Le principe d'Ax, Kochen et Ershov

Tibo Goupil et Jianxin Wang
Encadrant: Silvain Rideau-Kikuchi

Table des matières

1 Introduction

La théorie des modèles des corps valués débute dans les années 1950 par les travaux de Robinson qui démontre le résultat suivant :

Théorème 1.1 *La théorie des corps valués et algébriquement clos est complète, i.e. pour tous deux modèles $\mathcal{M}$, $\mathcal{N}$ de cette théorie, on a que $\mathcal{M} \equiv \mathcal{N}$.*

Dans les années 1960s, Ax-Kochen et, indépendamment, Ershov, ont montré un théorème pour les corps valués henséliens. Il y a des applications à la théorie de nombre p-adiques.
Dans ce mémoire, le but principal est ce théorème de Ax-Kochen Ershov (AKE).

Théorème 1.2 (AKE) *Soient (K, A) et (K', A') deux corps valués henséliens de corps résiduels k, k', et les groupes de valuations Γ, Γ'(comme groupes abéliens ordonnés). Supposons que car(k)=0. Alors*

$$(K, A) \equiv (K', A') \text{ si et seulement si } k \equiv k' \text{ et } \Gamma \equiv \Gamma'.$$

On suit la preuve donnée par Lou van den Dries dans le livre [1]. Avant d'exposer la démonstration, on donne des résultats préliminaires. Dans la section 2, on discute des anneaux henséliens, en particulier, $\mathbb{Z}_p$. Dans la section 3, on donne une introduction de la théorie des valuations. On montre que la théorie des corps valués algébriquement clos élimine les quantificateurs. Dans la section 4, on continue la discussion sur les corps valués, et surtout des extensions immédiates qui seront utiles dans la démonstration du théorème de AKE.
Revenons au théorème de AKE. Il y a des propriétés pour $\mathbb{Z}_p$ comme corollaires. Par exemple, le corollaire suivant :

Théorème 1.3 (Principe de AKE) *Soit σ un énoncé du language des anneaux, qui est le langage $L_{ann} = \{0, 1, +, \cdot\}$. Alors il existe $N \in \mathbb{N}$ tel que pour tout $p > N$ premier,*

$$\mathbb{Z}_p \models \sigma \text{ si et seulement si } \mathbb{F}_p[[t]] \models \sigma.$$

On peut aussi déduire le résultat suivant :

Corollaire 1.4 *Soient k_1, k_2 deux corps de caractéristique 0. Alors*

$$k_1[[t]] \equiv k_2[[t]] \text{ si et seulement si } k_1 \equiv k_2.$$

2 Anneaux locaux henséliens

Dans cette section on énonce le lemme d'Hensel, qui implique que tout anneau local et complet est hensélien. On définit les nombres p-adiques et on montre que les anneaux henséliens de caractéristique résiduelle nulle ammettant un relèvement de leur corps résiduel.

2.1 Premières définitions

Dans cette partie on introduit les première définitions. Les anneaux sont par convention commutatifs et unitaires.

Définition 2.1 *Un anneau R est dit local s'il admet un unique idéal maximal. Cet idéal maximal est alors noté $\mathfrak{m}_R$ (où juste $\mathfrak{m}$ si R est clair) et le corps $k = R/\mathfrak{m}$ est appelé corps résiduel de R.*

Remarque 2.2 *Si R est local, un élément $x \in R$ est inversible si et seulement si sa classe est non nulle dans k.*

Définition 2.3 *Soit R un anneau local, on dit que R est hensélien lorsque :*
Pour tous $f(X) \in R[X]$ et $\alpha \in R$ tels que $f(\alpha) \in \mathfrak{m}$ et $f'(\alpha) \notin \mathfrak{m}$, il existe $a \in R$ tel que $f(a) = 0$ et $a \equiv \alpha \ mod \ \mathfrak{m}$.

Définition 2.4 *Un anneau de valuation est un anneau intègre R dont l'ensemble de ses idéaux maximaux est totalement ordonné pour l'inclusion.*

Remarque 2.5 *Un anneau de valuation est un anneau local.*

Après avoir introduit des propriétés des anneaux, on veux établir une topologie sur ceux-ci :

Définition 2.6 *Soit R un anneau, une valuation sur R est une fonction*
$v : R \to \mathbb{Z} \cup \{\infty\}$ (dans cette partie on considère uniquement les valuations à valuations dans $\mathbb{Z}$, le cas général sera vu en partie 3) telle que pour tout $x, y \in R$:
— $v(1) = v(-1) = 0$

— $x = 0 \Leftrightarrow v(x) = \infty$
— $v(x + y) \geq min(|x|, |y|)$
— $v(xy) = v(x) + v(y)$

On munit alors R de la topologie engendrée par les ensembles
$\{x \in R \ : \ v(x - a) > n \}$ *pour tous $a \in R$ et $n \in \mathbb{N}$, et on dit que R est complet s'il est complet en temps qu'espace métrique (vu que l'on travaille avec des valuations et non des distances les suites convergent lorsque les valuations tendent vers l'infini et non 0).*

2.2 Lemme d'Hensel

La propriété de complétude entraîne les deux résultats suivants (les preuves sont traitées par Van den Dries dans son livre [1]) :

Lemme 2.7 *Soit R un anneau complet pour une valuation v telle que $v(x) \geq 0$ pour tout $x \in R$. Alors R est local et $\mathfrak{m} = \{x \in R \mid v(x) > 0\}$.*

Lemme 2.8 (Lemme d'Hensel) *On conserve les notations et hypothèses du lemme précédant. Alors l'anneau local R est hensélien.*

2.3 Le corps de nombres p-adiques $\mathbb{Q}_p$

Dans cette sous-section on fixe un nombre premier p. Définissons d'abord une valuation sur $\mathbb{Q}$.

Définition 2.9 *On appelle valuation p-adique la fonction $v_p : \mathbb{Z} \to \mathbb{Z} \cup \{\infty\}$ telle que :*
— $v_p(0) = \infty$
— $a = p^{v_p(a)} b$ *avec $p \nmid b$ pour tout $a \in \mathbb{Z} \setminus \{0\}$*

On vérifie alors que v_p est une valuation :

Lemme 2.10 *La valuation p-adique est une valuation au sens de la définition 2.6 .*

Remarque 2.11 *La valuation p-adique s'étend naturellement à $\mathbb{Q}$ et est alors une valuation sur $\mathbb{Q}$ (on pose $v(x/y) = v(x) - v(y)$, la définition est correcte car elle ne dépend pas du choix des représentants).*

Maintenant que l'on a défini une valuation sur $\mathbb{Q}$, on peut définir les nombres p-adiques et les entiers p-adiques :

Définition 2.12 *On note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour v_p, que l'on appelle corps des nombres p-adiques. De plus on note $\mathbb{Z}_p$ la clôture de $\mathbb{Z}$ dans $\mathbb{Q}_p$, que l'on appelle anneau des entiers p-adiques.*

La continuité des opérations entraîne le résultat suivant :

Lemme 2.13 *L'ensemble $\mathbb{Q}_p$ est un corps et $\mathbb{Z}_p$ est un anneau.*

Remarque 2.14 *Comme les opérations algébriques v_p se prolonge continuement à $\mathbb{Q}_p$ et est toujours une valuation.*

Des considérations topologiques et algébriques sur $\mathbb{Q}_p$ permettent alors d'établir les résultats suivants :

Proposition 2.15 *1. L'anneau $\mathbb{Z}_p$ est un anneau local hensélien d'idéal maximal $p\mathbb{Z}_p$.*

2. *Le morphisme surjectif d'anneau*
   $\mathbb{Z} \to \mathbb{Z}_p/p\mathbb{Z}_p$ *induit un isomorphisme d'anneaux* $\mathbb{F}_p \to \mathbb{Z}_p/p\mathbb{Z}_p$*, le corps résiduel de* $\mathbb{Z}_p$ *est donc isomorphe à* $\mathbb{F}_p$*.*
3. *L'anneau* $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ : \ v(x)_p \geq 0 \ \}$ *et* $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ : \ v(x)_p > 0 \ \}$

Preuve *On regardera la preuve de la proposition 2.8 de Van den Dries [1].*

2.4 Relèvement du corps résiduel

Dans cette sous-section 2.4 nous allons montrer que tout anneau hensélien de caractéristique résiduelle nulle admet un relèvement du corps résiduel, ce qui sera utilisé dans la démonstration du théorème d'AKE. On commence d'abord par définir ce qu'un relèvement :

Lemme 2.16 *Soient* R *un anneau local et* E *un un sous-corps de* R *(un sous-anneau qui est en plus un corps). Alors la projection canonique envoie isomorphiquement* E *vers un sous-corps* $\overline{E}$ *du corps résiduel* k*.*

Définition 2.17 *On conserve les notations que du lemme* 2.16*. Si* $\overline{E} = k$*, on dit que* E *est un relèvement de* k*.*

Un anneau local n'admet pas forcément de relèvement du corps résiduel, par exemple $\mathbb{Z}/p^2\mathbb{Z}$ est un anneau local qui n'admet pas de sous-corps. En revanche cela est vrai si on se restreint aux anneaux henséliens de caractéristique résiduelle nulle.

Théorème 2.18 *Soit* R *un anneau hensélien tel que* $car(k) = 0$*. Alors le corps résiduel* k *possède un relèvement.*

Preuve *L'ensemble des sous-corps de* R *muni de l'inclusion est inductif, pour appliquer le lemme de Zorn il suffit donc de montrer qu'il est non vide.*
Comme $car(k) = 0$*, on a* $car(R) = 0$*, donc* R *contient* $\mathbb{Z}$ *et d'après la remarque 2.2, comme* $\mathbb{Z} \cap \mathfrak{m} = 0$ *(car* $car(k) = 0$*),* R *contient* $\mathbb{Q}$*. Donc d'après le lemme de Zorn,* R *admet un sous-corps maximal* E*. Supposons que* $\overline{E} \neq k$ *et considérons* $y \in k \setminus \overline{E}$ *et* $x \in R$ *un représentant de* y*. Il y a deux cas à traiter :*

Cas n°1 y *est transcendant sur* $\overline{E}$*. Alors* x *est transcendant sur* E *et la projection plonge* $E[x]$ *dans* k*, donc d'après la remarque 2.2,* R *contient* $E(x)$

Cas n°2 y *est algébrique sur* $\overline{E}$*. Considérons* $f(X) \in E[X]$ *un polynôme unitaire tel que son image* $\overline{f}[X] \in \overline{E}[X]$ *par la projection soit le polynôme minimal de* y *sur* E*. Comme* f *est irréductible dans* $\overline{E}$*, il est à racines simples dans* k*, donc* $f(x) \in \mathfrak{m}$ *et* $f'(x) \notin \mathfrak{m}$*. Ainsi, comme* R *est hensélien, quitte à changer de représantant on peut supposer que* $f(x) = 0$*, donc* x *est irréductible et* $E[x]$ *est un sous-corps de* R*.*

Dans les deux cas, E *est inclus dans un sous-corps strictement plus grand, ce qui contredit la maximalité.*
Ainsi, $\overline{E} = k$ *et* E *est un relèvement de* k*.* □

3 La théorie de la valuation

Dans cette section, on introduit la théorie de la valuation sur un corps. De plus, on montre que la théorie des corps valués algébriquement clos (ACF_{val}) élimine les quantificateurs.

3.1 Valuation

Définition 3.1 *Soit A un anneau intègre. Une valuation sur A est une fonction $v : A\backslash\{0\} \to \Gamma$, où Γ est un groupe abélien ordonné, tel que*
(V1) $v(x+y) \geqslant \min\{v(x), v(y)\}$, si $x+y \neq 0$,
(V2) $v(xy) = v(x) + v(y)$.

Remarque 3.2 *Soit $v : A\backslash\{0\} \to \Gamma$ une valuation de A. Alors,*
(i) $v(1) = v(-1) = 0$, car v est un morphisme de groupes quand on la restreint sur $U(A)$, l'ensemble des éléments inversibles de A. Et donc $v(x) = v(-x)$ pour tout $x \in A\backslash\{0\}$.
(ii) Notons K le corps des fractions de A, alors toute valuation $v : A\backslash\{0\} \to \Gamma$ s'étend uniquement en une valuation $v : K^\times \to \Gamma$, par
$v(x/y) = v(x) - v(y)$, pour tous $x, y \in A\backslash\{0\}$.
(iii) Par convention, on étend v en K en posant $v(0) = \infty$, où $\Gamma_\infty = \Gamma \cup \{\infty\}$, et on définit $\gamma + \infty = \infty + \gamma = \infty$, $\gamma < \infty$ pour tout $\gamma \in \Gamma$. Alors (V1) et (V2) dans la définition 3.1 restent vrai pour tous $x, y \in K$.
(iv) Pour tout $x \in K^\times$, on a $v(x) = -v(x^{-1})$ par $(V2)$.
(v) Par (V1), pour $\alpha_1, \ldots, \alpha_n \in A$, si $v(\alpha_1) < v(\alpha_i)$ pour tout $i > 1$, alors

$$v(\alpha_1 + \cdots + \alpha_n) = v(\alpha_1).$$

En effet, par récurrence il suffit de traiter le cas où $n = 2$. Par $(V1)$, $v(\alpha_1 + \alpha_2) \geq v(\alpha_1)$ et $v(\alpha_1) \geq \min\{v(\alpha_1 + \alpha_2), v(\alpha_2)\} = v(\alpha_1 + \alpha_2)$ car $v(\alpha_1) < v(\alpha_2)$. D'où l'égalité.

Quand on considère une valuation $v : K^\times \to \Gamma$, on suppose toujours que $v(K^\times) = \Gamma$, et on appelle Γ **le groupe de valuation** de v. Et on appelle $(K, \Gamma; v)$ un **corps valué**.

Définition 3.3 *Soit $v : K^\times \to \Gamma$ une valuation sur un corps K. On pose :*
(i) $\mathcal{O}_v = \{x \in K,\ v(x) \geqslant 0\}$,
(ii) $\mathfrak{m}_v = \{x \in K,\ v(x) > 0\}$,
(iii) $k_v = \mathcal{O}_v/\mathfrak{m}_v$.

Remarque 3.4 *En utilisant la remarque 3.2 (iv), on a que $v(x) = v(x^{-1}) = 0$ pour tout $x \in \mathcal{O}_v\backslash\mathfrak{m}_v$, et $x^{-1} \notin \mathcal{O}_v$ si $x \in \mathfrak{m}_v$. Par $(V1)$ et $(V2)$, les éléments non inversibles de $\mathcal{O}_v$ forment un idéal, donc on en déduit que $\mathcal{O}_v$ est un anneau local d'idéal maximal $\mathfrak{m}_v$.*

Réciproquement, étant donné k un corps et Γ un groupe abélien ordonné, il existe un corps valué (K, v) associé tel que $k_v = k$ et $v(K^\times) = \Gamma$. Posons $K = k((t^\Gamma))$ l'ensemble des séries formelles $f(t) = \sum_{\gamma\in\Gamma} a_\gamma t^\gamma$, avec les coefficients $a_\gamma \in k$, tel que le support de f,

$$supp(f) = \{\gamma \in \Gamma : a_\gamma \neq 0\},$$

est un sous-ensemble bien ordonné de Γ. On définit les deux opérations suivantes sur K :

$$\sum a_\gamma t^\gamma + \sum b_\gamma t^\gamma = \sum (a_\gamma + b_\gamma) t^\gamma,$$

$$\big(\sum a_\gamma t^\gamma\big)\big(\sum b_\gamma t^\gamma\big) = \sum_\gamma \Big(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\Big) t^\gamma.$$

Proposition 3.5 ([1, Section 3.1]) *Les opérations ci-dessus sont bien définies et K est un corps. On définit l'application $v : K\backslash\{0\} \to \Gamma$ par*

$$v\big(\sum a_\gamma t^\gamma\big) = \min\{\gamma : a_\gamma \neq 0\}.$$

Alors v est une valuation de K avec $k_v = k$, $v(K^\times) = \Gamma$. De plus, $\mathcal{O}_v = \{f \in K : supp(f) \subseteq \Gamma^{\geq 0}\}$, $\mathfrak{m}_v = \{f \in K : supp(f) \subseteq \Gamma^{>0}\}$.

Remarque 3.6 *On appelle $k((t^\Gamma))$ un **corps de Hahn**. Un exemple classique est $k((t^{\mathbb{Z}}))$, pour lequel $\mathcal{O}_v = k[[t]]$ les séries de Laurent.*

La proposition suivante s'agit d'une estimation de la cardinalité d'un corps valué. Elle est due à Krull.

Proposition 3.7 ([1, Proposition 3.6]) *Soit $(K, \Gamma; v)$ un corps valué. Notons $k \overset{def}{=} k_v$, alors*

$$|K| \leq |k|^{|\Gamma|}.$$

Cette proposition sera utile pour pouvoir utiliser le lemme de Zorn.

3.2 Extensions des corps valués

D'abord on s'intéresse aux extensions des anneaux de valuations. Dans cette partie, les anneaux sont toujours locaux et intègre.
Soit $(K, \Gamma; v)$ un corps valué, alors $\mathcal{O}_v$ est un anneau de valuation. Et réciproquement, étant donné un anneau de valuation A dans $K = Frac(A)$, considérons $\Gamma_A = K^\times / U(A)$, avec une relation $\leq$ définie par

$$yU(A) \leq xU(A) \iff x/y \in A, \quad x, y \in K^\times,$$

alors Γ_A est un groupe abélien ordonné et

$$v_A : K^\times \to \Gamma_A, \quad v_A(x) = xU(A)$$

est une valuation. De plus, $\mathcal{O}_{v_A} = A$.
Soient $(v_1, \Gamma_1), (v_2, \Gamma_2)$ deux valuations sur K, d'après [1, Section 3.1], il existe un unique isomorphisme de groupes abéliens ordonnés $i : \Gamma_1 \to \Gamma_2$ tel que $i \circ v_1 = v_2$ si et seulement si $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$. Dans ce cas, on dit que v_1, v_2 sont **équivalentes**. Autrement dit, à équivalence près, un corps valué est totalement déterminé par $A = \mathcal{O}_v$, et on notera $k_A = k_v$. Cela ne dépend pas du choix de v à équivalence pprès.

Définition 3.8 *(i) Soient A, B deux anneaux d'idéaux maximaux $\mathfrak{m}_A, \mathfrak{m}_B$. On dit que B **domine** A, si $\mathfrak{m}_A \subseteq \mathfrak{m}_B$ et $A \subseteq B$. Dans ce cas, on a $\mathfrak{m}_A = \mathfrak{m}_B \cap A$.*
*(ii) En utilisant la discussion précédente, par abus de notation, un **corps valué** est la donnée d'un couple (K, A) où A est un anneau de valuation de K.*
*(iii) Soient (K, A), (L, B) deux corps valués. On dit que (L, B) est une **extension de corps valué** de (K, A) si $j : K \to L$ est une extension de corps, et $B \cap j(K) = A$. On le note par $(K, A) \subseteq (L, B)$.*

Remarque 3.9 *Dans (iii), on peut remplacer $B \cap j(K) = j(A)$ par B domine $j(A)$. Les deux conditions sont équivalentes.*

Maintenant considérons K^{ac} une clôture algébrique de K.

Proposition 3.10 ([1, Corollaire 3.15 et 3.16]) *Soit A un anneau de valuation de K, alors il existe A^{ac} un anneau de valuation de K^{ac} qui domine A. De plus, pour toute extension de corps valué $(K, A) \to (L, B)$ avec L algébriquement clos, on peut l'étendre en une extension $(K^{ac}, A^{ac}) \to (L, B)$.*

Soit (K, A) un corps valué algébriquement clos, il y a des propriétés de k_A et Γ_A.

Proposition 3.11 *On garde les notations ce-dessus, alors k_A l'est aussi, et Γ_A est divisible.*

Preuve Fixons $u_0, \dots, u_n \in k_A$, on peut trouver $a_0, \dots, a_n \in A$ tels que $\overline{a_i} = u_i$ pour tout $i = 0, \dots, n$. K est algébriquement clos, donc il existe $x \in K$ tel que $x^{n+1} + a_n x^n + \cdots + a_0 = 0$. Si $x \notin A$, alors d'après la remarque 3.2(v), $v(x^{n+1} + a_n x^n + \cdots + a_0) = v(x^{n+1}) \neq \infty$, contradiction. Donc $x \in A$, et $\overline{x}$ est une racine de $X^{n+1} + u_n X^n + \cdots + u_0$, k_A est algébriquement clos.
Pour tout $v(t) = \gamma \in \Gamma$ et $n \geq 1$ avec $t \in K$, prenons $x \in K$ tel que $x^n = t$, alors $nv(t) = \gamma$. Donc Γ est divisible. □

Revenons au cas général. D'abord posons un lemme qui s'agit des degrés d'une extension :

Lemme 3.12 *Soit $(K, A) \subseteq (L, B)$ une extension de corps valué. Soient $b_1, \dots, b_p \in B$ tels que $\overline{b_1}, \dots, \overline{b_p}$ sont linéairement indépendents sur k_A, soient $c_1, \dots, c_q \in L^\times$ tels que $v(c_1), \dots, v(c_q)$ sont dans de différentes classes de Γ_B/Γ_A. Alors, pour tout $a_{ij} \in K$, $1 \leq i \leq p, 1 \leq j \leq q$, $v(\sum_{i,j} a_{ij} b_i c_j) = \min_{i,j}\{v(a_{ij}) + v(c_j)\}$. En particulier, les $b_i c_j$ sont linéairement indépendents sur K.*

Preuve D'abord fixons $(a_i)_i \in K^p \backslash \{0\}$ et montrons que $v(\sum_i a_i b_i) = \min_i\{v(a_i)\}$. Quitte à diviser les a_i par une constante non nulle, on peut supposer que pour tout $i, a_i \in A$ et qu'il existe $i, v(a_i) = 0$. Il suffit de montrer que $v(\sum_i a_i b_i) = 0$, et ça vient du fait que $\overline{\sum_i a_i b_i} = \sum_i \overline{a_i}\,\overline{b_i} \neq 0$. Maintenant considérons le cas général. Il suffit de traiter le cas où $a_{ij} \in K$ ne sont pas tous 0, quitte à supprimer j, on peut supposer que pour tout j, il existe i tel que $a_{ij} \neq 0$. Pour tout j fixé,

$$v(\sum_i a_{ij} b_i c_j) = v(\sum_i a_{ij} b_i) + v(c_j) = \min_i\{v(a_{ij})\} + v(c_j) \in \Gamma_A + v(c_j).$$

Donc par hypothèse sur les c_j, les $v(\sum_i a_{ij} b_i c_j)$ sont distincts, et donc

$$v(\sum_{i,j} a_{ij} b_i c_j) = v(\sum_j (\sum_i a_{ij} b_i c_j)) = \min_{i,j}\{v(a_{ij}) + v(c_j)\}.$$

□

Corollaire 3.13 *On garde les notations du lemme 3.11. Alors*

$$[L : K] \geq [k_B : k_A] \cdot [\Gamma_B : \Gamma_A].$$

Si L est une clôture algébrique de K, alors k_B est une clôture algébrique de k_A, Γ_B est une enveloppe divisible de Γ_A

Preuve Il se déroule en utilisant le lemme et la proposition ci-dessus. □

A l'aide du lemme précédent, démontrons les résultats suivants sur les extensions de corps valués.

Lemme 3.14 *Soit (K,A) un corps valué. Soit L=K(x) avec x transcendant sur K. Alors il existe un unique anneau de valuation B de L qui domine A, tel que $x \in B$, et $\overline{x}$ est transcendant sur k_A. Dans ce cas, $k_B = k_A(x)$ et $\Gamma_A = \Gamma_B$.*

Preuve **Unicité** : Posons B comme dans l'énoncé, pour tout $f_0, \dots, f_n \in K$, par le lemme 3.12, on a que $v_B(f_0 + \cdots + f_n x^n) = \min_i v_A(f_i)$. Donc v_B est unique sur $K[x]$, et donc v_B est aussi unique sur L.
Existence : On définit v_B sur $K[x]\backslash\{0\}$ par la formule ci-dessus. Et on peut vérifier (V1) et

(V2). Ensuite v_B s'étend uniquement en une valuation sur L.
Pour les autres proprétés, la seule propriété non triviale est que $k_B = k_A(\overline{x})$. Posons $b = \frac{f(x)}{g(x)} \in B$ avec f, $g \in K[x]\backslash\{0\}$ tels que $v_B(b) = 0$. Quitte à diviser f, g par une constante dans K, on peut supposer que $v(f) = v(g) = 0$. Alors $\overline{f}(\overline{x}) \neq 0$ et $\overline{g}(\overline{x}) \neq 0$. Donc dans k_B,

$$\overline{b} = \frac{\overline{f}(\overline{x})}{\overline{g}(\overline{x})} \in k_A(\overline{x}).$$

Le lemme suivant est similaire.

Lemme 3.15 ([1, Lemme 3.23]) *Soit (K,A) un corps valué avec v la valuation. Posons L=K(x) avec x transcendant sur K. Soit δ dans un groupe abélien ordonné qui prolonge Γ tel que $n\delta \notin \Gamma$ pour tout $n \geq 1$. Alors v s'étend uniquement en une valuation $w : L^\times \to \Gamma + \mathbb{Z}\delta$ telle que $w(x) = \delta$. Dans ce cas, $k_v = k_w$.*

On énonce aussi le lemme suivant pour la preuve du théorème 3.19.

Lemme 3.16 ([1, Lemme 3.30]) *Soit $(K, A) \subseteq (L, B)$ une extension de corps valués telle que $k_A = k_B$. Posons $n \geq 1$, $a_1, \ldots, a_n \in K$ et $x \in L$ tels que $v(x - a_i) \in v(K^\times)$, pour tous $i = 1, \ldots, n$. Alors il existe $a \in K$ tel que $v(x - a_i) = v(a - a_i)$, pour tous $i = 1, \ldots, n$.*

3.3 Corps valués algébriquement clos

D'abord traduisons la valuation en termes de relation binaire.

Définition 3.17 *Une **divisibilité de valuation** sur un anneau intègre est une relation binaire $|$ sur R telle que $\forall x, y, z \in R$*
(VD1) On n'a pas $0 \mid 1$;
(VD2) Si $x \mid y$ et $y \mid z$ alors $x \mid z$;
(VD3) Si $x \mid y$ et $x \mid z$ alors $x \mid y + z$;
(VD4) $x \mid y$ si et seulement si $xz \mid yz$ pour $z \neq 0$;
(VD5) $x \mid y$ ou $y \mid x$.

Pour un anneau de valuation A de K, on peut identifier v_A et $|_A$ par

$$x \mid_A y \iff v_A(x) \leq v_A(y).$$

Cela nous donne en fait ([1, Lemme 3.27]) une bijection entre les divisibilités de valuations de K et les anneaux de valuations de K.

Définition 3.18 *(i) Posons $L_{val} = \{0, 1, +, -, \cdot, |\}$, on note ACF_{val} la théorie dans ce langage dont les modèles sont $(K, |)$ avec $K \models ACF$ où ACF est la théorie des corps algébriquement clos, et $|$ est une divisibilité de valuation non triviale (i.e. l'anneau de valuation associé n'est pas K).*
*(ii) Soient L un language, $\mathcal{M}$ une structure de L et $n \geq 1$. Posons A un ensemble et $L_A = L \cup \{c_a\}_{a \in A}$, ici les c_a n'appartiennent pas à L. Un **n-type** sur A est un ensemble des formule $X = \{\phi(x_1, \ldots, x_n)\}$ dans L_A tel que pour tout Y sous-ensemble fini de X, il existe $b \in M^n$ tel que $\mathcal{M} \models \phi(b)$ pour tout $\phi \in Y$. Un **type complet** est un n-type qui est maximal par l'inclusion. On dit que $\mathcal{M}$ **réalise un n-type** X s'il existe $b \in M^n$ tel que $\mathcal{M} \models \phi(b)$ pour tout $\phi \in X$.*
*(iii) Soient κ une cardinalité, L un language et $\mathcal{M}$ une structure de L. On dit que $\mathcal{M}$ est **κ^+-saturé** si pour tout ensemble A de cardinalité inférieur ou égal à κ, $\mathcal{M}$ réalise tous les types complets de A.*

Théorème 3.19 ([1, Théorème 3.29]) *La théorie ACF_{val} élimine les quantificateurs.*

Preuve (esquisse) On va utiliser un test de EQ (élimination des quantificateurs) dans [2, Proposition 4.3.28]. Pour une théorie T, les deux assertions suivantes sont équivalentes :
(i) T a EQ ;
(ii) Pour tous modèles $\mathcal{M}$, $\mathcal{N}$ de T où $\mathcal{N}$ est $|\mathcal{M}|^+$-*saturé*, posons $\mathcal{A}$ une sous-structure propre de $\mathcal{M}$ et $j : \mathcal{A} \to \mathcal{N}$ un prolongement. On peut étendre $\mathcal{A}$ en un prolongement $j : \mathcal{A}' \to \mathcal{N}$ où $\mathcal{A}'$ est une sous-structure de $\mathcal{M}$ qui prolonge proprement $\mathcal{A}$.
Soient (E, A), $(F, B) \models ACF_{val}$ tels que (F, B) est $|E|^+$-*saturé*. Soit $\mathcal{A}$ une sous-structure de (E, A) et $i : \mathcal{A} \to (F, B)$ un prolongement. D'après la proposition 3.10 on peut supposer que $\mathcal{A} = (K, A)$ est un corps valué avec $K = K^{ac}$, et on trouvera un $x \in E \backslash K$ tel que i s'étend en un prolongement $j : (K(x), A \cap K(x)) \to (F, B)$.
Cas 1 : $k_{A\cap K} \neq k_A$. On prend $x \in A$ tel que $\overline{x} \notin k_{A\cap K}$. Par saturation, on peut trouver un $y \in B$ tel que $\overline{y} \notin k_{B\cap iK}$. Alors par le lemme 3.14, le morphisme $j : K(x) \to (iK)(y)$ est un isomorphisme de corps valués.
Cas 2 : $v(K^\times) \neq v(E^\times)$. Prenons $\gamma \in v(E^\times) \backslash v(K^\times)$. Par saturation, il existe $\delta \in v(F^\times) \backslash v(i(K^\times))$ tel que pour tout $a \in K^\times$,

$$\gamma < v(a) \text{ si et seulement si } \delta < v(i(a)).$$

Soit $x \in E^\times$, $y \in F^\times$ telles que $v(x) = \gamma$, $v(y) = \delta$. En utilisant le lemme 3.15, on peut obtenir un isomorphisme de corps valués

$$(K(x), A \cap K(x)) \xrightarrow{\sim} ((iK)(y), B \cap (iK)(y)) \subseteq (F, B).$$

Cas 3 : $k_{A\cap K} = k_A$ et $v(K^\times) = v(E^\times)$, on les note par Γ. Pour simplifier les notations, on note toujours les valuations par v. Soit $x \in E \backslash K$. Une valuation $v|_{K(x)} : K(x) \to \Gamma_\infty$ est totalement déterminée par $v|_K$ et l'application $a \mapsto v(x-a) : K \to \Gamma$, comme K est algébriquement clos. Par le lemme 3.16 et l'hypothèse de saturation, on peut trouver $y \in F \backslash iK$ tel que $v(x-a) = v(y-a)$ pour tout $a \in K$. Enfin on peut construire un isomorphime de corps valués

$$(K(x), A \cap K(x)) \xrightarrow{\sim} ((iK)(y), B \cap (iK)(y)) \subseteq (F, B).$$

4 Extensions immédiates

Dans cette section, on étudie certaines extensions particulières de corps valué : les extensions immédiates. On considère aussi comment la notion d'hensélianité interagit avec ces extensions. Dans cette section, on fixe $(K, \Gamma; v)$ un corps valué.

4.1 Pseudoconvergence

Dans cette partie, on introduit la pseudoconvergence. Elle nous fournit des caractérisations pour des extensions immédiates, qui seront également introduites plus tard.

Définition 4.1 *(i) Une suite $\{a_\rho\}$ dans K est **bien-indexée** dans K si $\{a_\rho\}$ est indexée par un ensemble infini bien ordonné qui n'a pas d'élément maximal. On dit que $\{a_\rho\}$ **pseudoconverge** vers $a \in K$ si $\{v(a - a_\rho)\}$ est strictement croissante à partir d'un certain rang (ou simplement pour $\rho \gg 1$). On note la pseudoconvergence par $a_\rho \rightsquigarrow a$.*
*(ii) Une extension $(K', \Gamma'; v')$ de $(K, \Gamma; v)$ est dite **immédiate** si $\Gamma' = \Gamma$ et $k_v = k_{v'}$.*

Pour une suite $a_\rho \rightsquigarrow a$ dans K, la limite n'est pas toujours unique, mais il y a des propriétés de $\{a_\rho\}$ associé à la limite :

Proposition 4.2 ([1, Lemme 4.1]) *Soit $a_\rho \rightsquigarrow a$ dans K, et on note $\gamma_\rho = v(a - a_\rho)$, alors*
(i) pour tout $b \in K$, $a_\rho \rightsquigarrow b$ si et seulement si $v(a-b) > \gamma_\rho$ pour $\rho \gg 1$;
(ii) soit $v(a_\rho) < v(a)$ pour $\rho \gg 1$, dans ce cas $\{v(a_\rho)\}$ est strictement croissante pour $\rho \gg 1$; soit $v(a_\rho) = v(a)$ pour $\rho \gg 1$, dans ce cas $\{v(a_\rho)\}$ est constant pour $\rho \gg 1$.

Proposition 4.3 ([1, Lemme 4.2]) *Soit $(K', \Gamma'; v')$ une extension immédiate de $(K, \Gamma; v)$ et prenons $a' \in K' \backslash K$. Alors il existe $\{a_\rho\}$ bien-indexée tel que $a_\rho \rightsquigarrow a'$ et $\{a_\rho\}$ n'a pas de pseudolimite dans K.*

Maintenant posons la définition d'une suite de pseudoCauchy :

Définition 4.4 *Une suite $\{a_\rho\}$ est une **suite de pseudoCauchy (pc-suite)** dans K si elle bien-indexée et qu'il existe un ρ_0 tel que*

$$\text{Pour tous } \tau > \sigma > \rho > \rho_0,\ v(a_\tau - a_\sigma) > v(a_\sigma - a_\rho).$$

Le lemme suivant nous donne un lien entre cette notion et la pseudoconvergence.

Lemme 4.5 ([1, Lemme 4.3]) *Soit $\{a_\rho\}$ une suite bien-indexée dans K. Alors $\{a_\rho\}$ est une pc-suite dans K ssi $\{a_\rho\}$ a une pseudolimite dans une extension de $(K, \Gamma; v)$. Dans ce cas, $\{a_\rho\}$ peut avoir une pseudolimite dans une extension élémentaire de $(K, \Gamma; v)$.*

En particulier, par ce lemme, on peut utiliser la proposition 4.2, et on en déduit que pour une pc-suite $\{a_\rho\}$ dans K, $\{v(a_\rho)\}$ est soit strictement croissante pour $\rho \gg 1$, soit constante pour $\rho \gg 1$. En fait, les polynômes préservent bien la pseudoconvergence ([1, Proposition 4.7]) :

Proposition 4.6 *Soit $\{a_\rho\}$ une suite bien indexée dans K telle que $a_\rho \rightsquigarrow a \in K$, soit $f \in K[x] \backslash K$, alors $f(a_\rho) \rightsquigarrow f(a)$.*

En combinaisant le lemme précédent, on en déduit un corollaire :

Corollaire 4.7 *Soient $\{a_\rho\}$ une pc-suite dans K et $f \in K[x]$ un polynôme non constant. Alors $\{f(a_\rho)\}$ est une pc-suite.*

Rappelons que dans la proposition 4.2, les pc-suites sont réparties en 2 cas. Et considérons les compositions par les polynômes. Soit $\{a_\rho\}$ une pc-suite dans K et soit $f \in K[x]$. Alors il n'y a que 2 cas :
(1) Soit $\{v(f(a_\rho))\}$ est strictement croissante pour $\rho \gg 1$;
(2) Soit $\{v(f(a_\rho))\}$ est constant pour $\rho \gg 1$.
Notons que si f est constant, il vérifie le cas (2).

Définition 4.8 *On dit que $\{a_\rho\}$ est*
*(i) de **type algébrique** s'il existe $f \in K[x]$ qui vérifie (1). Dans ce cas, un **polynôme minimal** de $\{a_\rho\}$ sur K est un polynôme de degré minimal qui vérifie (1).*
*(ii) de **type transcendant** si pour tout $f \in K[x]$, f vérifie la condition (2).*

Remarque 4.9 *Un polynôme minimal de $\{a_\rho\}$ (s'il existe) n'est pas unique même si on suppose de plus qu'il soit unitaire.*

Maintenant introduisons deux théorèmes pour les extensions immédiates.

Théorème 4.10 *Soit $\{a_\rho\}$ une pc-suite dans K de type transcendant. Alors $\{a_\rho\}$ n'a pas de pseudolimite dans K. La valuation v s'étend uniquement en une valuation $v : K(x)^\times \to \Gamma$ (x transcendant sur K)*

$$v(f) = v(f(a_\rho)) \text{ pour } \rho \text{ suffisamment grand}$$

pour tout $f \in K[x]$. Et cela fait $(K(x), \Gamma; v)$ d'une extension immédiate de $(K, \Gamma; v)$ dans laquelle $a_\rho \rightsquigarrow x$.
Réciproquement, si $a_\rho \rightsquigarrow a$ dans une extension de $(K, \Gamma; v)$, alors il existe un isomorphisme de corps valués $K(x) \to K(a)$ sur K qui envoie x sur a.

Preuve (esquisse) Si $a_\rho \rightsquigarrow a \in K$, alors $f = x - a$ vérifie (1), cela contredit que $\{a_\rho\}$ est de type transcendant. Ensuite, on peut vérifier directement que v est bien définie sur $K(x)^\times$ et est une valuation sur $K(x)$. Par définition, $\Gamma = v(K(x)^\times)$. Montrons que $k_v = k_{\overline{v}}$: Soit $a = f/g$ avec $v(a) = 0$ et $f, g \in K[x]$. Quitte à diviser une constante dans K, on suppose que $v(f) = v(g) = 0$. Comme $0 = v(f) = v(f(a_\rho))$ pour $\rho \gg 1$, et d'après la proposition 4.6, $\{v(f - f(a_\rho))\}$ est strictement croissante pour $\rho \gg 1$, donc $v(f - f(a_\rho)) > 0$ pour $\rho \gg 1$. Prenons un tel ρ, alors $f = f - f(a_\rho) + f(a_\rho)$, donc $\overline{f} = \overline{f(a_\rho)}$. De même pour g, enfin $\overline{a} \in k_v$.
Posons $a_\rho \rightsquigarrow a$ avec a dans une extension de $(K, \Gamma; v)$. Alors $\forall f \in K[x]$, $f(a_\rho) \rightsquigarrow f(a)$. D'après la proposition 4.2 et l'hypothèse de $\{a_\rho\}$, $v(f(a_\rho)) = v(f(a))$ pour $\rho \gg 1$, donc $f(a) \neq 0$, et $v(f(a)) = v(f) \in \Gamma$. Donc on peut construire un isomorphime comme dans l'énoncé.

Il y a aussi un théorème parallèle pour le cas algébrique. Vous trouverez une preuve dans ([1, Théorème 4.10]).

Théorème 4.11 *Soit $\{a_\rho\}$ une pc-suite dans K de type algébrique telle qu'elle n'a pas de pseudolimite dans K. Soit μ un polynôme minimal de $\{a_\rho\}$ sur K. Alors μ est irréductible et* deg $\mu \geq 2$. *Soit a une racine de μ dans une extension de corps de K. Alors v s'étend uniquement en une valuation $v : K(a)^\times \to \Gamma$*

$$v(f(a)) = v(f(a_\rho)) \text{ pour } \rho \text{ suffisamment grand}$$

pour tout $f \in K[x]$ de degré strictement inférieur à deg μ. Et cela fait $(K(a), \Gamma; v)$ d'une extension immédiate de $(K, \Gamma; v)$ dans laquelle $a_\rho \rightsquigarrow a$.
Réciproquement, si $\mu(b) = 0$ et $a_\rho \rightsquigarrow b$ dans une extension de $(K, \Gamma; v)$, alors il existe un isomorphisme de corps valué $K(a) \to K(b)$ qui envoie a sur b.

4.2 Corps valués maximaux et algébriquement maximaux

Comme indiqué dans le titre, on étudie dans cette partie les corps valués maximaux et algébriquement maximaux dont on donne aussi des caractérisations alternatives. D'abord on donne les définitions :

Définition 4.12 *Soit $(K, \Gamma; v)$ un corps valué. On dit qu'il est*
(i) ***maximal*** *si toute extension immédiate de $(K, \Gamma; v)$ est triviale.*
(ii) ***algébriquement maximal*** *si toute extension immédiate algébrique de $(K, \Gamma; v)$ est triviale.*

Remarque 4.13 *Étant donné un corps valué, il découle du lemme de Zorn et de la proposition 3.6 que (K, v) admet une extension immédiate qui est maximale (resp. algébriquement maximale et algébrique sur K).*

D'abord traitons les corps valués maximaux. En combinaisant les théorèmes 4.10, 4.11 et la proposition 4.3, on en déduit le théorème suivant :

Théorème 4.14 *Un corps valué $(K, \Gamma; v)$ est maximal ssi toute pc-suite dans K a une pseudo-limite dans K.*

Pour les corps valués algébriquement maximaux, il y a deux caractérisations, l'un des deux est le suivant :

Théorème 4.15 ([1, Corollaire 4.16]) *Un corps valué $(K, \Gamma; v)$ est algébriquement maximal ssi toute pc-suite de type algébrique dans K a une pseudolimite dans K.*

Pour l'autre caractérisation, on a un lien entre l'hensélianité et la maximalité algébrique.

Définition 4.16 *(i) On dit que $(K, \Gamma; v)$ est équicaractéristique 0 (ou simplement de caractéristique (0,0)) si les caractéristiques de K et k_v sont 0.*
*(ii) On dit que $(K, \Gamma; v)$ est **hensélien** si $\mathcal{O}_v$ est un anneau hensélien. On dit qu'une extension $(K', \Gamma'; v')$ de $(K, \Gamma; v)$ est hensélienne si $(K', \Gamma'; v')$ est hensélien.*

Théorème 4.17 ([1, Corollaire 4.22]) *Soit $(K, \Gamma; v)$ algébriquement maximal, alors il est hensélien. S'il est de caractéristique (0,0), alors la réciproque est vraie.*

4.3 Unicité

Maintenant, considérons l'unicité de ces extensions immédiates. Dans le cas de caractéristique (0,0), on a l'unicité des extensions immédiates maximales (resp. immédiates algébriques et algébriquement maximales).

Définition 4.18 *Une **hensélisation** de $(K, \Gamma; v)$ est une extension hensélienne $(K^h, \Gamma^h; v^h)$ telle que pour toute extension*

$$(K, \Gamma; v) \to (K', \Gamma', v')$$

où $(K', \Gamma'; v')$ est hensélien, on peut l'étendre uniquement en une extension

$$(K^h, \Gamma^h; v^h) \to (K', \Gamma', v').$$

Remarque 4.19 *Par définition, une hensélisation (s'elle existe) est unique à unique isomorphisme sur $(K, \Gamma; v)$ près.*

À l'aide du corps valué construit dans la proposition 4.13, on peut déduire le corollaire ci-dessous :

Corollaire 4.20 *Toute hensélisation de (K, Γ, v) est une extension immédiate et est algébrique sur K.*

Ensuite, le théorème suivant nous donne la "réciproque".

Théorème 4.21 ([1, Théorème 4.27]) *Soit $(K, \Gamma; v)$ de caractéristique (0,0) et $(K_1, \Gamma_1; v_1)$ une extension immédiate hensélienne de $(K, \Gamma; v)$ telle que K_1/K est algébrique. Alors $(K_1, \Gamma_1; v_1)$ est une hensélisation de $(K, \Gamma; v)$. En particulier, pour le cas de caractéristique (0,0), il existe une unique (à unique isomorphime près) hensélisation de $(K, \Gamma; v)$.*

Pour la maximalité, dans le cas de caractéristique (0,0), voici un résultat similaire ([1, Corollaire 4.29]).

Théorème 4.22 *Soit $(K, \Gamma; v)$ de caractéristique (0,0). Alors toutes deux extensions immédiates maximales de $(K, \Gamma; v)$ sont isomorphes sur $(K, \Gamma; v)$.*

Vous trouverez une version générale de la proposition suivante dans [1, Proposition 4.21].

Proposition 4.23 *Soient $(K,\Gamma;v)$ de caractéristique (0,0), $\{a_\rho\}$ une pc-suite de type algébrique dans K et f un polynôme minimal de $\{a_\rho\}$. Alors pour tout extension hensélienne $(K',\Gamma';v')$ de $(K,\Gamma;v)$, il existe un unique $b\in K'$ tel que $f(b)=0$ et $a_\rho \rightsquigarrow b$.*

Le lemme suivant est utile dans la preuve du théorème de AKE.

Lemme 4.24 *Soit $(K,\Gamma;v)$ non trivial de caractéristique (0,0) et $(K^*,\Gamma;v^*)$ une extension immédiate maximale de $(K,\Gamma;v)$. Alors pour toute extension hensélienne $|\Gamma|^+$-saturée $(K',\Gamma';v')$ de $(K,\Gamma;v)$, on peut prolonger $(K^*,\Gamma;v^*)$ dans $(K',\Gamma';v')$ sur $(K,\Gamma;v)$.*

Preuve Par le théorème précédent, il suffit de trouver un corps valué maximal $(K_1,\Gamma;v_1)$ tel que $(K,\Gamma;v)\subseteq(K_1,\Gamma;v_1)\subseteq(K',\Gamma';v')$ et $k_{v_1}=k_v$. Par le lemme de Zorn, il existe une extension immédiate de $(K,\Gamma;v)$ dans $(K',\Gamma';v')$ qui est maximale pour l'inclusion dans l'ensemble des extensions immédiates de $(K,\Gamma;v)$ dans $(K',\Gamma';v')$. Notons cette extension par $(K_1,\Gamma;v_1)$ et montrons qu'elle convient. D'après le théorème 4.14, on fixe $\{a_\rho\}$ une pc-suite dans $(K_1,\Gamma;v_1)$ sans pseudolimite dans K_1, et on déduit une contradiction.
(i) $\{a_\rho\}$ est de type algébrique. D'après la proposition 4.23 et le théorème 4.10, on peut trouver $a\in K'$ tel que $a_\rho\rightsquigarrow a$ et $(K_1(a),\Gamma;v'|_{K(a)})$ est une extension immédiate de $(K,\Gamma;v)$, cela contredit l'hypothèse de $(K_1,\Gamma;v_1)$.
(ii) $\{a_\rho\}$ est de type transcendant. Pour $\rho\gg 1$ (suivant on garde cette hypothèse), $\gamma_\rho=v(a_\sigma-a_\rho),\sigma>\rho$ est bien défini et ne dépend pas du choix de $\sigma>\rho$. Comme γ_ρ est strictement croissant, $|\{\gamma_\rho\}_\rho|\leq|\Gamma|$. Pour tout ρ, soient c_{γ_ρ} et c_{a_ρ} deux symboles constants qui correspondent à $a_\sigma-a_\rho$ (fixons un $\sigma>\rho$ pour chaque ρ) et a_ρ respectivement. Alors $\{v(x-c_{a_\rho})=v(c_{\gamma_\rho})\}$ est un 1-type sur un ensemble de cardinalité inférieur ou égal à $|\Gamma\times\Gamma|$. Comme Γ est non trivial, soit $x\in\Gamma\backslash\{0\}$, alors $\{nx,n\in\mathbb{N}\}$ est de cardinalité $\mathbb{N}$. Donc $|\Gamma\times\Gamma|=|\Gamma|$. Par saturation, il existe un $b\in K'$ qui satisfait les formules ci-dessus. Donc par le théorème 4.11, $(K_1(b),\Gamma;v'|_{K_1(b)})$ est une extension immédiate de $(K,\Gamma;v)$, cela contredit l'hypothèse de $(K_1,\Gamma;v_1)$. □

À la fin de la section, on donne deux notions pour étudier le lien entre k_v,Γ et K.

Définition 4.25 *(i) Un **relèvement** de k est un morphisme de corps $i:k_v\to\mathcal{O}_v$ tel que $\overline{i(a)}=a$ pour tout $a\in k_v$.*
*(ii) Une **$\times$-section** de v est un morphime de groupe $s:\Gamma\to K^\times$ tel que $v\circ s=id_\Gamma$.*

Remarque 4.26 *D'après le théorème 2.18, tout corps valué hensélien de caractéristique (0,0) admet un relèvement.*

5 Le théorème de Ax-Kochen et Ershov

Dans cette section, on combine les préliminaires qu'on a introduit, et on introduit une démonstration du théorème 1.2 dans l'introduction.

5.1 Préliminaires

Comme les corps valués sont henséliens, on peut toujours prendre des relèvements. Et on va construire une $\times$-section dans une extension élémentaire. Dans cette partie, on fixe un corps valué $(K,\Gamma;v)$.

Définition 5.1 *Une $\times$-section partielle est un morphisme de groupe $s:\Delta\to K^\times$ tel que $v\circ s=id_\Delta$, où Δ est un sous-groupe de Γ.*
On dit qu'un sous-groupe d'un groupe abélien est pure si le groupe quotient est sans torsion.

Proposition 5.2 *Il existe une extension élémentaire de $(K, \Gamma; v)$ qui a une $\times$-section.*

Preuve Étape 1 : Supposons qu'on a une $\times$-section partielle $s : \Delta \to K^\times$ avec Δ pure dans Γ. Posons Δ' un sous-groupe de Γ qui contient Δ et Δ'/Δ est de type fini. Alors par pureté de Δ, on peut prendre une $\mathbb{Z}$-base $\{\gamma_i, 1 \leq i \leq k\}$ telle que

$$\Delta' = \Delta \oplus \mathbb{Z}\gamma_1 \oplus \cdots \oplus \mathbb{Z}\gamma_k.$$

Donc on peut directement prolonger s sur Δ'. Ensuite par compacité de la logique propositionnelle, on peut trouver une extension éléementaire $(K_1, \Gamma_1; v_1)$ de $(K, \Gamma; v)$ avec $s : \Gamma \to K_1$ une $\times$-section.
Étape 2 : Comme $\Gamma \preccurlyeq \Gamma_1$, il est pure dans Γ_1. En effet, pour tout $n \geq 1$, on considère la formule $nx = y$. S'il existe $x \in \Gamma_1$ et $y \in \Gamma$ tels que $nx = y$, alors il existe $x' \in \Gamma$ tel que $nx = y$ car $\Gamma \preccurlyeq \Gamma_1$, et donc $x = x'$. Donc on peut itérer étape 1 pour obtenir :

$$(K, \Gamma; v) \preccurlyeq (K_1, \Gamma_1; v_1) \preccurlyeq (K_2, \Gamma_2; v_2) \preccurlyeq \ldots$$

avec $s_n : \Delta_n \to K_n^\times$ où $\Delta_0 = 0$, $\Delta_{n+1} = \Gamma_n$ et s_{n+1} prolonge s_n. Enfin $(K', \Gamma'; v') = \cup_n (K_n, \Gamma_n; v_n)$ convient avec $s' = \cup_n s_n$.

Maintenant posons deux lemmes utiles dans la démonstration suivante ([1, Lemme 5.6, Corollaire 5.9]).

Lemme 5.3 *Soit p un nombre premier, et x un élément dans une extension de corps de K telle que $x^p = a \in K^\times$ mais $v(a) \notin p\Gamma$. Alors $X^p - a$ est le polynôme minimal de x sur K, et v s'étend uniquement en une valuation $w : K(x)^\times \to \Delta$ avec $\Delta \subseteq \mathbb{Q}\Gamma \overset{def}{=} \mathbb{Q} \otimes_{\mathbb{Z}} \Gamma$. Dans ce cas, $k_w = k_v$ et $[\Delta : \Gamma] = p$, avec*

$$\Delta = \sqcup_{i=0}^{p-1} (\Gamma + iw(x)).$$

Lemme 5.4 *Soit $(K', \Gamma'; v')$ une extension de $(K, \Gamma; v)$, et $x \in K' \backslash K$. Si $\Gamma = v(K^\times)$ est dénombrable, alors $v'(K(x)^\times)$ l'est aussi.*

5.2 La démonstration du théorème de AKE

Maintenant introduisons une version plus forte du théorème de AKE.

Définition 5.5 *Un corps rc-valué est une 3-sortes structure*

$$\mathcal{K} = (K, k, \Gamma; \pi, v, i, s)$$

où $\pi : \mathcal{O}_v \to k_v$ la projection canonique, $i : k \to \mathcal{O}_v$ morphisme d'anneaux tels que $\pi \circ i = id_k$, $s : \Gamma \to K^\times$ une $\times -$ section de v.

Par le théorème 2.18 et la proposition 5.2, on en déduit directement que tout corps valué hensélien de caractéristique (0,0) admet une extension élémentaire qui peut être vue comme un corps rs-valué. Donc suivant pour la réciproque du théorème de AKE, on peut remplacer les corps originaux par ses extensions élémentaires comme ci-dessus.

Définition 5.6 *Soit $\mathcal{K} = (K, k, \Gamma; \pi, v, i, s)$, $\mathcal{K}' = (K', k', \Gamma'; \pi', v', i', s')$ deux corps rc-valués. Un **prolongement** $\mathcal{K} \to \mathcal{K}'$ est la donnée (f, f_v, f_v) où $f : K \to K', f_r : k \to k'$ des morphismes de corps, $f_v : \Gamma \to \Gamma'$ un prolongement de groupes ordonnés, tels que*

$$f_r \circ \pi = \pi' \circ f \text{ sur } \mathcal{O}_v, \quad f \circ i = i' \circ f_r \text{ sur } k$$

$$f_v \circ v = v' \circ f \text{ sur } K^\times, \quad f \circ s = s' \circ f_v \text{ sur } \Gamma.$$

Maintenant on va montrer une version plus forte :

Théorème 5.7 *Soient $\mathcal{K}, \mathcal{K}'$ deux corps rs-valués henséliens (0,0). Alors*

$$\mathcal{K} \equiv \mathcal{K}' \iff k \equiv k' \text{ et } \Gamma \equiv \Gamma'.$$

Preuve Dans son livre [1], Van der Dries suppose l'hypothèse du continue pour cette preuve, il en explique les raisons après le corollaire 5.15.
Le sens direct $\Rightarrow$ est immédiat (c'est le même principe que dans la preuve du théorème 5.13), supposons donc que $k \equiv k'$ et $\Gamma \equiv \Gamma'$. Si $\Gamma = \{0\}$, on a $K = k$ ce qui conclut, on peut donc supposer que $\Gamma \neq \{0\}$ (et donc $\Gamma' \neq \{0\}$).

D'après [1] quitte à remplacer $\mathcal{K}$ et $\mathcal{K}'$ par des corps rs-valués henséliens de caractéristique résiduelle nulle équivalents, on peut supposer que $\mathcal{K}$ et $\mathcal{K}'$ sont saturés de cardinalités $\aleph_1$.
Alors k et k' sont saturés de cardinalités $\aleph_1$, comme ils sont élémentairements équivalents, il existe un isomorphisme de corps $f_r : k \to k'$ (d'après le théorème 4.3.20 du livre de David Marker[2]). Il existe de même un isomorphisme de groupes abéliens ordonnés $f_v : \Gamma \to \Gamma'$. On cherche à construire un isomorphisme de corps $f : K \to K'$ qui associé à f_r et f_v donne un isomorphisme $(f, f_r, f_v) : \mathcal{K} \to \mathcal{K}'$.
On va construire f par une méthode de va-et-vient. On dit qu'un sous-corps E de K est un bon sous-corps de K si $i(k) \subseteq E$, $s(v(E^\times)) \subseteq E$ et $v(E^\times)$ est dénombrable. On dit qu'un isomorphisme $f : E \to E'$ est un bon morphisme si E et E' sont des bons sous-corps de K et K' et que

- $e(E \cap \mathcal{O}_v) = E' \cap \mathcal{O}_{v'}$
- $f_r(\pi(a)) = \pi'(e(a))$ pour tout $a \in E \cap \mathcal{O}_v$
- $f_v(v(a)) = v'(e(a))$ pour tout $a \in E^\times$
- $e(i(r)) = i'(f_r(r))$ pour tout $r \in k$
- $e(s(\gamma)) = s'(f_v(\gamma))$ pour tout $\gamma \in v(E^\times)$

Par exemple, $\begin{array}{ccc} i(k) & \to & i'(k') \\ i(r) & \mapsto & i'(f_r(r)) \end{array}$ est un bon morphisme.
Montrons que l'ensemble des bons morphismes a la propriété du va-et-vient.
Soit $e : E \to E'$ un bon morphisme. Comme E et E' sont des sous-corps valués de $(K, \mathcal{O}_v)$ et $(K', \mathcal{O}_{v'})$, e est un morphisme de corps valués. Montrons d'abord deux façons de prolonger e.

1. A l'aide d'un élément de Γ qui possède une torsion première modulo $v(E^\times)$
   Soit $\delta \in \Gamma$ tel que $\delta \notin v(E^\times)$ et $p\delta \in v(E^\times)$ avec p premier. Posons $x = s(\delta)$, alors $x^p = s(p\delta) \in E^\times$. Ainsi, d'après le lemme 5.3 :
   $$v(E(x)^\times) = v(E^\times) \oplus \mathbb{Z}\delta$$
   Donc $s(v(E(x)^\times)) \subseteq E(x)^\times$ et $E(x)$ est un bon sous-corps de K. Posons $x' = s'(f_v(\delta))$, alors de même $E'(x')$ est un bon sous-corps de K' et d'après le lemme 5.3 il existe un bon morphisme $E(x) \to E'(x')$ qui étend e et envoie x sur x'.
2. A l'aide d'un élément de Γ sans torsion modulo $v(E^\times)$
   Soit $\gamma \in \Gamma$ tel que $n\gamma \notin v(E^\times)$ pout tout $n \geq 1$. Posons $x = s(\gamma)$, alors d'après le corollaire 3.13 et le lemme 3.14, x est transcendant sur E et $v(E(x)^\times) = v(E^\times) \oplus \mathbb{Z}\gamma$. Donc $s(v(E(x)^\times)) \subseteq E(x)^\times$ et $E(x)$ est un bon sous-corps de K. Posons $x' = s'(f_v(\gamma))$, alors de même $E'(x')$ est un bon sous-corps de K' et x' est transcendant sur E', donc d'après le lemme 3.14 il existe un bon morphisme $E(x) \to E'(x')$ qui étend e et envoie x sur x'.

Montrons aussi que pour tout sous-groupe Δ de Γ dénombrable contenant $v(E^\times)$, e peut être étendu en un bon morphisme dont le domaine à pour groupe de valuations Δ. Pour cela on construit une suite croissante (Δ_k) de sous-groupe telle que $\Delta_0 = v(E^\times)$ et pour tout $k \in \mathbb{N}$:

— Soit $\Delta_{k+1} = \Delta_k$
— ou $\Delta_{k+1} = \Delta_k + \mathbb{Z}\delta_k$ avec $\delta_k \in \Delta \setminus \Delta_k$ et $p\delta_k \in \Delta_k$ avec p premier
— ou $\Delta_{k+1} = \Delta_k + \mathbb{Z}\delta_k$ avec $\delta_k \in \Delta \setminus \Delta_k$ et $n\delta_k \notin \Delta_k$ pour tout $n \geq 1$

Pour que l'union de ces sous-groupes soit égale à Δ, il suffi de prendre choisir les (δ_k) comme la suite de tous les éléments de $\Delta \setminus v(E^\times)$ qui est au plus dénombrable. Alors en appliquant les points 1 et 2 vus précédemment et en prenant l'union des corps, on trouve un bon sous-corps E_Δ tel que $v(E_\Delta^\times) = \Delta$, de plus e peut être étendu en un bon morphisme de domaine E_Δ.

Montrons maintenant la propriété de va-et-vient, soit $x \in K$, alors $v(E(x)^\times)$ est dénombrable d'après le lemme 5.4 et contient $v(E^\times)$, il existe donc un bon morphisme e_1 qui étend e de domaine E_1 tel que $v(E(x)^\times) = v(E_1^\times)$. Par itération de ce procédé puis en faisant une union, on obtient un corps que l'on nomme encore E qui vérifie $v(E^\times) = v(E(x)^\times)$. Alors le corps valué $E(x)$ est une extension immédiate de E.

D'après le lemme 4.24, il existe une extension immédiate maximale $E_\bullet$ de $E(x)$ dans $(K, \Gamma; v)$, et on a de même une extension immédiate $E'_\bullet$ de E'.Alors d'après le théorème 4.22, comme E et E' sont isomorphes, les extensions $E_\bullet$ et $E'_\bullet$ sont isomorphes sur E. Donc comme $e(K)$ est la version de K dans $E'_\bullet$, cet isomorphisme de corps valués étend e et x et dans son domaine, ce qui montre la partie **va** de la méthode va-et-vient.
La partie **vient** se montre de manière analogue. Ainsi, en appliquant le lemme de Zorn, on trouve un isomorphisme entre $\mathcal{K}$ et $\mathcal{K}'$, qui sont donc élémentairements équivalents.

5.3 Le Principe d'Ax,Kochen et Ershov

Dans cette dernière sous-section on montre le principe d'Ax, Kochen et Ershov. Pour cela on montre d'abord deux résultats généraux sur les algèbres de Boole qui permettront, à l'aide du théorème d'AKE, de montrer que tout énoncé dans le language des corps valués est équivalente dans la théorie des corps henséliens de caractéristique résiduelle nulle à un énoncé dans l'union du language des anneaux et du language des groupes ordonnés. Le théorème de compacité de la logique du premier ordre permettra alors d'en déduire le principe d'Ax, Kochen et Ershov.

Lemme 5.8 *Soient B une algèbre de Boole et A et A' des sous-algèbres de Boole de B. Alors la sous-algèbre de Boole engendrée par $A \cup A'$ est égale à*

$$\{(a_1 \wedge a'_1) \vee \cdots (a_k \wedge a'_k) \ : \ k \in \mathbb{N},\ a_1, \ldots, a_k \in A,\ a'_1, \ldots, a'_k \in A'\} \quad .$$

Preuve Il suffit de vérifier que l'ensemble proposé est une sous-algèbre de Boole contenant $A \cup A'$ et qu'il est inclus dans toute sous-algèbre de Boole contenant $A \cup A'$.

Lemme 5.9 *Soit B une algèbre de Boole, notons $S(B)$ l'espace de Stone de ses ultrafiltres. Soit*

Ψ une partie de B telle que la fonction $\begin{array}{ccc} S(B) & \to & \mathcal{P}(\Psi) \\ F & \mapsto & F \cap \Psi \end{array}$ *est injective.*
Alors la sous-algèbre de Boole engendrée par Ψ est B.

Preuve Notons C la sous-algèbre de Boole engendrée par Ψ, on a alors une surjection continue

$f : \begin{array}{ccc} S(B) & \to & S(C) \\ F & \mapsto & F \cap C \end{array}$ de l'espace de Stone des ultrafiltres de B vers celui des ultrafiltres de C. f est de plus injective par l'hypothèse du lemme, et comme $S(B)$ est quasi-compact et $S(C)$

séparé, f est un homéomorphisme. Le théorème de dualité de Stone permet alors de montrer que l'inclusion $C \to B$ est surjective, ce qui implique que $B = C$.

On considère les corps valués comme des structures à 3 sortes $\mathcal{K} = (K, k, \Gamma; \pi, v)$, on note L le langage à 3 sortes associé, L_r le langage des corps résiduels (celui des anneaux) et L_v le langage des groupes de valuations (celui des groupes ordonnés). On note T la théorie des corps valués henséliens de caractéristique résiduelle nulle.

Les deux lemmes précédents et le théorème d'AKE permettent alors de montrer le résultat suivant :

Corollaire 5.10 *Pour tout énoncé σ dans L, il existe des énoncés $\sigma_r^1, \dots, \sigma_r^k$ dans L_r et des énoncés $\sigma_v^1, \dots, \sigma_v^k$ dans L_v tels que :*

$$T \models \sigma \longleftrightarrow (\sigma_r^1 \wedge \sigma_v^1) \vee \dots \vee (\sigma_r^k \wedge \sigma_v^k) \quad .$$

Preuve Notons B l'algèbre de Boole des énoncés dans le language L à équivalence dans la théorie T (deux énoncés σ et σ' sont équivalents dans T si $T \models \sigma \leftrightarrow \sigma'$). On note également A la sous-algèbre de Boole des classes d'équivalence contenant un énoncé du language $L_r$et A' la sous-algèbre de Boole des classes d'équivalence contenant un énoncé du language L_v.
Posons $\Psi = A \cup A'$, alors d'après le lemme 5.8, il suffit de montrer que Ψ engendre B.

Soient $F, F' \in S(B)$ tels que $F \cap \Psi = F' \cap \Psi$, construisons une L-structure ayant pour théorie (à équivalence dans T près) F. Notons $A(M)$ l'ensemble des termes du langage L sans variables ($A(M)$ est non vide car L contient des constantes) quotienté par la relation d'équivalence $\simeq$ définie par $t \simeq s \Leftrightarrow [t = s] \in F$ pour tous termes sans variables t et s (où $[\sigma]$ est la classe d'équivalence de l'énoncé σ modulo T).
On interprète ensuite des fonctions et relation d'arité n du language L de la manière suivante (ces interprétations sont bien définies car F est un filtre) :
— $f^M(a_1/\simeq, \dots, a_n/\simeq) = f(a_1, \dots, a_n)/\simeq$
— $(a_1/\simeq, \dots, a_n/\simeq) \in R^M \Leftrightarrow [Ra_1 \dots a_n] \in F$
On montre alors par récurrence sur les formules (en utilisant le fait que F est un ultrafiltre) que pour toute formule $\varphi(x_1, \dots, x_n)$ du langage L et tous termes sans variables $a_1, \dots, a_n$, on a ;

$$M \models \varphi(a_1/\simeq, \dots, a_n/\simeq) \Leftrightarrow [\varphi(a_1, \dots, a_n)] \in F \quad .$$

En particulier la théorie de M (à équivalence dans T près) est F, de plus, comme $T = [\top] \in F$, M est un modèle de T.
On construit de manière analogue une L-structure N pour F', alors comme $F \cap \Psi = F' \cap \Psi$, les corps résiduels et les groupes de valuations de M et N sont élémentairements équivalents, donc d'après le théorème d'AKE, $M \equiv N$. Ainsi, par construction $F = F'$, et donc d'après le lemme 5.9, Ψ engendre B, ce qui conclut.

En appliquant le théorème de compacité de la logique propositionnelle au corollaire précédant, on obtiens le résultat suivant.

Proposition 5.11 *Soit σ un énoncé du langage des anneaux valués, alors il existe $N \in \mathbb{N}$ tel que pour tout nombre premier $p > N$:*

$$(\mathbb{Q}_p, \mathbb{Z}_p) \models \sigma \Leftrightarrow (\mathbb{F}_p((t)), \mathbb{F}_p[[t]]) \models \sigma \quad .$$

Preuve Notons T_{hens} la théorie des corps valués henséliens alors d'après le corollaire 5.10, il existe un énoncé $\overline{\sigma}$ dans l'union du langage des anneaux des des groupes ordonnés tels que :

$$T_{hens} \cup \{v(p \cdot 1) > 0 \ : \ p \ premier\} \models \sigma \leftrightarrow \overline{\sigma} \quad .$$

Donc d'après le théorème de compacité de la logique du premier ordre :

$$T_{hens} \cup \{v(p_1 \cdot 1) > 0, \ldots, v(p_n \cdot 1) > 0\} \models \sigma \leftrightarrow \overline{\sigma} \text{ avec } p_1, \ldots, p_n \text{ premiers.}$$

De plus comme $(\mathbb{Q}_p, \mathbb{Z}_p)$ et $(\mathbb{F}_p((t)), \mathbb{F}_p[[t]])$ ont les mêmes corps résiduels et groupes de valuations (qui sont $\mathbb{F}_p$ et $\mathbb{Z}$), on a $(\mathbb{Q}_p, \mathbb{Z}_p) \models \overline{\sigma} \Leftrightarrow (\mathbb{F}_p((t)), \mathbb{F}_p[[t]]) \models \overline{\sigma}$. En posant $N = max(p_1, \ldots, p_n)$, on a alors $(K, A) \models v(p_i \cdot 1) > 0$ pour tout corps valué de caractéristique résiduelle nulle et $i \in \{1, \ldots, n\}$, ce qui permet de conclure.

On déduit de cette proposition le principe d'Ax,Kochen et Ershov.

Théorème 5.12 (Pricipe d'Ax, Kochen et Ershov) *Soit σ un énoncé du langage des anneaux , alors il existe $N \in \mathbb{N}$ tel que pour tout nombre premier $p > N$:*

$$\mathbb{Z}_p \models \sigma \Leftrightarrow \mathbb{F}_p[[t]] \models \sigma \quad .$$

Preuve Pour toute formule φ dans le langage des anneaux, on construit par récurrence une formule $\overline{\varphi}$ dans les langage des corps valués telle que pour tout corps valué (K, A) et toute assignation $\alpha : V \to A$, $A \models \varphi \Leftrightarrow (K, A) \models \overline{\varphi}$. Pour cela on procède ainsi :

— $\overline{t_1 = t_2} = (t_1 = t_2)$ et $\overline{\bot} = \bot$
— $\overline{\varphi \leftrightarrow \psi} = \overline{\varphi} \leftrightarrow \overline{\psi}$
— $\overline{\forall x \varphi(x)} = \forall x (v(x) \geq 0 \wedge \overline{\varphi}(x))$

Ceci permet de conclure à l'aide de la proposition précédente.

Références

[1] L. van den Dries, J. Koenigsmann, H. D. Macpherson, A. Pillay, C. Toffalori, A. J. Wilkie, D. Macpherson, and C. Toffalori, "Model theory in algebra, analysis and arithmetic : A preface," *Model Theory in Algebra, Analysis and Arithmetic : Cetraro, Italy 2012, Editors : H. Dugald Macpherson, Carlo Toffalori*, pp. 1–11, 2014.

[2] D. Marker, *Model theory : an introduction.* Springer Science & Business Media, 2006, vol. 217.