{a})$ -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 $p := \text{tp}(\bar{a})$, 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 $\psi[\bar{y}] \in \text{tp}(\bar{a})$ telle que $\mathcal{N} \models \forall \bar{y} (\psi[\bar{y}] \wedge \forall \bar{x} \varphi[\bar{x}, \bar{y}] \iff \varphi[\bar{x}, \bar{a}]) \Rightarrow \bar{y} = \bar{a}$. Il s'en suit donc que X est codé par \bar{a} via $\varphi[\bar{x}, \bar{y}] \wedge \psi[\bar{y}]$. ■

Définition 1.5 (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 (1.2) 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 les points dits « imaginaires ») par de « vrais » points du modèle.

Lemme 1.6 :

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 définit une fonction f dans T telle que $T \vdash E[\bar{x}, \bar{y}] \iff f(\bar{x}) = f(\bar{y})$.

Démonstration. Soit T qui élimine uniformément les imaginaires, $\mathcal{M} \models T$ 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, Définition 6.2, p. 129]) à travers la construction suivante, dont l'utilité en théorie des modèles n'est plus à démontrer.

Définition 1.7 (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 $E[\bar{x}, \bar{y}]$ \emptyset -définissable (où \bar{x} et \bar{y} ont la même longueur) telle que $T \Rightarrow \ll E \text{ est une relation d'équivalence} \gg$, une sorte S_E et un symbole de fonction $f_E : S_- \rightarrow S_E$. 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 $\mathcal{M}^{\text{eq}} \models T^{\text{eq}}$ 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 donc la structure de \mathcal{M} et de tous ses imaginaires.

Remarque 1.8 (Quelques propriétés de \mathcal{M}^{eq}) :

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

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

où S_{E_i} est la sorte de x_i .

- (ii) Si $\mathcal{M} \models T^{\text{eq}}$ et $N \subseteq M$ alors $\mathcal{N} \models T^{\text{eq}}$ si et seulement si $S_=(N) \models T$.
- (iii) Si $\mathcal{N} \leq \mathcal{M}$ alors $\mathcal{N}^{\text{eq}} \leq \mathcal{M}^{\text{eq}}$.
- (iv) Si T est modèle-complète alors T^{eq} l'est aussi. Néanmoins, si T élimine les quantificateurs, ce n'est pas forcément le cas de T^{eq} .
- (v) T^{eq} élimine uniformément les imaginaires.

Lemme 1.9 :

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 $\text{dcl}^{\text{eq}}(\bar{a}) = \text{dcl}^{\text{eq}}(\langle X \rangle)$, où $\langle X \rangle$ est un code de X dans M^{eq} et X est faiblement codé par \bar{a} si et seulement si $\langle X \rangle \in \text{dcl}^{\text{eq}}(\bar{a})$ et $\bar{a} \in \text{acl}^{\text{eq}}(\langle X \rangle)$.

Démonstration. Quitte à agrandir \mathcal{M} , on peut le supposer assez saturé et homogène. Si X est codé par \bar{a} , un automorphisme de M^{eq} fixe X si et seulement si il fixe $\langle X \rangle$ si et seulement si il fixe \bar{a} et on a donc bien que $\bar{a} \in \text{dcl}^{\text{eq}}(\langle X \rangle)$ et $\langle X \rangle \in \text{dcl}^{\text{eq}}(\bar{a})$. 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 $\bar{a} \in \text{acl}^{\text{eq}}(\langle X \rangle)$. Comme X est définissable sur \bar{a} on a aussi bien sûr $\langle X \rangle \in \text{dcl}^{\text{eq}}(\bar{a})$. Réciproquement, si $\langle X \rangle \in \text{dcl}^{\text{eq}}(\bar{a})$, il existe $\varphi[x, \bar{a}]$ qui définit X . Si l'on note $p := \text{tp}(\bar{a})$ et n la taille de son orbite au dessus de $\langle X \rangle$, par une compacité à peine plus compliquée qu'au lemme (1.4), 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 par \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 1.10 :

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.

Démonstration. 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 M^{eq}) et $\sigma \in \text{Aut}(M^{\text{eq}}/\langle X \rangle)$. 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 $\bar{a}' \in E$, $\varphi[x, \bar{a}']$ définit 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 1.11 :

- (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) $\text{Th}(\mathbb{Q}, <)$ élimine les imaginaires, mais pas uniformément. Soit $\varphi[x, y, y'] := y = y'$, on a alors $\varphi[\mathcal{M}, a, b] = M$ ou \emptyset . 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 $\theta[\mathcal{M}, \bar{c}_2] = \emptyset$ 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 $\text{Th}(\mathbb{Q}, <)$ ne contient aucune constante. On a donc (si le langage n'a qu'une sorte) une réciproque du lemme (I.2).

- (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 $\text{acl}(\emptyset)$ 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 \emptyset -définissable d'un produit des S_i sur S qui soit surjective. Pour tout modèle $\mathcal{M} \models T$, on note alors $\text{dom}(M) = \bigcup_{i \in I} S_i(\mathcal{M})$.

Pour démontrer le critère abstrait de [HMo8], on a besoin de la notion de germe que l'on commence donc par définir.

Définition I.12 (Germe) :

Soient \mathcal{M} une \mathcal{L} -structure, f_1 et f_2 des fonction M -définissable définies par $\varphi_i[\bar{x}, \bar{y}, \bar{m}_i]$ pour $i = 1, 2$, où $\bar{m}_i \in M$. Soit $p \in S(M)$ un type tel que les f_i soient définies sur p . On dit que les f_i ont le même germe sur p si $(\forall \bar{y} \varphi_1[\bar{x}, \bar{y}, \bar{m}_1] = \varphi_2[\bar{x}, \bar{y}, \bar{m}_2]) \in p$, c'est à dire que f_1 et f_2 coïncident sur une réalisation (et même sur toute réalisation) de $p|\bar{m}_1\bar{m}_2$. On note alors $\partial_p f_1 = \partial_p f_2$.

De plus, si on a $A \subseteq M$ tel que p est $\text{Aut}(\mathcal{M}/A)$ -invariant, on définit l'action de $\text{Aut}(\mathcal{M}/A)$ sur $\partial_p f$, en posant $\sigma(\partial_p f) = \partial_p \sigma(f)$.

Remarque I.13 :

Dans le cas où p est définissable et qu'on se restreint à des fonctions définies uniformément, i.e. $\varphi_1 = \varphi_2$ dans la définition précédente, la relation « f_1 et f_2 (ou plus précisément les fonctions définies par \bar{m}_1 et \bar{m}_2 en utilisant φ) ont le même germe sur p » devient une relation d'équivalence définissable. Donc, si $\text{Th}(\mathcal{M})$ élimine les imaginaires, $\partial_p f$ peut être assimilé à un point de M .

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

Lemme I.14 (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.

Démonstration. Ce lemme est prouvé dans [Neu54, Lemma 4.1, p. 239]. ■

Corollaire I.15 :

Soient M un modèle assez universel et homogène et $(\varepsilon_i)_{i < \kappa}$ une famille de points telle pour tout automorphisme σ de M il existe $\alpha < \kappa$ tel que σ fixe tous les ε_i , pour $i \geq \alpha$. Alors il existe $\alpha < \kappa$ tel que pour tout $i \geq \alpha$, les ε_i ont une orbite finie sous l'action des automorphismes de M .

Démonstration. Supposons par l'absurde que ce ne soit pas le cas. Quitte à se restreindre à un intervalle cofinal, on peut supposer que tous les ε_i ont une orbite infinie. Montrons qu'il existe alors un automorphisme qui ne fixe aucun de ces ε_i .

Montrons tout d'abord que pour tout ensemble fini de ε_i il existe des automorphismes qui n'en fixent aucun. Soient donc $\varepsilon_{i_1}, \dots, \varepsilon_{i_n}$ des éléments de la suite et notons H_j le stabilisateur de ε_j dans $G = \text{Aut}(M)$. Comme tous ces sous-groupes sont d'indice infini (leur indice est égal au cardinal de l'orbite de ε_i correspondant), par le lemme de Neumann (voir (I.14)) $\bigcup_i H_i \not\subseteq G$. Tout $\tau \in G \setminus \bigcup_i H_i$ convient.

Notons alors $p := \text{tp}(\bar{\varepsilon})$. L'ensemble de formules $p[\bar{c}] \cup p[\bar{d}] \cap \bigcup_i \{c_i \neq d_i\}$ est alors finiment satisfaisable dans \mathcal{M} . En effet, il suffit de prendre $c_i = \varepsilon_i$ pour tous les i qui apparaissent et si σ est un automorphisme qui ne fixe aucun des ε_i qui apparaissent, de prendre $d_i = \sigma(\varepsilon_i)$. Soit alors \mathcal{N} un modèle (petit) dans lequel cet ensemble est satisfaisable. Par universalité de \mathcal{M} , $\mathcal{N} \subseteq \mathcal{M}$ et, comme $\text{tp } \bar{c}^{\mathcal{N}} = \text{tp}(\bar{\varepsilon}/)$, on a une application élémentaire qui envoie $c_i^{\mathcal{N}}$ sur ε_i . On peut l'étendre en un automorphisme de \mathcal{M} . Mais, comme $\text{tp } \bar{\varepsilon} = \text{tp } \sigma(\bar{d}^{\mathcal{N}})$, on a aussi une application élémentaire qui envoie $\sigma(c_i^{\mathcal{N}}) = \varepsilon_i$ 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 ε_i , ce qui est absurde. ■

On peut alors, comme on l'a déjà annoncé, démontrer le critère abstrait de [HMo8], qui sera appliqué pour démontrer l'élimination des imaginaires dans les corps p -adiquement clos.

Proposition I.16 :

Soient $\tilde{\mathcal{L}} \subseteq \mathcal{L}$ deux langages, \tilde{T} une $\tilde{\mathcal{L}}$ -théorie complète qui admet l'élimination des quantificateurs (en conséquence, toutes les $\tilde{\mathcal{L}}$ -formules considérées seront sans quantificateurs) et l'élimination des imaginaires, T une \mathcal{L} -théorie complète telle que $\tilde{T}_{\forall} \subseteq T$ (i.e. tout modèle de T se plonge en tant que $\tilde{\mathcal{L}}$ -structure dans un modèle de \tilde{T}).

Soient $\mathcal{M} \models T$ suffisamment saturé et homogène et $\tilde{\mathcal{M}} \models \tilde{T}$ tel que $\mathcal{M} \upharpoonright_{\tilde{\mathcal{L}}}$ est une sous-structure de $\tilde{\mathcal{M}}$ (quitte à le grossir, on peut également le supposer suffisamment saturé et homogène). On note $\text{dcl}_{\tilde{\mathcal{L}}}$ la clôture définissable par des $\tilde{\mathcal{L}}$ -formules sans quantificateurs dans $\tilde{\mathcal{M}}$ et $\text{dcl}_{\mathcal{L}}^{\text{eq}}$ la clôture définissable par des \mathcal{L} -formules dans \mathcal{M}^{eq} . De même pour $\text{acl}_{\mathcal{L}}^{\text{eq}}$, $\text{acl}_{\tilde{\mathcal{L}}}^1$, $\text{tp}_{\mathcal{L}}^2$ et $\text{tp}_{\tilde{\mathcal{L}}}$.

On suppose que :

- (i) pour tout $\mathcal{M}_0 \leq \mathcal{M}$ et $c \in \text{dom}(M)$, $\text{dcl}_{\mathcal{L}}^{\text{eq}}(M_0 c) \cap M \subseteq \text{acl}_{\tilde{\mathcal{L}}}(M_0 c)$;
- (ii) pour tout $A \subseteq M$ tel que $A = \text{acl}_{\mathcal{L}}^{\text{eq}}(A) \cap M$ et $c \in \text{dom}(M)$, $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap M \subseteq \text{dcl}_{\tilde{\mathcal{L}}}^{\text{eq}}(Ac) \cap M$;
- (iii) soit $e \in \text{dcl}_{\tilde{\mathcal{L}}}(M)$, il existe $e' \in M$ tel que tout $\tilde{\mathcal{L}}$ -automorphisme de $\tilde{\mathcal{M}}$ qui fixe globalement M , fixe e si et seulement si il fixe e' ;
- (iv) tout ensemble $X \subseteq \text{dom}(M)$ M -définissable³ a un code dans M ;

1. Il faut cependant faire attention que M^{eq} n'est pas, a priori, inclus dans $\tilde{\mathcal{M}}$ et donc que pour $A \subseteq M$, $\text{dcl}_{\mathcal{L}}^{\text{eq}}(A)$ et $\text{acl}_{\mathcal{L}}^{\text{eq}}(A)$ ne sont pas inclus dans $\tilde{\mathcal{M}}$.

2. Pour ce dernier, on ne précise pas le eq car on cette notation ne sera utilisé que pour des types d'éléments réels sur des paramètres réels.

3. Cette propriété est alors aussi vraie pour les ensembles M^{eq} -définissables

- (v) soient $c \in \text{dom}(M)$ et $A \subseteq M$ tel que $\text{acl}_{\mathcal{L}}^{\text{eq}}(A) \cap M = A$. Il existe un type $\tilde{p} \in S_{\tilde{\mathcal{L}}}(\tilde{M})$ $\text{Aut}_{\tilde{\mathcal{L}}}(\tilde{M}/A)$ -invariant tel que $\tilde{p}|_M$ soit consistant avec $\text{tp}_{\mathcal{L}}(c/A)$ et que pour toute fonction f $\tilde{\mathcal{L}}_M$ -définissable, telle que $\tilde{p} \subseteq \mathcal{D}_f$, on ait :
- (*) il existe $(\varepsilon_i)_{i < \kappa} \in \text{dcl}_{\tilde{\mathcal{L}}}(A \langle f \rangle)$, tel que $\sigma \in \text{Aut}_{\tilde{\mathcal{L}}}(\tilde{M}/A)$ fixe $\partial_{\tilde{p}} f$ si et seulement si il existe $\alpha < \kappa$ tel que σ fixe tous les ε_i pour $i \geq \alpha$;

La théorie T élimine alors les imaginaires.

Démonstration. Avant de commencer la preuve, comme ceci sera utilisé tout au long de la preuve, expliquons comment $\text{Aut}_{\mathcal{L}}(\mathcal{M}^{\text{eq}})$ agit sur \tilde{M} . Tout automorphisme σ de \mathcal{M}^{eq} provient d'un automorphisme de \mathcal{M} qui est une $\tilde{\mathcal{L}}$ -application élémentaire et qu'on peut donc étendre en un automorphisme $\tilde{\sigma}$ de \tilde{M} . Comme σ ne peut s'étendre à $\text{dcl}_{\tilde{\mathcal{L}}}(M)$ que d'une seule façon, cette action est bien définie sur $\text{dcl}_{\tilde{\mathcal{L}}}(M)$ et donc (via son code) sur tout ensemble $\tilde{\mathcal{L}}_M$ -définissable.

Continuons en remarquant une conséquence immédiate de la condition (iii).

Lemme 1.17 :

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

Démonstration. 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 \tilde{M} . Soit e un code dans \tilde{M} , comme $e \in \text{dcl}_{\tilde{\mathcal{L}}}(M)$, soit $e' \in M$ donné par (iii). Soit alors $\sigma \in \text{Aut}_{\mathcal{L}}(M)$ que l'on s'étend en $\tilde{\sigma} \in \text{Aut}_{\tilde{\mathcal{L}}}(\tilde{M})$. On a alors que σ fixe E si et seulement si $\tilde{\sigma}$ fixe E (car $E \subseteq M$) si et seulement si $\tilde{\sigma}$ fixe e , si et seulement si $\tilde{\sigma}$ fixe e' (par définition car $\tilde{\sigma}$ 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 les lemmes (1.10) et (1.17), il suffit de montrer que T élimine faiblement les imaginaires. Soit donc $e \in M^{\text{eq}}$, il faut qu'on montre que cet imaginaire a un code faible dans M , i.e. par le lemme (1.9), il faut montrer que $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(\text{acl}_{\mathcal{L}}^{\text{eq}}(e) \cap M)$. Soient $(c_i)_{1 \leq i \leq n} \in \text{dom}(M)$ tels que $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(c_1 \dots c_n)$ (qui existent car $\text{dom}(M)$ est dominant dans M qui est dominant dans M^{eq}). On pose $A_l = \text{acl}_{\mathcal{L}}^{\text{eq}}(ec_1 \dots c_l) \cap M$ et on montre par récurrence (décroissante) sur l que $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l)$ (ce qui conclura la preuve car on veut exactement montrer que $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_0)$). Comme les c_i sont dans A_n , on a bien $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_n)$.

Tout d'abord montrons que pour tout l ,

$$\text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l e) \cap M = \text{acl}_{\mathcal{L}}^{\text{eq}}(A_l e) \cap M = A_l \tag{1}$$

En effet,

$$\begin{aligned} \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l e) \cap M &\subseteq \text{acl}_{\mathcal{L}}^{\text{eq}}(A_l e) \cap M \\ &= \text{acl}_{\mathcal{L}}^{\text{eq}}(e \text{acl}_{\mathcal{L}}^{\text{eq}}(ec_1 \dots c_l) \cap M) \cap M \\ &\subseteq \text{acl}_{\mathcal{L}}^{\text{eq}}(e \text{acl}_{\mathcal{L}}^{\text{eq}}(ec_1 \dots c_l)) \cap M \\ &= \text{acl}_{\mathcal{L}}^{\text{eq}}(ec_1 \dots c_l) \cap M \\ &= A_l \end{aligned}$$

Supposons maintenant qu'on ait montré que $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_{l+1})$. Comme

$$\begin{aligned} \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_{l+1}) &= \text{dcl}_{\mathcal{L}}^{\text{eq}}(\text{acl}_{\mathcal{L}}^{\text{eq}}(ec_1 \dots c_{l+1}) \cap M) \\ &\subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(\text{acl}_{\mathcal{L}}^{\text{eq}}(eA_l c_{l+1}) \cap M) \end{aligned}$$

où la dernière inclusion provient du fait que $c_1 \dots c_n \in A_l$, il existe $\bar{d} \in \text{acl}_{\mathcal{L}}^{\text{eq}}(A_l e c_{l+1}) \cap M$ et une fonction \mathcal{L}_{A_l} -définissable g telle que $g(\bar{d}) = e$. Comme pour tout conjugué \bar{d}' de \bar{d} au dessus de $A_l e c_{l+1}$, on a $g(\bar{d}') = e$, quitte à remplacer \bar{d} par le code de son orbite (finie) au dessus de $A_l e c_{l+1}$, on peut supposer que $\bar{d} \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l e c_{l+1}) \cap M$. Il existe donc une fonction \mathcal{L}_{A_l} -définissable $f(x, y)$ telle que $e = g(f(e, c_{l+1}))$. On notera aussi $f_e(c)$ pour $f(e, c)$.

On note alors p le type de $\text{tp}_{\mathcal{L}}(c_{l+1}/A_l)$, $\tilde{p} \in S_{\tilde{\mathcal{L}}}(\tilde{M})$ le type donné par (v) , Φ l'ensemble des fonctions $\tilde{\mathcal{L}}_M$ -définissables φ telles que pour tout x , $\varphi(x)$ soit un ensemble fini (on parle alors de pseudo-fonction) et pour tout $c \in \mathcal{D}_{f_e}$ (le domaine de définition de f_e), $f_e(c) \in \varphi(c)$ et Φ_m l'ensemble des $\varphi \in \Phi$ telles que pour $c \models \tilde{p}$, $|\varphi(c)| = m$ (comme \tilde{p} est un type complet, ce m est bien défini quelque soit la réalisation de p considérée).

Lemme 1.18 :

L'ensemble Φ est non vide.

Démonstration. Soit $\mathcal{M}_0^{\text{eq}} \leq \mathcal{M}^{\text{eq}}$ (petit) qui contient $A_l e$. Pour tout $c \in \mathcal{D}_{f_e}$, on a $f_e(c) \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(M_0 c) \cap M \subseteq \text{acl}_{\tilde{\mathcal{L}}}(M_0 c)$, par (i). Il existe donc une pseudo-fonction $\tilde{\mathcal{L}}_{M_0}$ -définissable φ (qui dépend de c) telle que $f_e(c) \in \varphi(c)$. L'ensemble $\mathcal{L}_{A_l e}$ -définissable \mathcal{D}_{f_e} est donc recouvert par l'union des formules $f_e(x) \in \varphi(x)$ où φ parcourt l'ensemble des pseudo-fonctions $\tilde{\mathcal{L}}_{M_0}$ -définissables. Par compacité de $S_{\mathcal{L}^{\text{eq}}}(M_0^{\text{eq}})$, il existe un nombre fini de φ_i telles que $\mathcal{D}_{f_e} \subseteq \bigcup_{i=1}^n \ll f_e(x) \in \varphi_i(x) \gg$ et donc la pseudo-fonction $\varphi(x) = \bigcup_{i=1}^n \varphi_i(x)$ est dans Φ . \spadesuit

Soit alors m_0 minimal tel que Φ_{m_0} soit non vide.

Lemme 1.19 :

Tous les $\varphi \in \Phi_{m_0}$ ont le même germe au dessus de \tilde{p} . En particulier, $\partial_{\tilde{p}}\varphi$ est $\text{Aut}_{\mathcal{L}}(\mathcal{M}^{\text{eq}}/A_l e)$ -invariant.

Démonstration. Soit φ et $\varphi' \in \Phi_{m_0}$. Comme, pour tout $c \in \mathcal{D}_{f_e}$, $f_e(c) \in \varphi(c) \cap \varphi'(c)$, la pseudo-fonction définie par $\varphi''(c) = \varphi(c) \cap \varphi'(c)$ est aussi dans Φ et comme $|\varphi''(c)| \leq |\varphi(c)|$, pour tout $c \models \tilde{p}$, on a $|\varphi''(c)| = |\varphi(c)|$, i.e. $\varphi(c) = \varphi'(c)$.

De plus, si φ' est un conjugué de φ au dessus de $A_l e$, comme f_e est $A_l e$ invariant, on a $\varphi' \in \Phi$ et comme \tilde{p} est A_l -invariant, pour tout $c \models \tilde{p}$, $|\varphi'(c)| = m_0$ et donc $\varphi' \in \Phi_{m_0}$. Ils ont donc bien le même germe sur \tilde{p} . \spadesuit

On choisit alors une pseudo-fonction $F_{\bar{E}}$ dans Φ_{m_0} définie sur $\bar{E} \in M$.

Lemme 1.20 :

Le germe de $F_{\bar{E}}$ est $\text{Aut}_{\mathcal{L}}(M/A_l)$ -invariant.

Démonstration. Considérons les $\varepsilon_i \in \text{dcl}_{\tilde{\mathcal{L}}}(A_l \langle F_{\bar{E}} \rangle) \subseteq \text{dcl}_{\tilde{\mathcal{L}}}(M)$ comme dans le (v) et pour tout i , le $\varepsilon'_i \in M$ donné par le (iii). Tout automorphisme $\sigma \in \text{Aut}_{\mathcal{L}}(\mathcal{M}/A_l e)$ s'étend comme expliqué précédemment en un $\tilde{\sigma} \in \text{Aut}_{\tilde{\mathcal{L}}}(\tilde{\mathcal{M}}/A_l)$ qui laisse M globalement fixe. Mais comme, par le lemme (1.19), $\partial_{\tilde{p}} F_{\bar{E}}$ est laissé fixe par $\tilde{\sigma}$, il s'en suit qu'il existe $\alpha < \kappa$ tel que pour tout

$i \geq \alpha$, $\tilde{\sigma}$ fixe ε_i et donc σ fixe ε'_i , par définition des ε'_i . Par le corollaire (1.15) (appliqué dans le modèle $\mathcal{M}_{A_l e}^{\text{eq}}$), il existe $\alpha < \kappa$ tel que pour tout $i \geq \alpha$, $\varepsilon'_i \in \text{acl}_{\mathcal{L}}^{\text{eq}}(A_l e) \cap M = A_l$, par (1). Tout automorphisme $\sigma \in \text{Aut}(\mathcal{M}/A_l)$ fixe donc ε'_i et donc ε_i pour $i \geq \alpha$. Par définition des ε_i , σ fixe donc aussi $F_{\bar{E}}$. \clubsuit

Lemme 1.21 :

Soit $e' \in M^{\text{eq}}$ et $c, c' \in \text{dom}(M)$ tels que $e' \equiv_{\mathcal{L}_{A_l}} e$ et $c \equiv_{\mathcal{L}_{A_l}} c'$, alors $ce \equiv_{\mathcal{L}_{A_l}} c'e'$.

Démonstration. Montrons tout d'abord que $c \equiv_{\mathcal{L}_{A_l e}} c'$. Soit $X \subseteq M$ $\mathcal{L}_{A_l e}$ -définissable. Par (iv) il a un code $\langle X \rangle \in M$. Ce code est dans $\text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l e) \cap M = A_l$ (par l'équation (1)), donc X est \mathcal{L}_{A_l} -définissable et donc $c \in X \iff c' \in X$.

De plus, il existe un automorphisme $\sigma \in \text{Aut}_{\mathcal{L}}(\mathcal{M}^{\text{eq}}/A_l)$ qui envoie e sur e' . Soit $c'' = \sigma^{-1}(c')$, alors $c'' \equiv_{\mathcal{L}_{A_l}} c$ et donc, comme on vient de le démontrer, $c'' \equiv_{\mathcal{L}_{A_l e}} c$. Il existe alors $\tau \in \text{Aut}_{\mathcal{L}}(\mathcal{M}^{\text{eq}}/A_l e)$ qui envoie c sur c'' . La composée $\sigma \circ \tau \in \text{Aut}_{\mathcal{L}}(\mathcal{M}/A_l)$ envoie e sur e' et c sur c' , ce qui permet de conclure. \clubsuit

Lemme 1.22 :

On a $e \in \text{acl}_{\mathcal{L}}^{\text{eq}}(A_l)$.

Démonstration. Il suffit de démontrer que si $(e_i, \bar{E}_i)_{i \in \mathbb{N}}$ est une suite indiscernable dans M au dessus de A_l telle que $e_0 = e$ et $\bar{E}_0 = \bar{E}$, alors $e_i = e$ pour tout i .

Soit $c \models \tilde{p}|A(\bar{E}_i)_{i \in \mathbb{N}}$ tel que $c \models p$ (qui existe car $\tilde{p}|M$ est consistant avec p). Comme les $F_{\bar{E}_i}$ sont conjugués au dessus de A_l , par le lemme (1.20), on a « $F_{\bar{E}}(x) = F_{\bar{E}_i}(x)$ » $\in \tilde{p}$ et donc pour tout i , $F_{\bar{E}}(c) = F_{\bar{E}_i}(c)$ que l'on note donc par la suite $F(c)$.

De plus, pour tout $i \in \mathbb{N}$, il existe $\sigma \in \text{Aut}_{\mathcal{L}}(\mathcal{M}^{\text{eq}}/A_l)$ qui envoie e_i sur e et \bar{E}_i sur \bar{E} . Comme $\sigma(c) \equiv_{\mathcal{L}_{A_l}} c \equiv_{\mathcal{L}_{A_l}} c_{i+1}$, on a $\sigma(c)e \equiv_{\mathcal{L}_{A_l}} c_{i+1}e$, par le lemme (1.21), et donc $\sigma(c) \in \mathcal{D}_{f_e}$. Par définition de Φ , on a donc $f_e(\sigma(c)) \in F_{\bar{E}}(\sigma(c))$ et donc $f_{\sigma^{-1}(e)}(c) \in F_{\sigma^{-1}(\bar{E})}(c)$, i.e. $f_{e_i}(c) \in F_{\bar{E}_i}(c) = F(c)$ qui est un ensemble fini. Il existe donc une infinité (en particulier deux) i tels que les f_{e_i} sont égaux.

Comme $e = g(f(e, c_{i+1}))$, par le lemme (1.21), $e_i = g(f(e_i, c))$ et il y a donc deux e_i qui sont égaux. Comme la suite est indiscernable, tous les e_i sont égaux. \clubsuit

Rappelons qu'on avait $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(\bar{d})$ avec $\bar{d} \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l c_{l+1} e) \subseteq \text{acl}_{\mathcal{L}}^{\text{eq}}(A_l c_{l+1} \text{acl}_{\mathcal{L}}^{\text{eq}}(A_l)) = \text{acl}_{\mathcal{L}}^{\text{eq}}(A_l c_{l+1}) \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l c_{l+1})$ (la deuxième inclusion vient du lemme (1.22) et la dernière de l'hypothèse (ii)). Il s'en suit donc que $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l c_{l+1})$. Il existe donc une fonction \mathcal{L}_{A_l} -définissable telle que $e = h(c_{l+1})$. Soit $X = h^{-1}(e) \subseteq \text{dom}(M)$ qui a un code $e' \in M$ par (iv). Il est clair que $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l e')$ et $e' \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l e) \cap M = A_l$, d'où $e \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_l)$. \blacksquare

2 Élimination des imaginaires dans ACVF

Le but de cette section est de rappeler les résultats déjà connus dans ACVF qui seront utiles par la suite.

Une première conséquence de la modèle complétude de ACVF est que l'on sait exactement ce que sont les clôtures algébriques et définissables.

Remarque 2.1 :

- (i) La modèle complétude nous permet de comprendre la clôture algébrique dans ACVF. En effet, soit $(K, v) \models \text{ACVF}$ et $A \subseteq K$. Comme \mathcal{L}_{div} contient le langage des anneaux, il est évident que $\text{acl}(A)$ contient $K' = \overline{\text{Frac}(\langle A \rangle)}^{\text{alg}}$, i.e. la clôture algébrique du corps des fractions de l'anneau engendré par A (que l'on notera dorénavant $\overline{A}^{\text{alg}}$ même si A n'est qu'un ensemble quelconque de paramètres inclu dans le corps). De plus, il est évident que K' est un corps valué algébriquement clos et donc $K' \leq K$, ce qui implique que $\text{acl}(A) \subseteq K' = \overline{A}^{\text{alg}}$ et donc $\text{acl}(A) = \overline{A}^{\text{alg}}$.
- (ii) En revanche, dcl n'est pas la clôture rationnelle comme c'est le cas dans les corps algébriquement clos. C'est en fait la clôture inséparable de l'Hensélianisé. En reprenant les notations précédentes, comme \mathcal{L}_{div} contient le langage des anneaux, $\text{Frac}(\langle A \rangle) \subseteq \text{dcl}(A)$ on peut donc supposer que $A = \text{Frac}(\langle A \rangle)$ et donc que A est un corps. On choisit alors $i : A \rightarrow A^h$ un Hensélianisé de A . Comme K est algébriquement clos (et donc Hensélien) il s'en suit qu'on a $j : A^h \rightarrow K$ tel que $j \circ i$ est l'inclusion de A dans K ⁴. 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 . Pour montrer que σ fixe A^h , il suffit de montrer que $\sigma \circ j = j$ et comme σ fixe A , on sait que $\sigma \circ j \circ i = j \circ i$. Les deux morphismes $\sigma \circ j$ et j sont donc tous les deux solutions du problème universel suivant :

$$\begin{array}{ccc}
 A & \xrightarrow{\sigma \circ j \circ i} & K \\
 & \searrow i & \nearrow \text{---} \\
 & & A^h
 \end{array}$$

et ils sont donc égaux. Il s'en suit que A^h est fixé par σ et donc que $A^h \subseteq \text{dcl}(A)$. Comme \mathcal{L}_{div} contient le langage des anneaux, $\text{dcl}(A)$ doit contenir $K' = \overline{A^h}^{\text{ins}}$, la clôture inséparable de A^h . Montrons alors que $\text{dcl}(A) = K'$.

Soit $x \notin K'$. 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 (3.3), v et $v \circ \sigma$ qui sont deux valuations de K qui coïncident sur K' sont équivalentes, par la proposition (3.2), 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 $x \notin \text{dcl}(A)$.

Une autre conséquence de l'élimination des quantificateurs est un résultat de Holly (voir le théorème (2.3)), 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 $B_{\geq \gamma}(a) := \{x \in K : v(x - a) \geq \gamma\}$, 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 $K \leq L$, l'empreinte d'une boule de L dans K n'est pas forcément une boule.

4. La propriété universelle de l'Hensélianisé qui est utilisée tout au long de ce paragraphe est introduite en (3.4)

Définition 2.2 (Fromage suisse) :

Soit (K, v) un corps valué. Un fromage suisse de K est un ensemble de la forme $b \setminus (\bigcup_{i=1}^n b_i)$ 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.

Théorème 2.3 ([Hol95, Théorème 3.26]) :

Soit $(K, v) \models \text{ACVF}$, tout sous-ensemble définissable de K s'écrit de manière unique comme une union finie de fromages suisses non trivialement emboîtés.

Dans [HHM06], il est démontré que la théorie $\text{ACVF}_{(m,n)}$ 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 a la fois élimination des imaginaires et des quantificateurs.

Définition 2.4 (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 $\mathcal{S}(K) = \bigcup_{n \geq 1} \mathcal{S}_n(K)$ est appelé un réseau de K .

Un réseau de K a donc une base $e_1 \dots e_n$ dans K^n . Deux bases engendrent le même réseau s'il existe une matrice dans $\text{GL}_n(\mathcal{O}_K)$ qui conjugue ces deux bases. On a donc $\mathcal{S}_n(K) \simeq \text{GL}_n(K) / \text{GL}_n(\mathcal{O}_K)$. Il s'en suit donc que pour tout n , \mathcal{S}_n est bien une sorte de K^{eq} . De plus l'ensemble \mathcal{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 $\mathcal{S}_1(K) \simeq \Gamma_K$. D'ailleurs, la surjection canonique $K^* \rightarrow \mathcal{S}_1(K) \simeq \text{GL}_1(K) / \text{GL}_1(\mathcal{O}_K) = K^* / \mathcal{O}_K^* = \Gamma_K$ 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 2.5 :

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 $a + s$.

Démonstration. 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 $h(a + s)$. En effet, supposons que l'on ait $\sum_i \lambda_i (a + e_i, 1) = 0$, où $\lambda_i \in \mathcal{O}_K$. On a alors $(\sum_i \lambda_i a + \sum_{i \geq 1} \lambda_i e_i, \sum_i \lambda_i) = (0, 0)$. Il s'en suit donc que $\sum_i \lambda_i = 0$ et donc $\sum_{i \geq 1} \lambda_i e_i = 0$. Or c'est une famille libre donc pour tout $i \geq 1$, $\lambda_i = 0$ 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 $x = \sum_i \lambda_i (a + e_i, 1)$, où $x_i \in s$. En particulier, $x_i = \sum_{j \geq 1} \mu_j^i e_j$. On a donc $x = \sum_i \lambda_i (a + e_0, 1) + \sum_{i,j} \lambda_i \mu_j^i (e_j, 0)$. 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 $y = \sum_i \lambda_i a + \sum_i \lambda_i x_i = a + \sum_i \lambda_i x_i \in a + s$. L'inclusion réciproque est évidente. Il s'en suit donc que h est une fonction \emptyset -définissable qui injecte les translatés d'éléments de \mathcal{S}_n dans \mathcal{S}_{n+1} , i.e. $a + s$ est codé par $h(a + s)$ via la formule qui définit h . ■

On en déduit immédiatement que l'ensemble des boules fermées dont le rayon est dans Γ_K s'injecte dans $\mathcal{S}_2(K) \cup K$. 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 \mathcal{S}_1 , par le lemme précédent, ils s'injectent bien dans \mathcal{S}_2 . De plus l'image de cette injection est exactement l'ensemble des $e \in \mathcal{S}_2$ qui ont une base de la forme $((a, 1), (b, 1))$.

Définition 2.6 (Torseurs) :

Soit (K, v) un corps valué. On pose $\mathcal{T}_n(K) = \bigsqcup_{s \in \mathcal{S}_n(K)} s / (\mathfrak{M}_K s)$. Un élément de $\mathcal{T}(K) = \bigcup_{n \geq 1} \mathcal{T}_n(K)$ 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 de réseaux s (qui est bien un ensemble définissable) par $\mathfrak{M}_K s$ qui sont bien des sous-groupes définissables.

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 $\mathcal{O}_K / \mathfrak{M}_K$.

Enfin, si h est le code la boule fermée $B_{\geq \gamma}(a)$ défini au lemme (2.5), si h' est l'élément de $h / \mathfrak{M}_K h$ qui contient $(a, 1)$, alors il code la boule ouverte $B_{> \gamma}(a)$ (on retrouve la boule que l'on cherche en projetant l'intersection avec $K \times \{1\}$). L'ensemble des boules ouvertes s'injecte donc dans \mathcal{T}_2 . De plus l'image de cette injection est l'ensemble des torseurs qui proviennent d'un réseau qui code une boule fermée et qui contiennent un point de la forme $(a, 1)$. Ainsi l'ensemble des boules de K , que l'on notera dorénavant \mathbb{B}_K est un sous-ensemble définissable de $K \cup \mathcal{S}_2 \cup \mathcal{T}_2$.

Pour pouvoir définir le langage dans lequel on a à la fois élimination des imaginaires et élimination des quantificateurs pour $\text{ACVF}_{m,n}$, il faut introduire une dernière notion, celle de base générique. Il faut cependant commencer par montrer le lemme suivant :

Lemme 2.7 :

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 $\text{res}(b) = a$ ont alors le même type.

Démonstration. Quitte à agrandir K , on peut le supposer assez saturé. Soient b et c tels que $\text{res}(b) = a = \text{res}(c)$, 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 le théorème de Holly (voir (2.3)), $X = \bigcup_{i=1}^n (t_i \setminus (\bigcup_{j=1}^{m_i} t_i^j))$, 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 $X = \emptyset$, ce qui est absurde. ■

Définition 2.8 (Base générique) :

Soient K un corps valué algébriquement clos, $A \subseteq K^{\text{eq}}$ et $s \in \mathcal{S}_n(A)$. Si l'on note $\text{res}(s) =$

$s/\mathfrak{M}_K s$, $\text{res}(s)^n$ 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 $q_{\text{res}(s)^n}$, 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 $(\bar{a}_1 \dots \bar{a}_n) \models q_s$ si et seulement si $(\text{res}(\bar{a}_1) \dots \text{res}(\bar{a}_n)) \models q_{\text{res}(s)^n}$, où $\text{res}(\bar{a}_i) = \bar{a}_i + \mathfrak{M}_K s$.

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 $\text{res}(\bar{a}_i)$ est générique au-dessus de $A\bar{a}_1 \dots \bar{a}_{i-1}$ pour tout i et donc, par le lemme (2.7), tous les choix possibles de \bar{a}_i ont le même type au-dessus de ces paramètres. De plus, comme $q_{\text{res}(s)^n}$ 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 la formule $(\forall \bar{x}_1 \dots \bar{x}_n \wedge_i y_i = \text{res}(\bar{x}_i) \Rightarrow \varphi[x_1, \dots, x_n])$ est dans $q_{\text{res}(s)^n}$ (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 2.9 ($\mathcal{L}_{\text{div}}^{\mathcal{G}}$) :

Le langage $\mathcal{L}_{\text{div}}^{\mathcal{G}}$ 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}_{div} . On a aussi, pour tout n un symbole de relation ϵ_n sur $K^n \times \mathcal{S}_n$, un symbole de fonction $\tau_n : \mathcal{T}_n \rightarrow \mathcal{S}_n$ et un symbole de fonction $\nu_n : K^n \times \mathcal{S}_n \rightarrow \mathcal{T}_n$. 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 $\varphi^*[z_1, \dots, z_n, \bar{y}]$, 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 $n \geq 1$, \mathcal{S}_n par $\mathcal{S}_n(K)$, \mathcal{T}_n par $\mathcal{T}_n(K)$ et on pose :

- $\epsilon_n(a, s)$ si et seulement si $a \in s$;
- $\tau_n(t) = s$ si et seulement si $t \in \text{res}(s)$;
- $\nu_n(a, s) = a + \mathfrak{M} s$ si $a \in s$ sinon $\nu_n(a, s) = \mathfrak{M}^n$;
- $\varphi^*(s_1, \dots, s_n, a)$ 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 ϵ_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 φ^* , le problème est un peu plus compliqué. Comme q_s est un type définissable (uniformément en s), il s'en suit que dans ACVF^{eq} , les φ^* sont bien définissables. On note donc $\text{ACVF}_{m,n}^{\mathcal{G}}$ 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 $\text{ACVF}^{\mathcal{G}} \vdash \varphi^*[z_1, \dots, z_n, \bar{y}] \iff \theta[z_1, \dots, z_n, \bar{y}]$. 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 $\text{ACVF}^{\text{eq}} \vdash \forall \bar{x}_1 \bar{x}_2, f(\bar{x}_1) = f(\bar{x}_2) \Rightarrow \psi[\bar{x}_1] \iff \psi[\bar{x}_2]$ et donc

$$\text{ACVF}^{\mathcal{G}} \vdash \varphi^*[\bar{z}] \iff (\forall \bar{x} f(\bar{x}) = \bar{z} \Rightarrow \psi[\bar{x}]) \iff (\exists \bar{x} f(\bar{x}) = \bar{z} \wedge \psi[\bar{x}]). \quad (2)$$

On peut alors montrer que si $(K, v) \leq (L, w)$ 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 ϵ_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 φ^* sont respectés. Cependant, comme $\overline{K}^{\text{alg}} \leq \overline{L}^{\text{alg}}$ (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 $(\overline{K}^{\text{alg}})^{\text{eq}} \leq (\overline{L}^{\text{alg}})^{\text{eq}}$ et comme $\mathcal{L}_{\text{div}}^{\mathcal{G}}$ est une extension définissable dans les corps valués algébriquement clos $(\overline{K}^{\text{alg}})^{\mathcal{G}} \leq (\overline{L}^{\text{alg}})^{\mathcal{G}}$. Comme par définition $\varphi^*[K^{\mathcal{G}}] = \varphi^*[(\overline{K}^{\text{alg}})^{\mathcal{G}}] \cap K^{\mathcal{G}}$, on a

$$\begin{aligned} \varphi^*[L^{\mathcal{G}}] \cap K^{\mathcal{G}} &= (\varphi^*[(\overline{L}^{\text{alg}})^{\mathcal{G}}] \cap L^{\mathcal{G}}) \cap K^{\mathcal{G}} \\ &= \varphi^*[(\overline{L}^{\text{alg}})^{\mathcal{G}}] \cap (\overline{K}^{\text{alg}})^{\mathcal{G}} \cap K^{\mathcal{G}} \\ &= \varphi^*[(\overline{K}^{\text{alg}})^{\mathcal{G}}] \cap K^{\mathcal{G}} \\ &= \varphi^*[K^{\mathcal{G}}] \end{aligned}$$

Il s'en suit que les φ^* sont en fait définissables par les même formules qu'en (2). En effet, soit (K, v) un corps valué quelconque, on a alors, par définition, pour tout $\bar{c} \in K^{\mathcal{G}}$, $K^{\mathcal{G}} \models \varphi^*[\bar{c}]$ si et seulement si $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \varphi^*[\bar{c}]$ et donc $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \forall \bar{x} f(\bar{x}) = \bar{c} \Rightarrow \psi[\bar{x}]$. Comme ψ est sans quantificateurs, on a donc $K^{\mathcal{G}} \models \forall \bar{x} f(\bar{x}) = \bar{c} \Rightarrow \psi[\bar{x}]$. Mais comme $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \text{ACVF}^{\mathcal{G}}$, 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 $K^{\mathcal{G}} \models (\forall \bar{x} f(\bar{x}) = \bar{c} \Rightarrow \psi[\bar{x}]) \iff (\exists \bar{x} f(\bar{x}) = \bar{c} \wedge \psi[\bar{x}])$. Comme cette dernière formule est existentielle, si $K^{\mathcal{G}} \models \exists \bar{x} f(\bar{x}) = \bar{c} \wedge \psi[\bar{x}]$, on a aussi $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \exists \bar{x} f(\bar{x}) = \bar{c} \wedge \psi[\bar{x}]$, d'où $(\overline{K}^{\text{alg}})^{\mathcal{G}} \models \varphi^*[\bar{c}]$ et donc $K^{\mathcal{G}} \models \varphi^*[\bar{c}]$. On a donc bien démontré que tout corps valué vérifie en fait la formule (2) et donc qu'on a bien défini une extension définissables du langage dans tout corps valué.

Remarquons une dernière chose avant d'énoncer le théorème qui a motivé toutes ces définitions. On pourrait penser qu'il manque un prédicat d'appartenance pour les torseurs dans le langage géométrique. Mais il est définissable sans quantificateurs par la formule $\bar{x} \epsilon_n \tau_n(t) \wedge \nu_n(\bar{x}, \tau_n(t)) = t$ où $\bar{x} \in K^n$ et $t \in \mathcal{T}_n$.

Théorème 2.10 :

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

C'est le principal résultat de [HHMo6]. L'élimination des quantificateurs est prouvée au théorème 3.1.2 et celle des imaginaires au théorème 3.4.10.

3 Corps p-adiquement clos

Cette section est particulièrement définitionnelle. On y introduit toutes les notions nécessaires pour étudier les corps p-adiquement clos, en premier lieu la notion même de corps p-adiquement clos et on rappelle tous les résultats utiles sur ces corps qui seront utilisés par la suite.

Définition 3.1 (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 $\text{res}(P(a)) = 0$ et $\text{res}(P'(a)) \neq 0$, il existe $b \in \mathcal{O}$ tel que $P(b) = 0$ et $\text{res}(a) = \text{res}(b)$.

Proposition 3.2 :

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 $v(b - a) = v(P(a)) - v(P'(a))$.

Démonstration.

(iv) \Rightarrow (i) Soient $P \in \mathcal{O}[X]$ et $a \in \mathcal{O}$ tel que $\text{res}(P(a)) = 0$ et $\text{res}(P'(a)) \neq 0$ 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,

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

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, $v(Q'(1) + 1) = v(\sum_{i=2}^n a_i i (-1/P'(a))^i P(a)^{i-1}) \geq v(Q(1)) > 0$ 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 $K \leq L$ 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 3.3 :

Toute extension algébrique d'un corps Hensélien est Hensélienne.

Démonstration. Soit $(K, v) \leq (L, w)$ 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 3.4 (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 $i : K \rightarrow K^h$, 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 $j = \widehat{j} \circ i$

Démonstration. On peut la trouver dans [EP05, 5.2.2, p.121] ■

Définition 3.5 :

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.

Lemme 3.6 :

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 $\gamma + v(\pi)$.

Démonstration. 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 $i \neq j$, $v(x_i - x_j) \leq \gamma$, sinon ils seraient dans la même boule de rayon $\gamma + v(\pi)$. Mais d'un autre côté on a $v(x_i - x_j) = v(x_i - a - (x_j - a)) \geq \gamma$ 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 $i \neq j$, $\text{res}(\hat{x}_i - \hat{x}_j) \neq 0$, i.e. $\text{res}(\hat{x}_i) \neq \text{res}(\hat{x}_j)$. 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. ■

Rappelons ensuite des résultats classiques :

Proposition 3.7 :

Soit $(\mathbb{Q}_p, v_p) \leq (K, v)$ une extension finie de corps valués de degré d'inertie f et de degré de ramification e . Il existe alors α algébrique sur \mathbb{Q} , $K = \mathbb{Q}_p[\alpha]$ et $\mathcal{O}_K = \mathbb{Z}_p[\alpha]$. De plus, soit $Q_f \in \mathbb{Q}[x]$ unitaire de degré f tel que k_K soit un corps de rupture du réduct de Q_f dans $\mathbb{F}_p[X]$. On peut supposer que $Q_f(\alpha)$ est une uniformisante de K .

De plus si $(K, v) \leq (L, w)$ est une extension finie de corps valués, alors il existe β donc le polynôme minimal sur K est dans $\mathbb{Q}[\alpha][X]$ tel que $L = K[\beta]$ et $\mathcal{O}_L = \mathcal{O}_K[\beta]$.

Démonstration. Le résultat énoncé comme cela n'est probablement pas un résultat classique, mais il découle immédiatement du lemme de Krasner. En effet, comme K est Hensélien, on peut remonter un générateur de l'extension de corps résiduel $\bar{\beta}$ (i.e. une solution du réduct de Q_f) en $\beta \in K$ et par le lemme de Krasner, comme \mathbb{Z} est dense dans \mathbb{Z}_p , on peut le supposer entier sur \mathbb{Z} . Si $Q_f(\beta)$ est une uniformisante, il suffit de prendre $\alpha = \beta$. Sinon, soit β' une uniformisante de K (que l'on peut aussi supposer entière sur \mathbb{Z} par le lemme de Krasner), alors une expansion de Taylor nous donne que $\alpha = \beta + \beta'$ convient.

Le cas d'une extension de K se fait avec la même preuve car K n'est autre que le complété de $\mathbb{Q}[\alpha]$. ■

Proposition 3.8 :

Soit $(\mathbb{Q}_p, v_p) \leq (K, v)$ une extension finie de corps valués et $d \in \mathbb{N}$, alors K a un nombre fini d'extensions de degré d .

Démonstration. Ce résultat est une conséquence immédiate du cas où $K = \mathbb{Q}_p$. En effet, le nombre d'extensions de degré d de K est inférieur au nombre d'extension de degré $[K : \mathbb{Q}_p]d$ de \mathbb{Q}_p . ■

Définition 3.9 :

On définit $\mathcal{L}_{pCF} = \mathcal{L}_{\text{div}} \cup \{P_n : n \in \mathbb{N}^*\} \cup \{\alpha\}$. Soient e et $f \in \mathbb{N}$, $P \in \mathbb{Q}[X]$ irréductible de degré ef et Q_f tel que dans la proposition (3.7). La théorie $pCF_{P,f}$ dans le langage \mathcal{L}_{pCF} est donnée par les axiomes suivants :

- (i) K est un corps valué Hensélien.
- (ii) P_n définit l'ensemble des puissances n -ièmes.
- (iii) Le groupe de valuation est un \mathbb{Z} -groupe dont le plus petit élément strictement positif est $v(Q_f(\alpha))$.
- (iv) Le corps résiduel est \mathbb{F}_{p^f} .
- (v) $P(\alpha) = 0$.
- (vi) $v(p) = ev(Q_f(\alpha))$.

Remarque 3.10 :

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}_{pCF} .

- (i) Le seul problème est d'exprimer qu'il est Hensélien, mais il suffit d'énoncer que le corps vérifie le lemme de Hensel par un schéma d'axiomes indicé par n : pour tout $a_1 \dots a_n$ et a , si $1 \text{ div } a_i$, $1 \text{ div } a$, $\neg(\sum_i a_i a^i \text{ div } 1)$ et $\sum_i a_i i a^{i-1} \text{ div } 1$, alors il existe b tel que $1 \text{ div } b$, $\sum_i a_i b^i = 0$ et $\neg(a - b \text{ div } 1)$.
- (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 que $v(Q_f(\alpha))$ est son plus petit élément strictement positif: $\neg(Q_f(\alpha) \text{ div } 1)$; et pour tout x , $x \text{ div } Q_f(\alpha)$ implique $x \text{ div } 1$; et que pour tout $n \in \mathbb{N}^*$, $[\Gamma : n\Gamma] = n$: pour tout x , il existe y tel que $\bigvee_{i=0 \dots n-1} x \text{ div } (Q_f(\alpha))^i y^k \wedge (Q_f(\alpha))^i y^k \text{ div } x$.
- (iv) Les axiomes précédents impliquent que le corps résiduel contient au moins p^f éléments. En effet, soit \bar{P} le polynôme minimal annulateur de \bar{a} sur \mathbb{F}_p . Comme $\bar{Q}_f(\bar{a}) = 0$, $\bar{P} | \bar{Q}_f$ qui est irréductible, donc $P = Q_f$ et $[k_K : \mathbb{F}_p] \geq f$. Il suffit de dire que le corps résiduel a au plus p^f éléments : $\forall x_0 \dots x_{p^f} \bigvee_{i \neq j} \neg(x_i - x_j \text{ div } 1)$.
- (v) $P(\alpha) = 0$.
- (vi) $p \text{ div } (Q_f(\alpha))^e$ et $(Q_f(\alpha))^e \text{ div } p$.

Proposition 3.11 :

Soit $(\mathbb{Q}_p, v_p) \leq (K, v)$ une extension finie de corps valués de degré d'inertie f . Soit $P \in \mathbb{Q}[X]$ le polynôme minimal annulateur de α tel que dans la proposition (3.7). Alors $K \models p\text{CF}_{P,f}$. De plus cette théorie admet l'élimination des quantificateurs dans $\mathcal{L}_{p\text{CF}}$ et est complète. On a donc $\text{Th}(K) = p\text{CF}_{P,f}$.

Démonstration. La seule chose à vérifier pour montrer que $K \models p\text{CF}_{P,f}$ est que K est Hensélien mais c'est une conséquence immédiate du fait qu'il est complet en tant qu'extension finie d'un corps complet. L'élimination des quantificateurs et la complétude de la théorie sont montrés dans [PR84, Corollary 5.3]. Le langage utilisé dans ce livre contient ef constantes qui sont un système de représentants de $\mathcal{O}_K/p\mathcal{O}_K$, mais les axiomes qu'on a choisi impliquent que les $(\alpha^i(Q_f(\alpha))^j)$ forment un tel système de représentants. ■

On peut aussi démontrer un résultat d'élimination des quantificateurs dans une extension du langage tri-sorté qui permet de montrer que Γ est stablement plongé et est un pur \mathbb{Z} -groupe.

On définit aussi le langage $\mathcal{L}_{p\text{CF}}^{\mathcal{G}}$ en rajoutant les prédicats P_n au langage $\mathcal{L}_{\text{div}}^{\mathcal{G}}$ et en les interprétant toujours par l'ensemble des puissances n -ièmes. La théorie $p\text{CF}_{P,f}^{\mathcal{G}}$ est alors l'extension définissables de $p\text{CF}_{P,f}^{\text{eq}}$ donnée par les considérations qui suivent la définition (2.9). Il suit aussi de ces considérations que la restriction à $\mathcal{L}_{\text{div}}^{\mathcal{G}}$ de tout modèle de $p\text{CF}_{P,f}^{\mathcal{G}}$ se plonge dans un modèle de $\text{ACVF}_{0,p}^{\mathcal{G}}$.

Dans ce qui suit, on notera K un modèle de $p\text{CF}_{P,f}$ et $\pi = Q_f(\alpha) \in \mathbb{Q}[\alpha]$ une uniformisante de K , où, comme par la suite on confond α avec son interprétation.

Lemme 3.12 :

Soient $x \in K$ et $k \in \mathbb{N}^*$ alors $x \in (K^*)^k$ si et seulement si

$$(K^*)^k \cap B_{\geq(v(\pi)+v(x)+2v(k))}(x) \neq \emptyset.$$

Démonstration. Soient $y \in (K^*)^k \cap B_{\geq(v(\pi)+v(x)+2v(k))}(x)$ et $P(X) = X^k - x/y$. Comme $v(P(1)) = v(1 - y/x) = v(x - y) - v(x) \geq v(\pi) + 2v(k)$ et $v(P'(1)) = v(k)$, on a bien $v(P(1)) > 2v(P'(1))$ et donc par le lemme de Hensel-Rychlik (voir (3.2.iv)) il existe $b \in \mathcal{O}_K$ tel que $P(b) = 0$, i.e. $b^k = y/x$. Comme $y \in (K^*)^k$, il s'en suit directement que x aussi. La réciproque est évidente. ■

Remarque 3.13 :

Soit $k \in \mathbb{N}^*$. Il existe un système de représentants de $\mathcal{O}_K/\pi^k\mathcal{O}_K$ dans $\mathbb{Q}[\alpha] \subseteq \text{dcl}(\emptyset)$. En effet, $\mathbb{Q}[\alpha]$ est une extension de \mathbb{Q} de degré d'inertie f . Soit alors \mathcal{R}_k un système de représentants de $\mathcal{O}_{\mathbb{Q}[\alpha]}/\pi^k\mathcal{O}_{\mathbb{Q}[\alpha]}$. Comme ces deux quotients sont tous deux de taille p^{fk} (cela se démontre par exemple par récurrence sur k), il est facile de voir que c'est aussi un système de représentants de $\mathcal{O}_K/\pi^k\mathcal{O}_K$.

Dorénavant, on notera \mathcal{R}_k un tel système de représentants.

Lemme 3.14 :

Soient $x \in K$ tel que $v(x) = 0$ et $k \in \mathbb{N}^*$. Il existe alors $n \in \mathcal{R}_{1+2ev(k)}$ tel que $v(n) = 0$ (en particulier $n \neq 0$) et $x/n \in (K^*)^k$.

Démonstration. Soit \bar{x} le réduct de x modulo $\pi^{1+2ev(k)} \mathcal{O}_K$. Il existe $n \in \mathcal{R}_{1+2ev(k)}$ tel que $\bar{x} = \bar{n}$, i.e. $x \in n + \pi^{1+2ev(k)} \mathcal{O}_K$. Si $v(n) \neq 0$ alors, comme $v(x) \geq \min(v(n), 1 + 2ev(k))$, cela contredirait le fait que $v(x) = 0$. On a donc $v(x/n - 1) = v(x - n) - v(n) = v(x - n) \geq (1 + 2ev(k)) \cdot v(\pi) = v(\pi) + (2v(k)) \cdot v(p) = v(\pi) + 2v(k)$ et donc par le lemme (3.12), comme 1 est une puissance k -ième, x/n aussi. ■

Remarque 3.15 :

Remarquons une petite subtilité qui pourrait rendre la preuve de ce lemme confuse. L'action que je note \cdot est la structure canonique de \mathbb{Z} -module d'un groupe abélien, i.e. $k \cdot x := x + \dots + x$ k -fois. Mais contrairement à d'habitude, pour tout $k \in \mathbb{Z}$, $v(k) \in \mathbb{Z}$ n'est pas une notation (abusive) pour $v(k) \cdot v(\pi)$ (ce qui est tentant si on veut identifier le groupe engendré par $v(\pi)$ avec \mathbb{Z}), mais c'est l'image de $v(k) \in v(\mathbb{Q})$ dans Γ_K et donc $v(k) = v(k) \cdot v(p) = (ev(k)) \cdot v(\pi)$.

Corollaire 3.16 :

Soit $k \in \mathbb{N}^$. L'ensemble $\{m\pi^n : m \in \mathcal{R}_{1+2ev(k)} \text{ et } n \in \llbracket 0 \dots k-1 \rrbracket\}$ contient un système de représentants de $K^*/(K^*)^k$, composé d'éléments de $\mathbb{Q}[\alpha] \subseteq \text{dcl}(\emptyset)$. En particulier, $K^*/(K^*)^k$ est fini.*

Démonstration. Soit $x \in K$, comme Γ_K est un \mathbb{Z} -groupe de plus petit élément strictement positif $v(\pi)$, il existe $n \in \llbracket 0 \dots k-1 \rrbracket$ et $y \in K$ tel que $v(x) = kv(y) + nv(\pi)$. D'après le lemme (3.14), il existe $m \in \mathcal{R}_{1+2ev(k)}$ tel que $v(m) = 0$ et que $\frac{x}{y^k \pi^n m}$ est une puissance k -ième. Il s'en suit donc que x est dans la même classe d'équivalence modulo $(K^*)^k$ que $m\pi^n$. ■

Corollaire 3.17 :

Soit $A \subseteq K$ une sous-structure. Pour que A soit un modèle de $pCF_{P,f}$, il faut et il suffit que A soit Hensélien et $A \models \forall x P_n x \Rightarrow \exists y x = y^n$.

Démonstration. D'après la remarque (3.10), A vérifie bien tous les axiomes de $pCF_{P,f}$ sauf la définition de P_n et celui qui dit que pour tout n , $[\Gamma_A : n\Gamma_A] = n$ (en effet tout le reste est composé d'axiomes universels). 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 $A \models P_n x$.

De plus, soient $x \in A$ et $n \in \mathbb{N}^*$. Par le lemme (3.16), il existe $m \in \text{dcl}(\emptyset) \subseteq A$ et $k \in \llbracket 0 \dots k-1 \rrbracket$ tels que $v(m) = kv(\pi)$ et $x/m \in P_n(K)$. Comme la définition de P_n est aussi vérifiée dans A , il existe $y \in A$ tel que $xm^{-1} = y^n$ et donc que $v(x) \in kv(\pi) + n\Gamma_A$. ■

Lemme 3.18 :

Soit $(\mathbb{Q}_p, v_p) \leq (K, v)$ une extension finie de corps valués. On a alors $\bigcap_{k \geq 1} (K^)^k = \{1\}$.*

Démonstration. Soit $x \in \bigcap_{k \geq 1} (K^*)^k$, quitte à le remplacer par x^{-1} , on peut supposer que $x \in \mathcal{O}_K$ et on a alors $x \in \bigcap_{k \geq 1} (\mathcal{O}_K)^k$. Notons f le degré d'inertie de K et π une uniformisante de K . Par hypothèse, Pour tout k il existe donc y tel que $y^{p^{fk-1}} = x$. Mais comme $\mathcal{O}_K / \pi^k \mathcal{O}_K$ est un anneau fini de cardinal p^{fk} , $x = y^{p^{fk-1}} \equiv 1 \pmod{\pi^k \mathcal{O}_K}$. Il s'en suit donc que pour tout $k \in \mathbb{N}$, il existe z tel que $x = 1 + \pi^k z$. Comme K est un corps complet, tout $x \in K$ a un unique

développement de la forme $\sum_i a_i \pi^k$ où les a_i sont pris dans un système de représentants de k_K (que l'on peut supposer contenir 1). Il s'en suit donc que $x = 1$. ■

Pour finir, montrons que ce qu'on a montré pour les extensions des extensions finies de \mathbb{Q}_p est aussi vrai pour toute extension d'un modèle de $p\text{CF}_{P,f}$.

Théorème 3.19 :

Soit $K \models p\text{CF}_{P,f}$, alors K a un nombre fini d'extensions d'un degré donné et elles sont toutes engendrées par un élément dont le polynôme minimal annulateur au dessus de K est dans $\mathbb{Q}[\alpha]$ et qui engendre aussi l'anneau de valuation.

Démonstration. On a montré aux propositions (3.8) et (3.7) que ces propriétés sont vraies pour $\mathbb{Q}_p[\alpha]$, 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 $\mathbb{Q}[\alpha]$ tels que leurs corps de rupture sont les extensions de degré n de $\mathbb{Q}_p[\alpha]$ 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 . ■

4 Cloture algébrique et définissable dans $p\text{CF}_{P,f}$

Cette section se propose de démontrer quelles sont les clôtures algébriques et définissables dans $K \models p\text{CF}_{P,f}$.

Proposition 4.1 :

Soit $A \subseteq K$, on a alors $\overline{A}^{\text{alg}} \cap K \models p\text{CF}_{P,f}$.

Démonstration. D'après le corollaire (3.17), il suffit de montrer que $K' = \overline{A}^{\text{alg}} \cap K$ 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 $\text{res}(P(a)) = 0$ et $\text{res}(P'(a)) \neq 0$. Ces mêmes conditions sont vérifiées dans K qui est hensélien, il existe donc $b \in \mathcal{O}_K$ tel que $P(b) = 0$ et $\text{res}(b) = \text{res}(a)$. 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, si on a $K' \models P_n(x)$, c'est aussi vrai dans K car K' est muni de la structure induite. Il existe donc $y \in K$ tel que $y^n = x$, mais ce y est algébrique sur K' et donc appartient à K' . ■

Corollaire 4.2 :

Soit $A \subseteq K$, on a alors $\text{acl}(A) = \overline{A}^{\text{alg}} \cap K$.

Démonstration. On a montré au lemme (4.1) que $\overline{A}^{\text{alg}} \cap K$ est une sous-structure de K qui est un modèle de $p\text{CF}_{P,f}$. Comme $p\text{CF}_{P,f}$ est modèle complète, $\overline{A}^{\text{alg}} \cap K$ est une sous-structure

élémentaire qui contient A et donc $\text{acl}(A)$. Mais comme $\mathcal{L}_{p\text{CF}}$ contient le langage des anneaux, on a aussi $\overline{A}^{\text{alg}} \cap K \subseteq \text{acl}(A)$. Ils sont donc égaux. ■

Lemme 4.3 :

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

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

Corollaire 4.4 :

Soit $A \subseteq K \models p\text{CF}_{P,f}$ alors $\overline{A}^{\text{alg}} \cap K$ est un modèle premier et minimal au dessus de A .

Démonstration. C'est une conséquence immédiate du lemme (4.3), du corollaire (4.2) et de la proposition (4.1). ■

Proposition 4.5 :

Soit $A \subseteq K$ alors $K' = \overline{A}^{\text{alg}} \cap K$ est rigide au dessus de A .

Démonstration. Soit $\sigma \in \text{Aut}(K'/A)$ et soit B la sous-structure fixée par σ . Il suffit de montrer que $B \models p\text{CF}_{P,f}$. En effet, par modèle-complétude, on a alors immédiatement $K' = \text{acl}(A) \subseteq B$.

D'après le corollaire (3.17), 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 $C^h = \text{Frac}(\langle A \rangle)^h$ et comme $C = \text{Frac}(\langle A \rangle) \subseteq \text{dcl}(A)$, il est fixé par σ . Notons $i_1 : C \rightarrow C^h$ et $i_2 : C^h \rightarrow K'$ les injections, alors comme σ fixe C , on a $\sigma \circ i_2 \circ i_1 = i_2 \circ i_1$ et donc $\sigma \circ i_2$ et $\sigma \circ i_1$ font toutes deux commuter le diagramme suivant :

$$\begin{array}{ccc} & C^h & \\ i_1 \nearrow & & \searrow \\ C & \xrightarrow{\sigma \circ i_1 \circ i_2} & K' \end{array}$$

Par la propriété universelle de l'Hensélianisé (voir (3.4)) on a $\sigma \circ i_2 = i_2$ et donc pour tout $x \in C^h$, $\sigma(x) = x$, i.e. $C^h \leq B$. Mais cette extension est algébrique donc par le corollaire (3.3), 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 . Pour tout $k \in \mathbb{N}^*$, par le corollaire (3.16), il existe $q \in \mathbb{Q}[\alpha]^*$ 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 $x/x = 1$. Il s'en suit que $\sigma(y)/y \in \text{dcl}(\emptyset) \subseteq \mathbb{Q}_p[\alpha]$. Par le lemme (3.18), on a alors $\sigma(y)/y = 1$ et donc $y \in B$, i.e. $B \models \exists y x = y^n$. ■

Corollaire 4.6 :

Soit $A \subseteq K$ alors $\text{dcl}(A) = \text{acl}(A) = \overline{A}^{\text{alg}} \cap K$.

Démonstration. Quitte à en prendre une extension élémentaire, on peut supposer que K est assez saturé et homogène. Il suffit alors de montrer que tout $\sigma \in \text{Aut}(K/A)$ fixe $\overline{A}^{\text{alg}} \cap K$. Mais comme σ fixe A alors σ fixe (globalement) $\text{acl}(A) = \overline{A}^{\text{alg}} \cap K$. Mais on a montré dans le lemme (4.5) que $\overline{A}^{\text{alg}} \cap K$ 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 $pCF_{P,f}$ admet des fonctions de Skolem définissables. Pour cela on fait appel au critère suivant.

Lemme 4.7 (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 $\mathcal{M} \models T_{\forall}$ se plonge dans un modèle $\overline{\mathcal{M}} \models T$ qui est algébrique et rigide au dessus de M .

Démonstration. Voir [Dri84, Théorème 2.1] ■

Corollaire 4.8 :

La théorie $pCF_{P,f}$ admet des fonctions de Skolem définissables.

Démonstration. Soient $(K, v) \models pCF_{P,f}$ et $A \subseteq K$. D'après le lemme (4.1), $\overline{A}^{\text{alg}} \cap K$ est un modèle de $pCF_{P,f}$, algébrique au dessus de A . Mais par le lemme (4.5), il est rigide au dessus de A . On peut donc conclure par le lemme (4.7). ■

Remarque 4.9 :

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 $\mathcal{L}_{pCF_{P,f}}^{\text{eq}}$. 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.

5 Les Types unaires dans $pCF_{P,f}$

La section qui suit est une reprise des résultats de la section 4 de [HMo8], dans le cas particulier de la théorie $pCF_{P,f}$. Rappelons, que pour tout corps valué K , on note \mathbb{B}_K l'ensemble des boules de K (ouvertes ou fermées, avec un centre et un rayon dans K). Si $A \subseteq M$ où M est une structure qui contient une sorte de corps valué (notée K), on note $\mathbb{B}_{K(M)}(A)$ l'ensemble des boules A -définissables de $K(M)$. Si $b \in \mathbb{B}_{K(M)}(A)$, on note $x \in b$ pour $\varphi[x]$, où φ est une \mathcal{L}_A -formule qui définit b .

Définition 5.1 (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 algébrique sur A de P .

On note $\alpha_P|A$ le A -type partiel des points génériques de P sur A :

$$\alpha_P := \{x \in b_i : i \in I\} \cup \{-x \in b : b \in \mathbb{B}_K(\text{acl}(A)) \text{ et } b \not\subseteq P\}.$$

Remarque 5.2 :

On dira que P est une intersection stricte si ce n'est pas lui même une boule (qui serait alors immédiatement A -définissable). Dans le cas où P est une intersection stricte, il suffit de demander que x n'appartienne pas aux sous-boules A -définissables de P . En effet, si b est une boule algébrique sur A contenue dans A alors la plus petite boule qui contient tous les conjugués (en nombre fini) de b au dessus de A est incluse dans P et l'est nécessairement strictement vu que P est une intersection stricte.

Comme on l'a déjà fait remarquer précédemment, la notion de boule se comporte mal vis à vis des extensions de corps. Mais pour les corps p -adiquement clos et de sa clôture algébrique, cela cas ne peut pas se produire :

Lemme 5.3 :

Soient $(K, v) \models p\text{CF}_{P,f}$, $\gamma \in \Gamma_{\overline{K}^{\text{alg}}}$ et $a \in K$. Si $B_{\geq \gamma}(a)$ et $B_{> \gamma}(a)$ sont définissables sur K (dans $\overline{K}^{\text{alg}}$), alors leurs traces sur K sont des boules de K .

Démonstration. Considérons d'abord $b = B_{\geq \gamma}(a)$. Comme γ est dans $\Gamma_{\overline{K}^{\text{alg}}} = \text{div } \Gamma_K$, il existe $n \in \mathbb{N}$ 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 $k \in \llbracket 0 \dots n-1 \rrbracket$ 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 $\delta - v(p)\gamma \leq \delta$ et $b \cap M$ est donc la boule de centre de a est de rayon δ dans M .

De plus $B_{> \gamma}(a) \cap M = B_{\geq \gamma + v(p)}(a) \cap M$ qui est bien une boule de M par ce qu'on vient de démontrer. ■

On peut d'ailleurs remarquer qu'on a montré un résultat plus fort que celui énoncé, car b et sa trace sont inter-définissables sans quantificateurs dans \mathcal{L}_{div} .

D'après [HHMo6], le type générique d'une boule ou d'une intersection stricte de boules est complet dans ACVF. De plus, sur un ensemble algébriquement clos, tous les types d'éléments du corps sont d'une de ces deux formes. Dans le cas de $p\text{CF}_{P,f}$, la situation est un peu plus compliquée.

Lemme 5.4 :

Soient $\mathcal{M} \models p\text{CF}_{P,f}^{\text{eq}}$, $A \subseteq M$ tel que $\text{acl}^{\text{eq}}(A) \cap \mathbb{B}_{K(M)} \subseteq \text{dcl}^{\text{eq}}(A)$ et $x \in K(M)$ alors x est générique dans une intersection stricte de boules A -définissables au-dessus de A .

Démonstration. Soit $P = \bigcap \{b \in \mathbb{B}_{K(M)}(A) : x \in b\}$, 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 (3.6), la boule de centre x et de rayon $\gamma + 1$ est algébrique sur A . Elle est donc dans $\text{acl}^{\text{eq}}(A) \cap \mathbb{B}_{K(M)} \subseteq \text{dcl}^{\text{eq}}(A)$ et est donc dans $\mathbb{B}_{K(M)}(A)$. De plus elle contient x et est strictement contenue dans P , ce qui est absurde. ■

Définition 5.5 (f_{*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

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

Définition 5.6 (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 $q \mapsto f_*q$ est injective de $\{q \in \mathcal{S}(A) : p \subseteq q\}$ dans $\mathcal{S}(A)$.

En particulier, pour vérifier qu'un type est complet au dessus de A relativement à f , il suffit 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 5.7 :

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 $f_i(\bar{x})$.

Démonstration. 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 $\sigma : \llbracket 1 \dots n \rrbracket \rightarrow \{0, 1\}$, 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 $X := \{\sigma : \exists \bar{c} \in N \bar{c} \models p \text{ et } \mathcal{N} \models \varphi[\bar{c}] \wedge \theta_\sigma[f(\bar{c})]\}$ 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 , $\theta_i[f(\bar{c})] \iff \theta_i[f(\bar{c}')] \iff \theta_i[\bar{c}] \iff \theta_i[\bar{c}']$ et donc, comme $\mathcal{N} \models \varphi[\bar{c}']$, on a aussi $\mathcal{N} \models \varphi[\bar{c}]$. 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 $\mathcal{N} \models \varphi[\bar{c}] \iff \theta[f(\bar{c})] \iff \theta[f(\bar{c}')] \iff \varphi[\bar{c}']$ 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 lemme (3.16) que pour tout corps p -adiquement clos K , le groupe $K^*/(K^*)^n$ est fini et a un système de représentants dans $\text{dcl}(\emptyset)$. Soit alors (q_i^n) un tel système de représentants. La surjection canonique $K^* \rightarrow K^*/(K^*)^n$ 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 (3.12) implique que pour tout n , $B_{\geq v(\pi)+2v(n)}(1) \subseteq \ker(r_n)$. Il s'en suit donc que si $v(x-y) + v(\pi) +$

$2v(n) \leq v(x-z)$ alors $r_n(y-x) = r_n(y-z)$. En effet $\frac{y-z}{y-x} - 1 = \frac{z-x}{y-x}$ et $v(x-z) - v(x-y) \geq v(\pi) + 2v(n)$ 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 $n \in \mathbb{N}$, $x + nv(\pi) \leq y$. Comme on vient de le remarquer, on a alors que $v(x-y) \ll v(x-z)$ 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 $y \in b$, $v(x-y)$ est constant (c'est une conséquence immédiate du caractère ultramétrique de v), la notation $v(x-b)$ a donc un sens. De même, si $v(x-b) \ll \rho(b)$ (où $\rho(b)$ est le rayon de la boule) alors on vient de montrer que la notation $r_n(x-b)$ à un sens. En particulier, soient $x \models \alpha_P|A$ et $b \in \mathbb{B}_K(A)$ telle que $b \subseteq P$, alors comme les boules de rayon $\rho(b) - lv(\pi)$ autour de b sont toutes dans $\mathbb{B}_K(A)$, elles ne contiennent pas x et donc $v(x-b)$ et $r_n(x-b)$ sont bien définis. Cela dit, pour que $v(x-b)$ soit défini, il suffit d'avoir $v(x-b) + v(\pi) + 2v(n) \leq \rho(b)$, 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 $\mathcal{M} \models p\text{CF}_{P,f}^{\text{eq}}$, v est \emptyset -définissable (c'est même un symbole de \mathcal{L}^{eq}). En effet, le groupe de valeur n'est autre que $K^*/(\mathcal{O} \setminus \mathfrak{M})$ qui est bien un quotient définissable, et v est la projection canonique.

Lemme 5.8 :

Soient $\mathcal{M} \models p\text{CF}_{P,f}^{\text{eq}}$, $A \subseteq K(M)$, $P = \bigcap_{i \in I} b_i$ une intersection stricte de boules A -définissables et $b \in \mathbb{B}_{K(M)}(A)$ telle que $b \subseteq P$, alors le type $(\alpha_P|A)[x]$ est complet relativement à $v(x-b)$ et $r(x-b)$.

De plus si un tel b n'existe pas, alors $\alpha_P|A[x]$ est complet.

Démonstration. Quitte à clore A par dcl, on peut supposer que A est un corps.

Notons $K = K(M)$. Soit $L = \overline{K}^{\text{alg}}$ muni d'une valuation qui étend celle de K (que l'on notera aussi v). Dans un premier temps nous allons montrer que l'on peut étendre les r_n à L^* . Soit $H = (K^*)^n \cdot (1 + \pi^{1+2ev(n)} \mathcal{O}_L)$ un sous-groupe de L^* . Soit $xy \in H \cap K^*$ avec $x \in (K^*)^n$ et $y \in (1 + \pi^{1+2ev(n)} \mathcal{O}_L)$. On a alors $y \in K^*$, et comme $(1 + \pi^{1+2ev(n)} \mathcal{O}_L) \cap K^* = (1 + \pi^{1+2ev(n)} \mathcal{O}_K) \subseteq (K^*)^n$, on a $xy \in (K^*)^n$. On a donc montré que $H \cap K^* = (K^*)^n$ et donc $K^*/(K^*)^n$ s'identifie avec un sous groupe de L^*/H . 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 $v(x-y) \ll v(x-z)$ 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 $v(c-a) \equiv_A v(c'-a)$ et pour tout n , $r_n(c-a) \equiv_A r_n(c'-a)$, i.e. il existe $\sigma \in \text{Aut}(M/A)$ tel que $v(c-a) = \sigma(v(c'-a)) = v(\sigma(c')-a)$ (quitte à supposer \mathcal{M} assez homogène) et $r_n(c-a) = r_n(\sigma(c')-a)$. Comme $\sigma(c') \equiv_A c'$, il suffit de démontrer que $\sigma(c') \equiv_A c$. On peut donc supposer $v(c-a) = v(c'-a)$ et, pour tout n , $r_n(c-a) = r_n(c'-a)$.

Considérons maintenant $d \in \overline{A}^{\text{alg}}$. 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 $\rho(b_j) \geq \rho(b_i) + mv(\pi)$ sinon $X = \{\rho(b_j) : j \in I\}$ aurait un maximum, (parmi $\rho(b_i), \rho(b_i) + v(\pi), \dots, \rho(b_i) + mv(\pi)$) 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 et $c \in b_j$, $v(c-a) \geq \rho(b_j) \geq \rho(b_i) + mv(\pi) > v(d-a) + mv(\pi)$. 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 $d \in P$, soit b' la plus petite boule de L qui contient b et tous les conjugués de d au dessus de A . D'après le lemme (5.3), $b'' = b' \cap K$ est une boule et la boule de rayon $v(\pi)$ de moins autour de b'' contient b' . De plus la boule de rayon $(l+1)v(\pi) > 0$ de moins autour de b'' est A -invariante et donc A -définissable, de plus elle est incluse dans P (par le même raisonnement que précédemment mais en utilisant maintenant que $d \in P$), donc c ne peut y appartenir, i.e. $v(c-a) < \rho(b'') - (l+1)v(\pi) \leq v(d-a) - lv(\pi)$ 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 \bar{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 , $r_n(Q(c)) = r_n(Q(c'))$ et donc $P_n(Q(c)) \iff P_n(Q(c'))$. Or comme $A \subseteq K(M)$ et que toute $\mathcal{L}_{pCF_{P,F}}^{\text{eq}}$ -formule à paramètres et variables dans le corps est équivalente à une \mathcal{L}_{pCF} -formule (c'est une propriété de T^{eq} pour toute théorie T), le type de c sur A est entièrement déterminé par son type dans la \mathcal{L}_{pCF} -structure. Comme il y a élimination des quantificateurs et qu'on vient de démontrer que c et c' réalisent les mêmes atomes, on a bien $c \equiv_A c'$. On a donc bien démontré la première partie du lemme.

De plus, on peut remarquer que le seul cas où l'on utilise l'hypothèse sur $v(c-a)$ et les $r_n(c-a)$ est dans le cas où $d \in P$. Pour montrer la seconde partie du lemme, il suffit donc de montrer qu'il n'y a pas de $d \in \bar{A}^{\text{alg}}$ qui soit dans P . Supposons cependant qu'il y en ait un, et soient $(d_j)_{j=1\dots n}$ l'ensemble de ses conjugués sur A . Alors $1/n \sum_j d_j$ est dans P . En effet, soit e un point de P , alors $v(1/n \sum d_j - e) = -v(n) + v(\sum(d_j - e)) \geq \rho(b_i) - v(n)$ pour tout $i \in I$. Comme P est une intersection stricte, il existe i' tel que $\rho(b_{i'}) \geq \rho(b_i) + v(n)$ et donc $v(1/n \sum d_j - e) \geq \rho(b_{i'}) - v(n) \geq \rho(b_i)$. Mais $1/n \sum_j d_j$ est dans A , ce qui contredit le fait P ne contient aucune boule, et donc aucun point, A -définissable. ■

La proposition qui suit est une forme de réciproque au lemme (5.8). On y avait démontré que pour rendre complet un α_P , il faut spécifier le type de $(v(x-a), r(x-a))$ pour une certaine boule 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 5.9 (P_Γ) :

Si $P = \bigcap_{i \in I} b_i$ est une intersection de boules, on notera $P_\Gamma = \{\gamma \in \Gamma : \forall i \in I, \gamma \geq \rho(b_i)\}$. On notera aussi P_Γ l'ensemble de formules qui définit ce type partiel.

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

Proposition 5.10 :

Soient $\mathcal{M} \models pCF_{P,F}^{\text{eq}}$, $A \subseteq M$, $P = \bigcap_{i \in I} b_i$ 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.

Démonstration. 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 $\psi[y, \bar{z}] \Rightarrow y \geq \gamma$.

Comme \bar{z} n'apparaît pas à droite de l'implication, quitte à remplacer ψ par $\exists \bar{z} \psi[y, \bar{z}]$, on peut supposer que sa seule variable est y . Comme $\psi[M]$ a un minorant, elle admet une borne inférieure γ' (cette propriété est vraie dans \mathbb{Z} et s'exprime au premier ordre). Comme $\psi \in q$, ψ est consistant avec P_Γ et donc γ' est dans $P_\Gamma(A)$ et $q[y] \Rightarrow y \geq \gamma'$, ce qui est absurde.

Soit alors $(\gamma, s) \models q[y, \bar{z}] \cup \{y < \gamma : \gamma \in P_\Gamma(M)\}$ (dans une extension élémentaire de 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 morceau fini de cette formule est dans q). Par compacité, existe donc c tel que $(v(c), r(c)) \models q[y, z] \cup \{y < \gamma : \gamma \in P_\Gamma(M)\}$. 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 $v(c) = v(d - a) \geq \rho(b)$, ce qui contredit la définition de c . On a donc bien $d \models \alpha_P|_M$. 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 $c \models q[v(c), r(c)]$, on a bien $(v(d - a'), r(d - a')) \models q$. ■

La proposition qui suit a pour but d'étendre le lemme (5.8) à n'importe quel ensemble de paramètres imaginaires.

Proposition 5.II :

Soient $\mathcal{M} \models pCF_{P,F}^{\text{eq}}$, $A \subseteq M$, $P = \bigcap_{i \in I} b_i$ une intersection stricte de boules A -définissables et $b \in \mathbb{B}_{K(M)}(A)$ telle que $b \subseteq P$, alors le type $(\alpha_P|_A)[x]$ est complet relativement à $v(x - b)$ et $r(x - b)$.

De plus si un tel b n'existe pas, alors $\alpha_P|_A[x]$ est complet.

Démonstration. La réduction au lemme (5.8) se fait de deux façon très différentes suivant si P contient des boules de $\mathbb{B}_{K(M)}(A)$ ou pas. Il est donc naturel de la couper en deux.

Lemme 5.I2 :

Supposons qu'il existe $b \in \mathbb{B}_{K(M)}(A)$ telle que $b \subseteq P$, alors le type $(\alpha_P|_A)[x]$ est complet relativement à $v(x - b)$ et $r(x - b)$.

Démonstration. Soient c_1 et $c_2 \models \alpha_P|_A$ tels que $(v(c_1 - b), r(c_1 - b)) \equiv_A (v(c_2 - b), r(c_2 - b))$.

Supposons tout d'abord que $c_1 \models \alpha_P|_{M_0}$ où $A \subseteq M_0 < M$. Alors, quitte à prendre un conjugué de c_2 au dessus de A , on peut supposer que $(v(c_1 - b), r(c_1 - b)) = (v(c_2 - b), r(c_2 - b))$. Mais c_2 est alors aussi une réalisation de $\alpha_P|_{M_0}$. En effet, s'il existe une boule $b' \in \mathbb{B}_{K(M)}(M_0)$ avec $c_2 \in b' \subseteq P$, alors quitte à la remplacer par la plus petit boule qui contient b' et b , on peut supposer que b' contient b et donc $v(c_1 - b) = v(c_2 - b) \geq \rho(b')$, i.e. $c_1 \in b'$, ce qui est absurde. Par le lemme (5.8) (que l'on peut appliquer car dans un modèle le corps est dominant), on a $c_1 \equiv_{M_0} c_2$ et donc, en particulier $c_1 \equiv_A c_2$.

Dans le cas général, d'après le lemme (5.I0), il existe c'_1 tel que $c'_1 \models \alpha_P|_M$ et $(v(c'_1 - b), r(c'_1 - b)) \equiv_A (v(c_1 - b), r(c_1 - b)) \equiv_A (v(c_2 - b), r(c_2 - b))$. Par le cas déjà traité, on a $c_1 \equiv_A c'_1 \equiv_A c_2$. ✦

Lemme 5.I3 :

Supposons qu'il n'existe pas de tel b alors $\alpha_P|_A[x]$ est complet.

Démonstration. Supposons tout d'abord que A est dénombrable. Comme P est une intersection stricte, ce n'est pas un type (partiel) isolé sur A . En effet si on avait une formule θ à paramètres dans A telle que $\theta(\mathcal{M}) \subseteq P$, alors la plus petite boule contenant θ (qui existe car dans $\Gamma \cup \{\infty\}$, tout ensemble définissable a un maximum) est incluse dans P est A -définissable, ce qui est absurde. Par le théorème d'omission des types, il existe $A \subseteq \mathcal{M}_0 < \mathcal{M}$ tel que P ne contienne aucun point de \mathcal{M}_0 . Il ne contient alors pas non plus de boules \mathcal{M}_0 -définissables car, comme \mathcal{M}_0 est une sous-structure élémentaire de \mathcal{M} , cette boule contiendrait un point de \mathcal{M}_0 .

Par le lemme (5.8), $\alpha_P|_{\mathcal{M}_0}$ est un type complet. Ainsi si $c_i \models \alpha_P|_A$ pour $i = 1, 2$ alors, comme P ne contient aucune boule \mathcal{M}_0 -définissable, $c_i \models \alpha_P|_{\mathcal{M}_0}$ pour $i = 1, 2$ et donc $c_1 \equiv_{\mathcal{M}_0} c_2$. En particulier, $c_1 \equiv_A c_2$.

Dans le cas où A n'est pas dénombrable, pour tous $c_i \models \alpha_P|_A$ où $i = 1, 2$, soit $(\mathcal{M}_0, A_0) < (M, A)$ (dans le langage où on a rajouté un prédicat R pour A) dénombrable qui contient les c_i . Posons alors $Q = \bigcup \{b \in \mathbb{B}_{K(\mathcal{M}_0)}(A_0) : c_1 \in b\}$. Comme P est une intersection stricte de boules A -définissables et que c_1 est générique dans P sur A , tout boule A -définissable qui contient c_1 contient une sous-boule stricte A -définissable qui contient aussi c_1 . Comme cela s'exprime au premier ordre dans le langage avec un prédicat pour A , c'est aussi le cas dans (\mathcal{M}_0, A_0) et donc Q est une intersection stricte de boules A_0 -définissables dans laquelle c_1 est générique. De plus il est vrai dans (\mathcal{M}, A) que toute boule A -définissable qui contient c_1 contient aussi c_2 (car elle contient P), c'est donc aussi vrai dans (\mathcal{M}_0, A_0) et donc $c_2 \in Q$. Enfin, dans (\mathcal{M}, A) , le type partiel d'une boule A -définissable qui est contenue dans toutes les boules A -définissables qui contiennent c_1 implique que cette boule contient c_1 . C'est donc aussi le cas dans (\mathcal{M}_0, A_0) et donc Q ne contient aucune boule A_0 -définissable. Par le cas dénombrable on a donc que c_1 et c_2 ont le même type dans \mathcal{M}_0 sur A_0 , en particulier pour tout formule $\varphi[x, \bar{y}]$, la formule $\forall \bar{y} R(y) \Rightarrow \varphi[c_1, \bar{y}] \iff \varphi[c_2, \bar{y}]$ est vraie et donc elle est aussi vraie dans (\mathcal{M}, A) , i.e. ils ont le même type dans \mathcal{M} sur A . \spadesuit

On a donc bien montré les deux cas voulus. \blacksquare

Corollaire 5.14 :

Soient $\mathcal{M} \models pCF_{P,F}^{eq}$, $A \subseteq M$ tel que $\text{acl}^{eq}(A) \cap \mathbb{B}_{K(M)} \subseteq \text{dcl}^{eq}(A)$ et $B = \mathbb{B}_{K(M)}(A)$ alors pour tout $c \in K(M)$, $\text{tp}(c/B) \Rightarrow \text{tp}(c/A)$.

Démonstration. 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 (5.4), c est générique dans une intersection stricte P de boules A -définissables. Comme $\alpha_P \subseteq \text{tp}(c/B)$, c' est aussi générique sur P . D'après la proposition (5.11), si P ne contient pas de boule de B alors $\alpha_P|_A$ 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 cette même proposition, 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 $\mathbb{Q} \subseteq \text{dcl}(\emptyset)$ 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, à l'élimination des imaginaires (unaires) 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 $v(c-b) \equiv_A v(c'-b)$. \blacksquare

Pour finir montrons l'existence d'extensions invariantes dans $p\text{CF}_{P,f}$. Avant de commencer rappelons cependant que dans un \mathbb{Z} -groupe, il existe des extension invariantes. Tout type p sur un ensemble de paramètres A est déterminé par l'ensemble des $n_k \in \llbracket 0 \dots k-1 \rrbracket$ 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 si on met à droite tous les nouveaux points qui réalisent la coupure sur A , on obtient bien une extension A -invariante. En particulier une telle extension d'un type qui étend le type générique de P_Γ sur A est bien un type qui étend le type générique de P_Γ sur M .

Proposition 5.15 :

Soient $\mathcal{M} \models p\text{CF}_{P,f}^{\text{eq}}$, $A \subseteq M$ tel que $\text{acl}^{\text{eq}}(A) \cap \mathbb{B}_{K(M)} \subseteq \text{dcl}^{\text{eq}}(A)$ et $c \in K(M)$, $p = \text{tp}(c/A)$ alors une extension $\text{Aut}(\mathcal{M}/A)$ -invariante.

Démonstration. D'après le lemme (5.4), 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 $q = \text{tp}(v(c-a), r(c-a)/A)$. On pose alors $s_i = r_i(x-a)$ et soit q' une extension $\text{Aut}(\Gamma(M)/\Gamma(A))$ -invariante de $\text{tp}(v(c-a)/\Gamma(A))$. Comme Γ est stablement plongé, q' est un type complet sur \mathcal{M} et il est $\text{Aut}(\mathcal{M}/A)$ -invariant. De même le type $t[y, z] = q'[y] \cup \{z = s_i\}$ est un type complet sur \mathcal{M} qui est $\text{Aut}(\mathcal{M}/A)$ -invariant (il est consistant car comme précédemment toute sous formule finie de $\exists x v(x) = y \wedge r(x) = \bar{s}$ est dans q dont q' est une extension). Par le lemme (5.10), $p^* = \alpha_P | M \cup \bigcup_{m \in P(M)} t[v(x-m), r(x-m)]$ est consistant. Par la proposition (5.11), il est évident qu'il est complet et qu'il étend p . De plus, $\alpha_P | M$ est clairement $\text{Aut}(\mathcal{M}/A)$ -invariant et si $\sigma \in \text{Aut}(\mathcal{M}/A)$ et $m \in P(M)$ alors $\sigma(m) \in P(M)$ et $\sigma(t[v(x-m), r(x-m)]) = t[v(x-\sigma(m)), r(x-\sigma(m))]$ est aussi inclus dans p^* , d'où p^* est $\text{Aut}(\mathcal{M}/A)$ -invariant.

Si P ne contient pas de boules A -définissables, on peut prendre pour q n'importe quel type complet au dessus de A tel que $v(x)$ soit générique dans $P_\Gamma(A)$ et faire la même construction. ■

On peut remarquer que les réalisations de l'extension invariante qu'on a construite ici sont encore génériques dans P (maintenant au dessus de M).

Remarque 5.16 :

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 $p\text{CF}_{P,f}^{\text{eq}}$. Le passage à une extension définissable ne changeant rien aux types, on pourra les appliquer sans soucis.

Proposition 5.17 :

Soit $\mathcal{M} \models p\text{CF}_{P,f}^{\mathcal{G}}$ et $s \in \mathcal{S}(M)$. Il existe un type $\text{Aut}(M/s)$ -invariant de bases de s .

Démonstration. On note B_n le groupe des matrices triangulaires supérieures à coefficients dans K , B_n^* celles qui sont inversibles et $N_n = I_n + \{m \in B_n : v(b_{ij}) \gg 0\}$.

Lemme 5.18 :

Il existe un type p $\text{Aut}(M)$ -invariant de matrices de N_n qui est invariant sous multiplication à gauche, i.e. pour tout $A \subseteq M^{\text{eq}}$, $b \in N_n(A)$ et $c \models p|A$, $bc \models p|A$.

Démonstration. Soit q une extension $\text{Aut}(M)$ -invariante d'une complétion du type générique de $\bigcap_{n \in \mathbb{N}} p^n \mathcal{O}$ (une telle extension existe par la proposition (5.15)). Soit alors p le type des matrices $I_n + a$ telles que $a_{ij} = 0$ pour $i > j$ et sinon $a_{ij} \equiv q | M a_{kl > ij}$ où les couples sont ordonnés dans l'ordre lexicographique.

Il est clair que p est un type $\text{Aut}(M)$ -invariant (car outre les zéros, c'est une puissance tensorielle de q) d'éléments de N_n . Il suffit donc de montrer qu'il est invariant par multiplication à gauche. Soit donc $A \subseteq M^{\text{eq}}$, $(I_n + b) \in N_n(A)$ et $(I_n + c) \equiv p | A$. Soit $d = b + c + bc$, on a alors $(I_n + b)(I_n + c) = I_n + d$. Pour tout $i \leq j$, $d_{ij} = b_{ij} + c_{ij} + \sum_{i \leq k \leq j} b_{ik} c_{kj}$. Mais $v(c_{ij}) \ll v(b_{kj})$ et $v(c_{ij}) \ll v(c_{kj})$ pour tout $i < k$ car $c_{ij} \equiv q | A a_{kl > ij}$ et donc $v(d_{ij}) = v(c_{ij})$ et $r(d_{ij}) = r(c_{ij})$. Il s'en suit donc qu'on que pour tout $i \leq j$, $d_{ij} \equiv_{A c_{kl > ij}} c_{ij}$ et donc comme q est $\text{Aut}(M)$ -invariant, $(I_n + d) \equiv p | A$. \spadesuit

Lemme 5.19 :

Soit $R = gN_n$ un translaté de N_n dans $B_n^*(M)$. Il existe alors un type $\text{Aut}(M/\langle R \rangle)$ -invariant d'éléments de R .

Démonstration. Soit p le type d'élément de N_n donné au lemme (5.18). On note $p^g = \text{tp}(gc/M)$ pour $c \equiv p$ (c'est bien évidemment indépendant du choix de c). C'est un type d'éléments de R .

Soit alors $\sigma \in \text{Aut}(M/\langle R \rangle)$. Il envoie g sur gh pour un certain $h \in N_n(M)$. Soit $d \equiv p^g$, i.e. $d \equiv_M gc$ où $c \equiv p$. On a alors $\sigma(d) \equiv_M ghc'$ où $c' \equiv p$ car p est $\text{Aut } M$ -invariant. Comme p est invariant par multiplication à gauche, $hc' \equiv p$ et donc $\sigma(d) \equiv p^g$. \spadesuit

Par [HHMo6, Lemme 2.4.8], tout réseau a une base triangulaire et les bases triangulaires de tout réseau forment un translaté de $B_n^*(\mathcal{O})$ dans B_n^* . Soit b une base triangulaire de s et $\sigma \in \text{Aut}(M/s)$. Comme $e/p^m e$ est fini pour tout m , les vecteurs des bases b et $\sigma(b)$ de s sont égaux modulo $p^m e = bB_n(p^m \mathcal{O})$. On a donc $b^{-1}\sigma(b) \in I_n + B_n(p^m \mathcal{O})$ pour tout $m \in \mathbb{N}$, i.e. $b^{-1}\sigma(b) \in N_n$ et donc $\sigma(b) \in bN_n$. Il s'en suit donc que $\text{Aut}(M/s)$ laisse bN_n globalement invariant. Le type $\text{Aut}(M/\langle bN_n \rangle)$ -invariant d'éléments de bN_n du lemme (5.19) convient donc. \blacksquare

Corollaire 5.20 :

Soit $\mathcal{M} \equiv p\text{CF}_{P,f}^{\text{eq}}$ et $e \in M$, il existe $\bar{c} \in K(M)$ tel que $e \in \text{dcl}^{\text{eq}}(\bar{c})$ et $\text{tp}(\bar{c}/e)$ a une extension $\text{Aut}(M^{\text{eq}}/e)$ -invariante.

Démonstration. Pour $e \in K(M)$, on prend $\bar{c} = e$ et l'existence de l'extension est évidente car $\text{tp}(\bar{c}/e)$ est un type réalisé. Pour $e \in \mathcal{S}(M)$, c'est la proposition (5.17) et enfin pour $e \in \mathcal{T}(M)$, soit $s \in \mathcal{S}$ tel que $e \in s/\mathfrak{M}_M s$. Comme $\mathfrak{M}_M s \in \mathcal{S}(M)$, par le lemme (2.5) il existe $s' \in \mathcal{S}(M)$ qui est inter-définissable avec e . Le cas des réseaux appliqué à s' donne alors ce que l'on veut. \blacksquare

6 Élimination des imaginaires dans $p\text{CF}_{P,f}$

Dans cette section, on reprendra les notations de la proposition (1.16) avec $\mathcal{L} = \mathcal{L}_{p\text{CF}}^G$, $T = p\text{CF}_{P,f}^G$, $\tilde{\mathcal{L}} = \mathcal{L}_{\text{div}}^G$ et $\tilde{T} = \text{ACVF}_{0,p}^G$. On rappelle que \mathcal{M} est un modèle de $p\text{CF}_{P,f}^G$ assez

saturé et homogène et que $\widetilde{\mathcal{M}}$ est un modèle de $\text{ACVF}_{0,p}^{\mathcal{G}}$ qui contient M et qui est lui-même assez saturé et homogène.

Commençons par quelques remarques sur les boules et sur les types génériques.

Remarque 6.1 :

- (i) Les notions de génériques concordent bien dans \mathcal{M} et $\widetilde{\mathcal{M}}$. Soit $A \subseteq M^{\text{eq}}$ tel que $\text{acl}_{\mathcal{L}}^{\text{eq}}(A) \cap \mathbb{B}_{K(M)} \subseteq A$ et P est une intersection de boules $(b_i)_{i \in I}$ de \mathcal{M} telle que $b_i \in A$, alors si x est un point générique de P au dessus de A dans \mathcal{M} si et seulement s'il l'est aussi dans $\widetilde{\mathcal{M}}$. En effet, si x est générique dans $\widetilde{\mathcal{M}}$, comme toutes les boules de \mathcal{M} sont aussi des boules de $\widetilde{\mathcal{M}}$, x est générique dans \mathcal{M} . Réciproquement, soit $b \in \text{acl}_{\widetilde{\mathcal{L}}}(A)$ tel que $x \in b$, alors, comme on l'a démontré au lemme (5.3), $b' = b \cap M$ est une boule de \mathcal{M} . Soit $\sigma \in \text{Aut}_{\mathcal{L}}(\mathcal{M}/A)$, on peut l'étendre en $\tilde{\sigma} \in \text{Aut}_{\widetilde{\mathcal{L}}}(\widetilde{\mathcal{M}}/A)$ qui fixe globalement M . Comme $b \in \text{acl}_{\widetilde{\mathcal{L}}}(A)$, il y a un nombre fini de possibilités pour $\tilde{\sigma}(b)$ et donc il en est de même pour $\sigma(b')$. Il s'en suit donc que $b' \in \text{acl}_{\mathcal{L}}^{\text{eq}}(A) \cap \mathbb{B}_{K(M)} \subseteq A$. Comme b' contient x , elle ne peut être strictement incluse dans P et donc b non plus.
- (ii) Si une boule b de \mathcal{M} est \mathcal{L}_A -définissable où $\text{dcl}(A) \cap \mathbb{B}_{K(M)} \subseteq A$, alors $b \in A$ et comme $b(\widetilde{\mathcal{M}})$ est codé par le même point, b est aussi $\widetilde{\mathcal{L}}_A$ -définissable.

Montrons maintenant que les hypothèses de la proposition (1.16) sont vérifiées.

Proposition 6.2 ((i) dans $p\text{CF}_{P,f}$) :

Soient $\mathcal{M}' \preceq \mathcal{M}$ deux modèles de T et $c \in \text{dom}(M)$, on a alors $\text{dcl}_{\mathcal{L}}^{\text{eq}}(M'c) \cap M \subseteq \text{acl}_{\widetilde{\mathcal{L}}}(M'c)$.

Démonstration. Comme $\text{acl}_{\widetilde{\mathcal{L}}}(\text{dom}(M'c) \cap \text{dom}(M)) = \overline{\text{dom}(M'c)}^{\text{alg}}$ d'après la remarque (2.1.i), on a montré au lemme (4.1) que $\text{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap \text{dom}(M) = \text{acl}_{\widetilde{\mathcal{L}}}(\text{dom}(M'c) \cap \text{dom}(M))$ est un modèle de $p\text{CF}_{P,f}$. Par modèle complétude, on a $\text{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap \text{dom}(M) \preceq \text{dom}(M)$ et donc $\text{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap M^{\text{eq}} = (\text{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap \text{dom}(M))^{\text{eq}} \preceq \mathcal{M}^{\text{eq}}$. Comme $\mathcal{L}_{p\text{CF}}^{\mathcal{G}}$ est une extension définissable de $\mathcal{L}_{p\text{CF}_{P,f}}^{\text{eq}}$, on a donc aussi $\text{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap M \preceq \text{mod}$. Enfin, comme la clôture définissable ne dépend pas du modèle dans une extension élémentaire, on a bien que $\text{dcl}_{\mathcal{L}}^{\text{eq}}(M'c) \cap M \subseteq \text{acl}_{\widetilde{\mathcal{L}}}(M'c) \cap M \subseteq \text{acl}_{\widetilde{\mathcal{L}}}(M'c)$. ■

Proposition 6.3 ((ii) dans $p\text{CF}_{P,f}$) :

Pour tout $A = \text{acl}_{\mathcal{L}}^{\text{eq}}(A) \cap M$ et $c \in \text{dom}(M)$, on a $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) = \text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac)$ et donc, en particulier, $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap M \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap M$.

Démonstration. D'après le corollaire (4.6), on a, pour tout $A \subseteq K(M)$, $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap K(M) = \text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap K(M)$. Or cet ensemble est un modèle de $p\text{CF}_{P,f}$ et donc $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \subseteq (\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap K(M))^{\text{eq}} = \text{dcl}_{\mathcal{L}}^{\text{eq}}((\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap K(M))) = \text{dcl}_{\mathcal{L}}^{\text{eq}}((\text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap K(M))) = \text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac)$. Il faut cependant étendre ce résultat à des ensembles de paramètres géométriques (et pas uniquement dans la sorte du corps).

Soit $A = \{a_i : i \in \kappa\}$ une énumération de A . Pour tout i , soit $\bar{c}_i \in \text{dom}(M)$ tel que $a_i \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(\bar{c}_i)$ et $p_i \in S_{\mathcal{L}}(M)$ une extension $\text{Aut}_{\mathcal{L}}(\mathcal{M}/a_i)$ -invariante de $\text{tp}_{\mathcal{L}}(\bar{c}_i/a_i)$ (qui existe par le corollaire (5.20)). On construit alors $(A_i)_{i \in \kappa}$ par induction. On pose $A_0 = A$, $A_{i+1} = A_i \cup \{\bar{b}_i\}$ où $\bar{b}_i \models p_i | \text{acl}_{\mathcal{L}}^{\text{eq}}(A_i c)$ et $A_\lambda = \bigcup_{i < \lambda} A_i$ pour tout i et $\lambda < \kappa$. Montrons alors, par

induction, que $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_i c) \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac)$. Le cas $i = 0$ est évident et pour λ limite, $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_\lambda c) = \bigcup_{i < \lambda} (\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_i c)) \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac)$.

Reste alors le cas successeur. Soient $a \in \text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_{i+1}c)$ et $\sigma \in \text{Aut}_{\mathcal{L}}(\mathcal{M}/A_i c)$. Comme $a \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_{i+1}c)$, il existe $\varphi[x, y, \bar{z}] \in \mathcal{L}_{A_i}$ telle que a est défini par $\varphi[x, c, \bar{b}_{i+1}]$. Comme $a \in \text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \subseteq \text{acl}_{\mathcal{L}}^{\text{eq}}(A_i c)$, il s'en suit que $\varphi[a, c, \bar{z}] \in p_{i+1} | \text{acl}_{\mathcal{L}}^{\text{eq}}(A_i c)$ et comme p_{i+1} est $\text{Aut}_{\mathcal{L}}(\mathcal{M}/A)$ -invariant et que $\sigma(a) \in \text{acl}_{\mathcal{L}}^{\text{eq}}(Ac)$, on a aussi $\varphi[\sigma(a), c, \bar{z}] \in p_{i+1} | \text{acl}_{\mathcal{L}}^{\text{eq}}(A_i c)$ et donc $\mathcal{M} \models \varphi[\sigma(a), c, \bar{b}_{i+1}]$. Il s'en suit donc que $\sigma(a) = a$ et donc que $a \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_i c)$. On a donc $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_{i+1}c) \subseteq \text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_i c) \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac)$.

Pour tout i , comme $\bar{b}_i \equiv_A \bar{c}_i, a_i \in \text{dcl}_{\mathcal{L}}^{\text{eq}}(\bar{b}_i)$. Il s'en suit donc, comme $\bar{b}_i \in \text{dom}(M)$, que $A \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_k \cap \text{dom}(M))$. On a alors $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \subseteq \text{acl}_{\mathcal{L}}^{\text{eq}}(A_\kappa \cap \text{dom}(M)c) \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_\kappa \cap \text{dom}(M)c) \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_\kappa c)$ et donc $\text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) = \text{acl}_{\mathcal{L}}^{\text{eq}}(Ac) \cap \text{dcl}_{\mathcal{L}}^{\text{eq}}(A_\kappa c) \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(Ac)$. ■

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

Proposition 6.4 ((iii') dans $pCF_{P,f}$):

Soit $e \in \text{dcl}_{\mathcal{L}}(M) \subseteq \widetilde{\mathcal{M}}$, 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 $e \in \text{dcl}_{\mathcal{L}}(e')$.

Démonstration. Supposons tout d'abord que $e \in K(\widetilde{\mathcal{M}})$. D'après la remarque (2.1), comme $K(M)$ est Hensélien et qu'on est en caractéristique nulle, $K(M)$ est $\text{dcl}_{\mathcal{L}}$ -clos. On a donc $e \in K(M)$.

Si maintenant, $e \in \mathcal{S}(\widetilde{\mathcal{M}})$, comme $e \in \text{dcl}_{\mathcal{L}}(M) \subseteq \text{acl}_{\mathcal{L}}(M)$ et que $\text{acl}_{\mathcal{L}}(M) \models \text{ACVF}_{0,p}^{\mathcal{G}}$ (la preuve est similaire à celle de la proposition (6.2) dans le cas de $pCF_{P,f}^{\mathcal{G}}$), il s'en suit que e a une base dans $\text{acl}_{\mathcal{L}}(M)$. Il existe donc une extension finie $K(\mathcal{M}) \leq L$, telle que e ait une base dans L . Soit $m = [L : K(\mathcal{M})]$. On sait par le théorème (3.19), 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 $K(\mathcal{M}) \leq L'$ 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 $a \in \overline{\mathbb{Q}[\alpha]}^{\text{alg}}$ tel que $L = K(\mathcal{M})[a]$, $\mathcal{O}_L = \mathcal{O}_{\mathcal{M}}[a]$ et dont le polynôme minimal annulateur est dans $\mathbb{Q}[\alpha]$. On connaît l'existence d'un tel a par le théorème (3.19). Ce a permet donc de définir une bijection $f_a : L \rightarrow K(\mathcal{M})^m$ qui induit une bijection $f_a^n : L^n \rightarrow K(\mathcal{M})^{mn}$. 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), e 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 $S_{mn}(\mathcal{M})$.

Si a' est un conjugué de a au dessus de $\mathbb{Q}[\alpha]$, comme le polynôme minimal annulateur de a au dessus de $K(\mathcal{M})$ est dans $\mathbb{Q}[\alpha]$, c'est aussi le polynôme minimal annulateur au dessus de $\mathbb{Q}[\alpha]$ et donc a et a' sont conjugués au dessus de $K(\mathcal{M})$. Il existe donc $\sigma \in \text{Aut}(L/K(\mathcal{M}))$ un automorphisme de corps valués, qui envoie a sur a' . De plus, comme e et $e' \in \text{dcl}_{\mathcal{L}}(M)$ (à vrai dire on a même $e' \in M$), ces deux points sont fixés par σ et donc $f_{\sigma(a)}^n(e) = e'$. Il s'en suit donc que tout automorphisme de $\widetilde{\mathcal{M}}$ qui fixe globalement M fixe e si et seulement s'il fixe e' .

Il reste alors à démontrer que $e \in \text{dcl}_{\tilde{\mathcal{L}}}(e')$. Mais l'inverse de $f_a, g_a : (x_0 \dots x_{m-1}) \mapsto \sum_i x_i a^i$ peut être étendue par la même formule en un $\mathcal{O}_{\tilde{\mathcal{M}}}$ -module $\tilde{g}_a : K(\tilde{\mathcal{M}})^m \rightarrow K(\tilde{\mathcal{M}})$, qui induit donc un morphisme de $\mathcal{O}_{\tilde{\mathcal{M}}}$ -module $\tilde{g}_a^n : K(\tilde{\mathcal{M}})^{mn} \rightarrow K(\tilde{\mathcal{M}})^n$. Ce morphisme envoie une base de e' sur une base de e , on a donc $\tilde{g}_a^n(e') = e$. Comme précédemment $\tilde{g}_a = \tilde{g}_{a'}$ pour tout conjugué de a au dessus de $\mathbb{Q}[\alpha]$ et donc tout automorphisme de $\tilde{\mathcal{M}}$ qui fixe e' fixe bien e , i.e. $e \in \text{dcl}(e')$.

Pour ce qui est des $e \in \mathcal{T}_n(\tilde{\mathcal{M}})$, 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 (2.5), il existe $s \in \mathcal{S}_{n+1}(L)$ tel que tout automorphisme de L fixe e si et seulement si il fixe s . Comme on a déjà traité le cas des réseaux, on peut trouver e' tel que tout automorphisme de $\tilde{\mathcal{M}}$ 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, on a $e \in \text{dcl}_{\tilde{\mathcal{L}}}(s)$ et, comme on l'a montré précédemment, $s \in \text{dcl}_{\tilde{\mathcal{L}}}(e')$. Il s'en suit donc que $e \in \text{dcl}_{\tilde{\mathcal{L}}}(e')$ ■

Corollaire 6.5 :

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

Démonstration. Comme X un ensemble $\tilde{\mathcal{L}}_M$ -définissable sans quantificateurs, il a un code $\langle X \rangle \in \text{dcl}_{\tilde{\mathcal{L}}}(\mathcal{M})$. D'après la proposition (6.4), il existe $\bar{e}' \in M$ tel que tout automorphisme de $\tilde{\mathcal{M}}$ qui fixe globalement M fixe $\langle X \rangle$ si et seulement si il fixe \bar{e}' et que $\langle X \rangle \in \text{dcl}_{\tilde{\mathcal{L}}}(\bar{e}')$. Il suffit donc de montrer que $\bar{e}' \in A$. Soit $\sigma \in \text{Aut}(\mathcal{M}^{\text{eq}}/A')$ et $\tilde{\sigma}$ une extension de σ à $\tilde{\mathcal{M}}$ (qui laisse bien M globalement invariant). Par hypothèse, $\tilde{\sigma}(\langle X \rangle) = \langle X \rangle$ et donc $\sigma(\bar{e}') = \tilde{\sigma}(\bar{e}') = \bar{e}'$. Il s'en suit donc que $\bar{e}' \in \text{dcl}_{\tilde{\mathcal{L}}}^{\text{eq}}(A') = A'$ et comme $\bar{e}' \in M$, on a bien $\bar{e}' \in A$. ■

Proposition 6.6 ((iv) dans $pCF_{P,f}$) :

Tout sous-ensemble X \mathcal{L}_M -définissable inclus dans $\text{dom}(M)$ a un code dans M .

Démonstration. Soit x un code de X dans \mathcal{M}^{eq} . On pose $A = \text{acl}_{\tilde{\mathcal{L}}}^{\text{eq}}(x)$ et $B = \mathbb{B}_{K(M)}(A)$. D'après le corollaire (5.14), pour tout $c \in \text{dom}(M)$, on a $\text{tp}(c/B) \Rightarrow \text{tp}(c/A)$, 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 (1.17) (et la proposition (6.4)) et donc le lemme (1.10) permet de conclure. ■

Proposition 6.7 ((v) dans $pCF_{P,f}$) :

Soient $c \in \text{dom}(M)$ et $A \subseteq M$ tel que $\text{acl}_{\tilde{\mathcal{L}}}^{\text{eq}}(A) \cap M = A$. Il existe un type $\tilde{p} \in \mathcal{S}_{\tilde{\mathcal{L}}}(\tilde{\mathcal{M}})$ $\text{Aut}_{\tilde{\mathcal{L}}}(\tilde{\mathcal{M}}/A)$ -invariant tel que $\tilde{p}|_M$ soit consistant avec $\text{tp}_{\tilde{\mathcal{L}}}(c/A)$ et que pour toute fonction f $\tilde{\mathcal{L}}_M$ -définissable, telle que $\tilde{p} \subseteq \mathcal{D}_f$, on ait :

(*) il existe $(\varepsilon_i)_{i \in \kappa} \in \text{dcl}_{\tilde{\mathcal{L}}}(A, \langle f \rangle)$, tel que $\sigma \in \text{Aut}_{\tilde{\mathcal{L}}}(\tilde{\mathcal{M}}/A)$ fixe $\partial_{\tilde{p}} f$ si et seulement si il existe $\alpha < \kappa$ tel que σ fixe tous les ε_i pour $i \geq \alpha$;

Démonstration. Par le lemme (5.4), le type $p = \text{tp}_{\mathcal{L}}(c/A)$ d'un point $c \in \text{dom}(M)$ est le un type générique sur une intersection stricte $P = \bigcap_i b_i$ de boules (fermées) A -définissables. On note $\tilde{p} = \alpha_p|_{\tilde{M}}$. Comme toutes les boules b_i sont A -définissables et que $\text{dcl}_{\mathcal{L}}^{\text{eq}}(A) \cap \mathbb{B}_{K(M)} \subseteq \text{dcl}_{\mathcal{L}}^{\text{eq}}(A) \cap M = A$, d'après la remarque (6.1.ii), toutes les boules b_i sont aussi A -définissables dans \tilde{M} . Le type \tilde{p} est donc bien $\text{Aut}_{\mathcal{L}}(\tilde{M}/A)$ -invariant. De plus, d'après le lemme (5.10) et la remarque (6.1.i), $\tilde{p}|_M = \alpha_P|_M$ est consistant avec p .

Posons alors $e_i = \partial_{b_i} f$ qui existe bien car le type générique d'une boule dans ACVF est définissable. Montrons alors que ces e_i conviennent. Soit $\sigma \in \text{Aut}(\tilde{M}/A)$ et notons $X := \{x \in M : f(x) \neq \sigma(f)(x)\}$. Il est clair que $\partial_{\alpha_P} f = \partial_{\alpha_P} \sigma(f)$ si et seulement si $X \cap P$ est inclus dans une sous-boule stricte de P . Mais comme X est une combinaison booléenne finie de boules et que tout boule b vérifie qu'il existe i tel que $P \cap b = P \cap b_i$ (et donc pour tout $j \geq i$, $P \cap b = P \cap b_j$), c'est aussi le cas pour X . Soit donc i tel que $X \cap P = P \cap b_j$ pour tout $j \geq i$. Alors $X \cap P$ est inclus dans une sous-boule stricte de P si et seulement si pour tout $j \geq i$ $X \cap b_j$ est inclus dans une sous-boule stricte de b_j , i.e. $e_j = \partial_{b_j} f = \partial_{b_j} \sigma(f) = \sigma(e_j)$. ■

Théorème 6.8 :

La théorie $p\text{CF}_{P,f}$ élimine les imaginaires dans le langage $\mathcal{L}_{p\text{CF}}^G$. Elle les élimine en fait dans la restriction de ce langage au sortes K et \mathcal{S} .

Démonstration. Ce théorème est une conséquence immédiate de la proposition (1.16) dont les hypothèses sont démontrées dans les lemmes (6.2), (6.3), (6.4), (6.6) et (6.7).

Pour ce qui est des torseurs, comme on a vu dans la preuve du lemme (6.4), 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 (2.5). ■

Références

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

[Den84] Jan DENEFF. « 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.

[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.

[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.

[HMo8] 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.
- [Neu54] Bernhard H. NEUMANN. « Groups Covered by Permutation Subsets ». Dans : *The Journal of the London Mathematical Society* 29 (1954), p. 236–248.
- [Poi83] Bruno POIZAT. « Une théorie de Galois imaginaire ». Dans : *The Journal of Symbolic Logic* 48.4 (1983), p. 1151–1170.
- [PR84] Alexander PRESTEL et Peter ROQUETTE. *Formally p-adic Fields*. Lecture Notes in Mathematics 1050. Springer-Verlag, 1984.
- [She78] Saharon SHELAH. *Classification Theory and the Number of Non-Isomorphic Models*. Studies in Logic 92. North-Holland Publishing Company, 1978.