Bagayoko Vincent

Rapport de stage

Stage effectué en Juin-Juillet 2016 sous la direction de Mickaël Matusinski, maître de conférence à l'Institut de Mathématiques de Bordeaux.

Sommaire :

Remerciements

Je tiens à remercier Mickaël Matusinski pour son encadrement de qualité et amical, pour sa patience, son esprit d'initiative, et pour le temps qu'il a consacré à m'aider à comprendre le sujet ainsi qu'à m'ouvrir de nouvelles perspectives mathématiques. Je remercie également le personnel de l'IMB, en particulier les gérants de la bibliothèque et de l'accueil administratif qui m'ont chaleureusement et professionnellement accueilli durant ces deux mois.

Présentation

Le stage consistait en l'étude de la prépublication de Matthias Aschenbrenner, Lou van den Dries, et Joris van der Hoeven *Asymptotic Differential Algebra and Model Theory of Transseries* dont nous disposions de la version du 9 Novembre 2015.

Le livre se veut à la fois une introduction aux notions mathématiques liées à l'algèbre et la théorie des modèles corps différentiels, corps valués, corps valués différentiels, et un article volumineux démontrant un théorème d'éliminations des quantificateurs pour la théorie du premier ordre du corps des transseries. Je n'ai pas eu le temps d'approcher ce résultat même de loin, et l'essentiel de mon travail est concentré dans les trois premiers chapitres.

Autour de cette lecture, j'ai consulté divers ouvrages d'algèbre commutative ou de géométrie algébrique sans entrer dans les détails, mais je me suis régulièrement référé à l'article de Irving Kaplansky *Maximal fields with valuation I* publié en 1942 dans le Duke Mathematical Journal ainsi qu'à une note de lecture pour cet article, *A note on immediate extensions and maximal fields A la Kaplansky*, écrite par Koushik Pal.

Ce rapport présente l'ensemble de ce travail. Le fil directeur des cinq premières parties est la preuve d'un théorème de structure pour les corps valués maximaux d'équicaractéristique nulle, qui est un cas particulier de **[2], Theorem 6, p317**. La preuve sert de prétexte à l'introduction des notions fondamentales de la théorie des corps valués, afin de donner un aperçu des et subtilités de cette dernière.La dernière partie, tirée du chapitre 3.7 de **[1]**, propose un algorithme trouvé dans l'esprit par Issac Newton pour résoudre des équations polynomiales dans un corps en s'aidant d'une valuation.

I - Algèbre commutative

Avant de s'intéresser à la notion de corps valué, on donne ici plusieurs résultats d'algèbre commutative qui seront utiles par la suite. Ces résultats sont pour la plupart des faits connus. La **proposition I.4**, plus spécifique à ce qui nous occupe se trouve dans une version alternative et tronquée dans **[1], Prop 3.1.21, p100**

Proposition I.1 :

Les groupes abéliens divisibles sont des objets injectifs de la catégorie des groupes abéliens, c'est-à-dire que si B est un groupe abélien divisible, et A, C sont des groupes abéliens tels qu'il existe des morphismes $\varphi : A \to B$ et $\rho : A \to C$, alors il existe un morphisme $\psi : C \to B$ tel que $\psi \circ \varphi = \rho$.

$\star \star \star$

(on notera ici les groupes additivement)

Il suffit de le montrer dans le cas où A est un sous-groupe de C.

Considérons l'ensemble X des couples (D, f) où D est un sous-groupe de C contenant A et f est un morphisme $D \to B$ qui prolonge φ. On munit X de l'ordre $\preceq := (\subseteq, \subseteq)$.

X n'est pas vide car il contient (A, φ), et si $\mathcal{C}$ est une chaîne de X, alors son union coordonnée par coordonnée est un majorant de $\mathcal{C}$ dans X, donc $(X, \preceq)$ est inductif, et d'après le lemme de Zorn, il admet un élément maximal (M, ψ).

Montrons que $M = C$. On suppose le contraire et on se donne $c \in C - M$.

Si $M \cap \langle c \rangle = \{0_C\}$, on peut définir un morphisme ψ' sur la somme directe (interne) $M \oplus \langle c \rangle$ en posant $\psi'|_M = \psi$ et $\psi(c) = 0_C$, ce qui contredit la maximalité de (M, ψ).

Donc il existe $n \in \mathbb{Z}$ non nul tel que $n.c \in M$.

On fixe alors $b \in B$ tel que $\psi(n.c) = n.b$ (possible car B est divisible), et pour $x = m + p.c \in M + \langle c \rangle$, on pose $\psi'(x) = \psi(m) + p.b$.

ψ' est bien définie ; en effet, soient $(m, p), (m', p') \in M \times \mathbb{Z}$ tels que $m + p.c = m' + p'.c$.

$\psi(m) + p.b - (\psi(m') + p'.b) = \psi(m - m') + (p - p').b = \psi((p' - p).c) + (p - p').b = \psi(\frac{p'-p}{n}.(n.c)) + (p - p').b = \frac{p'-p}{n}.\psi(n.c) + (p - p').b = \frac{p'-p}{n}.(n.b) - (p - p').b = 0_B$.

Il est alors clair que ψ' est un morphisme $M + \langle c \rangle \to B$, ce qui contredit la maximalité de (M, ψ). On en déduit que $M = C$, ce qui montre que B est injectif.

$\star \star \star$

La réciproque, à savoir que les objets injectifs de la catégorie des groupes abéliens sont divisibles, est vraie mais inutile dans ce qui nous importe.

Bases rationnellement indépendantes

Si $(G, +)$ est un groupe abélien sans torsion, $g \in G$ et $n \in \mathbb{Z} - \{0\}$, il existe au plus un élément de G, noté $\frac{1}{n}.g$, tel que $n.(\frac{1}{n}.g) = g$.

Si B est une partie de G, on note $B^{(\mathbb{Z})}$ l'ensemble des applications $\mathbb{Z} \to B$ à support fini. Pour $f =\in B^{(\mathbb{Z})}$, on note $\overline{f} := \sum_{n \in \mathbb{Z}} n.f(n)$.

On dit que B est une **base rationellement indépendante** de G si $\forall g \in G - \{0\}, \exists!(f, r) \in B^{(\mathbb{Z})} \times \mathbb{N}^*, r.g = \overline{f}$ et $\exists b \in \mathbb{B}, r \wedge f(b) = 1$.

Dans le cas où G est de plus divisible, G admet une base rationnellement indépendante en tant que $\mathbb{Q}$-espace vectoriel, on montre ici que ce résultat est encore vrai lorsque G n'est pas divisible.

Proposition I.2

Soit $(G,+)$ un groupe abélien sans torsion. Il existe une base rationnellement indépendante de $(G,+)$.

$\star\star\star$

Si G est trivial, c'est immédiat. Supposons G non trivial, et soit $g_0 \in G$.

Soit $X := \{B \subset G \mid \forall f, f' \in B^{(\mathbb{Z})}, \overline{f} = \overline{f'} \to f = f'\}$.

On munit X de l'ordre $\subseteq$ d'inclusion large des parties de G.

X n'est pas vide car G étant sans torsion, $\{g_0\} \in X$.

L'union de toute chaîne $\mathcal{C}$ de $(X,\subseteq)$ est un majorant de cette chaîne car les éléments de $\bigcup \mathcal{C}^{(\mathbb{Z})}$ sont à support fini.

Ainsi, d'après le théorème de Zorn, X admet un élément maximal, noté M.

Soit $g \in G$. On suppose que $\forall n \in \mathbb{N}^*, \forall f \in M^{(\mathbb{Z})}$, $n_0.g \neq \overline{f}$.

En particulier, $g \notin M$. Montrons que $M \cup \{g\} \in X$.

Soient $f, f' \in M \cup \{g\}^{(\mathbb{Z})}$ tels que $\overline{f} = \overline{g}$.

$\overline{(f-f')|_M} = (f'-f)(g).g$ où $(f-f')|_M \in M^{(\mathbb{Z})}$. Par définition de g, cela implique que $(f'-f)(g) = 0$, et l'égalité $\overline{f|_M} = \overline{f'|_M}$ implique $f|_M = f'|_M$ car $M \in X$, d'où $f = f'$, et donc $M \sup\{g\} \in X$.

Cela contredit la maximalité de M. On obtient l'existence dans la condition de la définition d'une base rationnelle de G en notant que pour $(f,r,g) \in M^{(\mathbb{Z})} \times \mathbb{N} \times G, \overline{f} = r.g \longrightarrow \overline{\frac{1}{r \wedge \bigwedge\limits_{m \in M} f(m)}.f} = \frac{r}{r \wedge \bigwedge\limits_{b \in \mathbb{Z}} f(m)}.g$ où $\exists m_0 \in M, r \wedge \frac{1}{r \wedge \bigwedge\limits_{m \in M} f(m)}.f(m_0) = 1$.

L'unicité dans la condition découle du théorème de Gauss. M est une base rationnellement indépendante de $(G,+)$.

$\star\star\star$

Expansion de Taylor

Soit A un anneau commutatif, soit $P \in A[X]$.

Pour $i \in \mathbb{N}$ et $a \in A$, on note $P_{(i)}(a)$ l'unique élément de A tel que $P(a+X) = \sum\limits_{i \geq 0} P_{(i)}(a)X^i$.

On a par exemple $P_{(0)}(a) = P(a)$ et $P_{(1)}(a) = P'(a)$.

Si A est un corps de caractéristique nulle, la formule de Taylor donne en général $P_{(i)}(a) = \frac{P^{(i)}(a)}{i!}$, $P^{(i)}$ désignant la i-ième dérivée formelle de P.

En général, $\binom{P_{(i)}(a) = \sum\limits_{j \geq i} j}{i a_j a^{j-i}}$.

Lemme de Krull

On utilisera ces deux résultats connus parfois sans mention ; ils résultent d'une application du lemme de Zorn :

-Si A est un anneau et q est un idéal de A, alors q est contenu dans un idéal maximal de A.

-De plus, si S est une partie multiplicative de A dont q est disjoint, on peut choisir m disjoint de S.

Proposition I.3

Soient $A \subset A'$ des anneaux commutatifs intègres et I' un idéal de A'. On suppose A' entier sur A.

I' est un idéal maximal de A' si et seulement si $I := I' \cap A$ est un idéal maximal de A.

$\star \star \star$

Montrons tout d'abord que A'/I' est entier sur A/I.

Soit $x \in A'$. Il existe $p \in \mathbb{N}$ et $a_0, ..., a_{p-1} \in A$ tels que $x^p + a_{n-1}x^{n-1} + ... + a_0 = 0$.

$(x+I')^p + ... + (a_0 + I') = I'$, et donc $I' = (x+I')^p + ... + (a_0 + I)$, c'est-à-dire que $x + I'$ est entier sur A/I.

On utilise maintenant le lemme suivant : si $B \subset B'$ sont deux anneaux commutatifs intègres et B est entier sur B, alors B' est un corps si et seulement si B est un corps.

En effet, supposons que B est un corps et considérons $x \in B'$ non nul. x est solution d'une équation entière sur B de la forme $x^n + ... + b_0 = 0$. En choisissant une équation de degré minimum, par intégrité de B', on peut se ramener au cas où a_0 est non nul donc inversible dans B, et alors $-{b_0}^{-1}(x^{n-1} + ...b_1) = x^{-1}$. B' est donc un corps.

Réciproquement, si B' est un corps, alors pour $x \in B$ non nul, x^{-1} est entier sur B donc il est solution d'une équation entière sur B de la forme $x^{-m} + ... + c_0 = 0$, et en multipliant par x^{m-1}, on obtient $x^{-1} = -(c_{m-1} + ... + c_0 x^{m-1}) \in B$ donc B est un corps.

L'application de ce lemme aux anneaux A/I et A'/I' fournit le résultat.

$\star \star \star$

Anneaux locaux

Un anneau local est un anneau commutatif intègre A possédant un unique idéal maximal, souvent noté m_A. Le corps A/m_A est appelé **corps résiduel** de A.

L'idéal maximal d'un anneau local est l'ensemble des éléments non-inversibles ou nul de cet anneau.

Si $A \subset A'$ sont des anneaux locaux, on dit que A' **domine** A si $m_A = A \cap m_{A'}$.

Théorème des restes chinois

On a besoin dans le lemme qui suit d'une version faible du célèbre théorème des restes chinois énoncé ici :

Soient A un anneau commutatif, n un nombre naturel, et $I_1, ..., I_n$ des idéaux de A tels que $\forall i \neq j \in \{1; ...; n\}, I_i + I_j = A$.

On note $I = \prod_{i=1}^{n} I_i$.

Alors $I = \bigcap_{i=1}^{n} I_i$ et l'application $\phi : A/I \longrightarrow \prod_{i=1}^{n} A/I_i$ donnée par $\phi(x + I) = (x + I_1, ..., x + I_n)$ est un isomorphisme d'anneaux.

En particulier, π induit un morphisme surjectif $A \to \prod_{i=1}^{n} A/I_i$. (l'application $x \mapsto (x + I_1, ..., x + I_n)$)

Proposition I.4

Soient K un corps, A un sous-anneau local de K d'idéal maximal m, L extension normale de K, B la clôture intégrale de A dans L, et q, q' deux idéaux maximaux de B tels que $q \cap A = q' \cap A = m$.

Il existe $\sigma \in Aut(L \mid K)$ tel que $\sigma(q) = q'$.

$\star \star \star$

On commence par le montrer par l'absurde pour $[L : K]$ fini.

Supposons donc que $\forall \sigma \in Aut(L \mid K), \sigma(q) \neq q'$. Par stabilité de $Aut(L \mid K)$ par inversion et composition, cela équivaut à ce que les ensembles $\{\sigma(q) \mid \sigma \in Aut(L \mid K)\}$ et $\{\sigma(q') \mid \sigma \in Aut(L \mid K)\}$ soient disjoints.

On note U leur réunion. B étant la clôture intégrale de A dans L, les éléments de $Aut(L \mid K)$ stabilisent B, donc $Aut(L \mid K) \subset Aut(B \mid K)$ et U est un ensemble d'idéaux maximaux de B. U est fini car L / K étant de degré fini, $Aut(L \mid K)$ est fini.

Soient $p_0 \neq p_1 \in U$. $p_0 + p_1$ est un sur-idéal propre de p_0 car par maximalité de p_1, $p_1 \subsetneq p_0$; par maximalité de p_0,$p_0 + p_1 = B$.

ON peut donc utiliser la version faible du théorème des restes chinois pour déduire l'existence d'un élément $x \in B$ tel que $\forall \sigma \in Aut(L \mid K), x + \sigma(q) = \sigma(q)$ et $x + \sigma(q') = 1 + \sigma(q')$.

En particulier $x \in \sigma(q) \quad \sigma(q') \forall \sigma \in Aut(L \mid K)$, donc $\sigma(x) \in q \quad q', \forall \sigma \in Aut(L \mid K)$.

Posons $a = \prod_{\sigma \in Aut(L \mid K)} \sigma(x)$. $a \in B$ car les $\sigma(x)$ sont dans B qui est stabilisé par les éléments de $Aut(L \mid K)$.

q étant un idéal contenant tous les $\sigma(x)$, $\prod_{\sigma \in Aut(L \mid K)} \sigma(x) \in q$. q' étant premier, $B \setminus q'$ est une partie multiplicative, et donc $a \in B \setminus q'$.

Donc $a \in q \setminus q'$.

La théorie des normes donne alors l'alternative suivante :

-Si K est de caractéristique nulle, a est le coefficient constant du polynôme caractéristique de x sur K, donc $a \in K$.

-Si K est de caractéristique strictement positive p, alors a est radiciel sur K, et il existe $m \in \mathbb{N}$ tel que $a^{p^m} \in K$.

Dans tous les cas, il existe $r \in \mathbb{N}^*$ tel que $a^r \in K$, donc a est entier sur A, qui est intégralement clos dans K, donc $a \in A$.

$a \in A \cup q = m = A \cap q'$, ce qui contredit le fait que $a \notin q'$. On en déduit que la supposition $\forall \sigma \in Aut(L \mid K), \sigma(q) \neq q'$ est absurde, et donc qu'il existe $\sigma \in Aut(L \mid K)$ tel que $\sigma(q) = q'$.

Il reste à montrer le résultat dans le cas général. On utilise le lemme de Zorn.

Soit X l'ensemble des couples (F, φ) où F est un sous-corps de L contenant K et φ est un automorphisme de F sur K tel que $\varphi(q \cap F) = q' \cap F$.

On munit X de l'inclusion $(\subseteq, \subseteq)$, qui en fait un ensemble partiellement ordonné non vide, car $(K, id_K) \in X$.

X est inductif car stable par union de chaînes. Il admet donc un élément maximal (F_0, φ_0).

On va montrer par l'absurde que $F_0 = L$, ce qui conclura la preuve.

Supposons le contraire, et considérons un élément quelconque $y \in L - F_0$. Soit Π_y son polynôme minimal sur K. On note F_1 le corps de décomposition de Π_z sur F_0.

F_1 est une extension normale de F_0 donc on peut prolonger φ_0 en un automorphisme φ_1 de F_1 sur K.

On note $q_0 = F_0 \cap q$, $q_1 = F_1 \cap q$, $q_1' = F_1 \cap q'$, et $q_1'' = {\varphi_1}^{-1}(q_1')$.

Soit $B_1 := B \cap F_1$ la clôture intégrale de A dans F_1, qui est également la clôture intégrale de . B est entier sur B_1 car entier sur $A \subset B_1$, donc d'après la **proposition I.3**, q_1, q_1' sont des idéaux maximaux de B_1. Puisque ${\varphi_1}^{-1}$ est un automorphisme de F_1 qui fixe K, il fixe A et stabilise donc B_1, donc q_1'' est également un idéal maximal de B_1.

De plus, $q_1 \cap A = F_1 \cap A \cap q = A \cap q = m$, et $\varphi_1(q_1'' \cap A) = \varphi_0(q_1 \cap A) = \varphi_0(A \cap q) = \varphi_0(m) = \varphi_1(m)$ donc $q_1'' \cap A = m$.

Enfin, F_1 est une extension finie de F_0.

On peut donc appliquer le résultat dans le cas fini (à $K \equiv F_0$, $L \equiv F_1$, $A \equiv A$, $B \equiv B_1$, $q \equiv q_1$ et $q' \equiv q_1''$ pour déduire l'existence de $\sigma \in Aut(F_1 \mid F_0)$ tel que $\sigma(q_1) = q_1''$.

On pose $\psi = \varphi_1 \circ \sigma \in Aut(F_1 \mid K)$. $\psi(q_1) = q_1'$.

Par ailleurs, F_1 est une extension normale de K (par transitivité de la normalité des extensions), donc $(F_1, \psi) \in X$.

Puisque σ fixe F_0 et φ_1 prolonge φ_0, ψ prolonge φ_0 et donc (F_1, ψ) est strictement supérieur à (F_0, φ_0) dans X, ce qui est contradictoire.

On en déduit que $F_0 = L$, ce qui conclut la preuve.

$\star \star \star$

II - Généralités sur les corps valués

Dans cette partie, on définit les corps valués et les objets qui leurs sont liés, en dérivant des propriétés fondamentales des résultats d'algèbre commutative donnés en première partie.

Les définitions et résultats sont tous tirés de **[1], chap 3.3.1**.

Définition II.1

Si K est un corps (commutatif, non nul), et $(\Gamma, +, <)$ est un groupe ordonné, on dit qu'une application $\nu : K \to \Gamma$ est une **valuation** sur K si elle satisfait les conditions suivantes.

$(V1) : \forall x, y \in K^\times, v(xy) = vx + vy$

$(V2) : \forall x, y \in K^\times, x + y \neq 0 \longrightarrow v(x + y) \geq \min(vx, vy)$.

Conventions et propriétés additionnelles :

Les propriétés suivantes sont des conséquences rapides des définitions qui seront utilisées sans mention dans la suite, on laisse les démonstrations au lecteur.

-Par convention, on pose $v(0) = +\infty$, et puisque $v(K^\times)$ est un sous-groupe de Γ, on supposera également que $\Gamma = v(K^\times)$. Dans la suite, on notera plutôt $\Gamma = vK$.

-Si x, y sont tels que $vx < vy$, alors $v(x + y) = vx$, et de manière générale, si $x_1, ..., x_n$ sont tels que $vx_i < \min_{j \neq i}(vx_j)$, alors $v(x_1 + ... + x_n) = v(x_i)$

-On définit une relation $\preceq$ sur K par $x \preceq y \longleftrightarrow vx \geq vy$.

Les relations $x \asymp y \longleftrightarrow vx = vy$ et $x \sim y \longleftrightarrow v(x-y) > vx$ sont des relations d'équivalence sur $K^\times$ respectivement appelées **équivalence asymptotique** et **équivalence forte** (ou plus simplement équivalence).

On note aussi $x \prec y$ pour signifier $x \preceq y \wedge \neg(x \asymp y)$, ce qui est équivalent à $vx > vy$.

On note $K^{\preceq 1}$ (resp $K^{\prec 1}$) l'ensemble des éléments x de K satisfaisant $x \preceq 1$, (resp $x \prec 1$).

$K^{\preceq 1}$ est un sous-anneau local de K appelé **anneau de valuation** de (K, v), d'idéal maximal $K^{\prec 1}$. Pour $x \in K^{\preceq 1}$, on note $xv := x + K^{\prec 1}$, et on note Kv le corps résiduel $K^{\preceq 1}/K^{\prec 1}$, Kv est appelé **corps résiduel** de $(\mathbf{K}, \mathbf{v})$.

-En tant que groupe ordonné, vK est soit trivial (v est alors dite **valuation triviale** sur K), soit infini, donc tout corps fini admet la valuation triviale pour seule valuation.

-La **caractéristique d'un corps valué** (K, v) est le couple $(\chi(K), \chi(Kv))$. (K, v) est dit **d'équicaractéristique** p (resp **d'équicaractéristique nulle**) si $\chi(K, v) = (p, p)$ (resp $\chi(K, v) = (0, 0)$). Dans tout autre cas, (K, v) est dit de caractéristique mixte, et alors il existe un nombre premier p tel que $\chi(K, v) = (0, p)$.

On se concentrera dans ce document sur l'étude des corps d'équicaractéristique nulle, puisque c'est le cas dans la situation qui nous intéresse où K et Kv sont ordonnés. A noter que dans ce cas (et seulement dans ce cas), ${K^{\preceq 1}}^\times$ contient le sous-corps $\mathbb{Q}.1v$ isomorphe à $\mathbb{Q}$. Sauf mention explicite, (K, v) désigne un corps valué de caractéristique quelconque.

Exemples simples de corps valués

Soit K un corps, soit n un nombre naturel. On considère le corps $K(X)$ des fractions polynomiales à 1 indéterminées sur K. Soit $a \in K$.

-On munit K de la valuation $v : K^\times \to \mathbb{Z}$ donnée par $v\frac{P}{Q} := mul_a(P) - mul_a(Q)$, où $mul_a(R)$ pour $R \in K[X]$ non nul désigne la plus grande puissance de $X - a$ qui divise R. (l'ordre sur $\mathbb{Z}$ étant l'ordre classique)

(K, v) est un corps valué de groupe de valeur $\mathbb{Z}$ et de corps résiduel isomorphe à K. Si K est un corps ordonné, les classes d'équivalence asymptotique pour cette valuation correspondent aux germes de fonctions rationnelles en a.

-On munit K de la valuation $w : K^\times \to \mathbb{Z}$ donnée par $v\frac{P}{Q} := \deg(P) - \deg(Q)$

(K, v) est un corps valué de groupe de valeur $\mathbb{Z}$ et de corps résiduel isomorphe à K. Si K est un corps ordonné, les classes d'équivalence asymptotique pour cette valuation correspondent aux germes de fonctions rationnelles en $+\infty$.

Définition II.2 : valuation convexe sur un corps ordonné

Soit $(K, <)$ un corps ordonné.

Une valuation sur K est dite **convexe** si son anneau de valuation est convexe pour l'ordre sur K, c'est-à-dire si $\forall x < y < z, x, z \in K^{\preceq 1} \rightarrow y \in K^{\preceq 1}$.

On dispose d'une valuation convexe v dite **naturelle** sur K définie pour $x \in K$ par $vx := \{y \in K^\times \mid \exists n \in \mathbb{N}, \frac{1}{n}.|x| \leq |y| \leq n.|x|\}$ (où $|x| := \max(x, -x)$).

Les vx sont les **classes archimédiennes**, et leur ensemble vK est muni de la loi $vx + vy := v(xy)$ qui en fait un groupe de neutre $v1$.

On munit vK de la relation d'ordre totale $A < B$ si et seulement si $A \cap K_+ < B \cap K_+$ au sens de l'ordre induit par $<$ sur les parties de K.

A noter que si $(K, <)$ est archimédien (ou de manière si c'est un sous corps ordonné de $\mathbb{R}$), alors la valuation naturelle sur k est triviale.

La résolution asymptotique d'équations différentielles dans des corps ordonnés comme le corps des transséries se fait à l'aide de valuations convexes.

Différents anneaux de valuations convexes produisent des notions d'équivalence asymtotique moins précises que l'équivalence archimédienne, ainsi, on munit souvent un corps ordonné de la valuation naturelle, et on considère d'autres valuations convexes pour étudier la valuation naturelle, ou dans des contextes divers.

Anneaux de valuation et relations de dominance

Il existe plusieurs notions équivalentes à celle de valuation sur un corps. Les deux que l'on va présenter rapidement ici sont plus appropriées dans certains contextes. La première est un *quasi*-ordre qui permet de voir les éléments d'un corps valué comme des germes de fonctions à l'infini, approche essentielle lorsqu'il s'agit d'utiliser les transséries pour résoudre des équations différentielles. L'autre est un anneau local permettant de traiter plus facilement les propriétés directement liées à l'algébre commutative.

Définition II.3 : relations de dominance

-Soit K un corps. Une **relation de dominance** sur K est une relation binaire $\preceq$ sur K satisfaisant :

$(D1) : \forall x \in K, x \preceq x$

$(D2) : \forall x, y, z \in K, x \preceq y \wedge y \preceq z \longrightarrow x \preceq z$

$(D3) : \forall x, y \in K, x \preceq y \vee y \preceq x$

$(D4) : \forall x \in K, 0 \preceq x.$

$(D5) : \forall x, y, z, t \in K x \preceq y \wedge z \preceq t \longrightarrow xy \preceq zt$

$(D6) : \forall x, y \in K, x + y \preceq x \vee x + y \preceq y.$

A toute relation de dominance $\preceq$, on associe la relation stricte $\prec$ définie par $x \prec y \longleftrightarrow x \preceq y \wedge y \not\preceq x$.

Définition II.4 : anneaux de valuation

Soit K un corps. Un **anneau de valuation** sur K est un sous-anneau local A de K tel que $\forall x \in K, x \in A$ ou $x^{-1} \in A$.

Remarque : Tout anneau de valuation sur K est intégralement clos dans K.

En effet, si A est un anneau de valuation et $x \in K$ satisfait $x^n + ... + a_0 = 0$ où $n \in \mathbb{N}^*$ et $a_0, .., a_{n-1} \in A$, alors $vx < 0$ est impossible car sinon la comparaison $vx^n = nvx < va_i x^i \ \forall i \in \{0; ...; n-1\}$ donnerait $v(x^n + ... + a_0) = vx^n < 0$: impossible. Donc $vx \geq 0$, c'est-à-dire que x est dans A.

La correspondance entre valuations, anneau de valuation, relation de dominance se fait comme suit :

Si v est une valuation sur K alors :
-$\{x \in K \mid vx \geq 0\}$ est l'anneau de valuation associé.
-$\{(x, y) \in K^\times \times K^\times \mid vx \geq vy\}$ est la relation de dominance associée.

Si A est un anneau de valuation sur K alors :
-$\{(x, y) \in K^\times \times K^\times \mid \frac{x}{y} \in A\}$ est la relation de dominance associée.
-$x \longmapsto xA^\times \in K^\times / A^\times$ est l'anneau de valuation associée, l'ordre sur le groupe de valeur étant donné par $xA^\times < yA^\times \longleftrightarrow \frac{y}{x} \in m_A$.

Si $\preceq$ est une relation de dominance sur K alors :
-$x \longmapsto [x] := \{y \in K^\times \mid x \preceq y \wedge y \preceq x\}$ est la valuation associée, la loi de groupe et l'ordre de groupe sur l'ensemble des valeurs étant donnés par $[x] + [y] = [xy]$ et $[x] < [y] \longleftrightarrow \frac{y}{x} \prec 1$.
-$\{x \in K \mid x \preceq 1\}$ est l'anneau de valuation associé.

Cette correspondance, combinée aux définitions de relation de dominance et d'anneau de valuation, montre que la théorie des corps valués est finiment axiomatisable dans le langage des corps auquel on ajoute un symbole de relation binaire ou de prédicat unaire.

Dans tout ce qui suit, on se permettra de jongler entre les valuations, les relations de dominance et les anneaux de valuation en fonction du contexte tout en s'efforçant de lever les ambiguïtés. On parlera donc du corps valué (K, v) aussi bien sous la forme (K, A) que $(K, \preceq)$.

Définition II.5 : Extension de corps valué

Une **extension d'un corps valué** (K, A) est la donnée d'un surcorps K' de K et d'un anneau de valuation A' sur K' qui domine A.

De manière équivalente, la valuation v' sur K' associée à A' prolonge v (après plongement naturel de $K^\times/A^\times$ dans ${K'}^\times/{A'}^\times$), et la relation de dominance $\preceq'$ associée à A' prolonge $\preceq$.

Les morphismes, plongements, isomorphismes, sont les morphismes d'extension, injectifs, bijectifs.

Si (K', A') est une extension de (K, A), alors vK, Kv se plongent naturellement respectivement dans $v'K', K'v'$ via $vx \longmapsto v'x$ et $xv \longmapsto xv'$.

Proposition II.1

Soit K un corps. Les anneaux de valuation sur K sont les sous-anneaux locaux de K maximaux pour la relation de dominance entre anneaux locaux.

$\star \star \star$

On démontre tout d'abord le lemme suivant :

Si A est un anneau local de K et x un élément non nul de K tel que $1 \in m_A + x^{-1}A[x^{-1}]$, alors x est entier sur A.

En effet, on peut écrire $1 = a_n x^{-n} + ... + a_1 x^{-1} + a_0$ où $a_0 \in m_A$ et les $a_i, i > 0$ sont dans A.

On a alors en multipliant par x^n : $x^n(1 - a_0) - a_n - ... - a_1 x^{n-1} = 0$, avec $(1 - a_0) \in A^\times$ car $a_0 \in m_A$.

Ainsi, x est solution de l'équation entière sur A : $X^n + (a_0 - 1)^{-1}a_1 X^{n-1} + ... + (a_0 - 1)^{-1}a_n = 0$, ce qui prouve le lemme.

Soit A un sous-anneau local de K maximal pour la relation de dominance.

Soit $x \in K^\times$.

Si x est entier sur A, alors $A[x]$ est entier sur A.

$m_A[x]$ est un idéal de $A[x]$ disjoint de la partie multiplicative $A - m_A$, donc $m_A[x]$ est inclus dans un idéal maximal q de $A[x]$ disjoint de $A - m_A$. (**lemme de Krull**)

$m_A \subset q$ et $q \cap A \subset m_A$ donc $q \cap A = m_A$.

$A[x]_q$ est alors un sous-anneau local de K qui domine A, donc $A[x]_q = A$, et $x \in A$.

Si x n'est pas entier sur A, par contraposition du lemme, $1 \notin m_A + x^{-1}A[x^{-1}]$.

$m_A A[x^{-1}]$ n'est donc pas maximal dans $A[x^{-1}]$, il est donc contenu dans un idéal maximal p de $A[x^{-1}]$.

$p \cap A = m_A$ car $m_A = A - A^\times$, et donc $A[x^{-1}]_p$ est un sous-anneau local de K qui domine A, on obtient comme précédemment $x^{-1} \in A$.

A est donc un anneau de valuation sur K.

$\star \star \star$

Proposition II.2

Si K est un corps, A est un sous-anneau local de K et est L une extension de corps de K, alors L admet un anneau de valuation qui domine A.

$\star \star \star$

D'après la proposition précédente, il suffit de montrer que l'ensemble des sous-anneaux locaux de L qui dominent A admet un élément maximal. Or cet ensemble contient A et est inductif car stable par union de chaînes ; d'après le lemme de Zorn, il admet un élément maximal qui est donc un anneau de valuation de L qui domine A.

$\star \star \star$

Corollaire

Si L est une extension de K et A un anneau de valuation de K, alors il existe un anneau de valuation V de L tel que (L, V) est une extension de (K, A).

Proposition II.3

Soient K un corps et A un sous-anneau local de K. La clôture intégrale B de A dans K est l'intersection des anneaux de valuation de K qui dominent A.

$\star \star \star$

Tout anneau de valuation de K qui contient A est intégralement clos dans K donc contient B.

Soit $x \in K^\times$ non entier sur A. Par contraposition du lemme utilisé dans la proposition précédente, $m_A A[x^{-1}] + x^{-1}A[x-1]$ est un idéal propre de $A[x^{-1}]$, qui est donc contenu dans un idéal maximal q de $A[x^{-1}]$.

$x^{-1} \in q$, et le sous-anneau local $A[x^{-1}]_p$ de K domine A.

Soit V un anneau de valuation de K qui domine $A[x^{-1}]_p$ (V existe d'après la **proposition II.2**).

V domine A et $x_{-1} \in m_V$, donc $x \notin V$, et x n'est pas dans l'intersection des anneaux de valuations de K qui dominent A.

Cela conclut la preuve.

$\star \star \star$

Proposition II.4

Soit (K, A) un corps valué, soit L une extension algébrique de K. On note B la clôture intégrale de A dans L.

Si V est un anneau de valuation de L qui domine A, alors $V = B_{m_V \cap B}$.

$\star \star \star$

Soit V un tel anneau de valuation. On note w la valuation associée sur L. V est intégralement clos et contient A donc $B \subset V$ donc $B_{m_V \cap B} \subset V$.

Montrons l'inclusion inverse. Soit $x \in V$.

x est algébrique sur $K = Frac(A)$ donc sur A : soient $n \in \mathbb{N}^*, a_0, ..., a_n \in A$ tels que $a_n x^n + ... + a_0 = 0$.

Soit $j \in \{0; ...; n\}$ maximal tel que $wa_j = \min(\{va_i \mid 0 \leq i \leq n\})$. On pose pour $0 \leq i \leq n, b_i = \frac{a_i}{a_j}$.

Pour tout i entre 0 et n, $b_i \in A$ et $i > j, b_j \in m_V \cap A = m_A$.

On obtient en divisant par $a_j x^j$:

$(b_n x^{n-j} + ... + 1) + x^{-1}(b_{j-1} + ... + b_0 x^{1-j}) = 0$. Posons $y, z = (b_n x^{n-j} + ... + 1), (b_{j-1} + ... + b_0 x^{1-j})$, de sorte que $x = -y^{-1} z$.

$y \notin m_V$ car pour $i > j, wb_i x^i \geq wb_i > 0$ d'où $wy = w1 = 0$.

Il suffit donc pour montrer que $-y^{-1}z$ est dans B_{m_V} de prouver que y et z sont dans B.

D'après la proposition précédente, B est l'intersection des anneaux de valuations de L dominant A, donc il suffit de montrer que tout tel anneau de valuation V' contient y et z.

Si $x \in V'$, $y \in V'$ car $y \in A[x] \subset V'[x] = V'$. Donc $z = -yx \in V'$.

Sinon, $x^{-1} \in V'$ donc de même $z \in V'$, puis $y = -zx^{-1} \in V'$: C.Q.F.D.

$\star \star \star$

Corollaire

Si L/K est normale, alors les anneaux de valuation de L qui dominent A sont isomorphes sur K.

$\star$

Soient V, V' deux anneaux de valuation de L qui dominent A.

D'après la **proposition I.4**, il existe $\sigma \in Aut(L\,|K)$ tel que $\sigma(m_V) = m_{V'}$.

Puisque $V = B_{m_V \cap B}$, $V' = B_{m_{V'} \cap B}$ et σ stabilise B (puisqu'il fixe $A \subset K$), $\sigma(V) = V'$.

$\star$

Définition II.6 : types particuliers d'extensions

Soit (K, v) un corps valué et (K', v') une extension de (K, v).

Une extension $(K', v')/(K, v)$ est dite **immédiate** si elle possède le même groupe de valeur et le même corps résiduel que (K, v). Plus précisément, les plongements naturels décrits en **définition II.6** sont surjectifs.

Une extension $(K', v')/(K, v)$ est dite **algébrique** si K' K est algébrique.

(K, v) est dit **maximal** s'il n'admet aucune extension immédiate propre.

(K, v) est dit **algébriquement maximal** s'il n'admet aucune extension algébrique immédiate propre.

Il est clair que la maximalité entraîne la maximalité algébrique. Voici maintenant un exemple de corps valué maximal dont le caractère fondamental sera illustré par un théorème de structure qui est le résultat principal des premières parties.

Définition II.6 : séries de Hahn avec cocycle

Soient C un corps, $(\Gamma, <)$ un groupe ordonné, et $\lambda : \Gamma^2 \to C^\times$ une application symétrique (i.e. $\lambda(\alpha, \beta) = \lambda(\beta, \alpha)\ \forall \alpha, \beta \in \Gamma$) appelée cocycle.

On considère l'ensemble $C((t^\Gamma))$ des applications $\Gamma \to C$ dont le support (image réciproque de $C^\times$) est bien ordonné par $<$, et on le munit des lois suivantes :

$f + g = \Gamma \ni \gamma \longmapsto f(\gamma) + g(\gamma)$

$fg = \Gamma \ni \gamma \longmapsto \sum_{\alpha+\beta=\gamma} \lambda(\alpha, \beta) f(\alpha) g(\beta)$

Il faut un certain travail pour justifier que la somme définissant $(fg)(\gamma)$ est toujours finie et que le support de fg est bien ordonné.

Ces lois permettent de voir $C((t^\Gamma))$ comme une structure de séries formelles de variable t, en utilisant la convention $f(\gamma) \equiv f_\gamma$ et $f \equiv \sum_{\gamma \in \Gamma} f_\gamma t^\gamma$.

Cette structure est en fait un corps, et l'application $v : f \longmapsto \min(f^{-1}(C^\times))$ est une valuation sur $C((t^\Gamma))$ dont on le munira systématiquement.

III - Suites pseudocauchy

Il semble que la notion de suite pseudocauchy que l'on introduit ici soit nécessaire pour faire le lien entre différentes qualités de corps valués. On tentera de la rendre pratique et de faire remarquer sa présence dans différentes méthodes de démonstration et de calcul.

Les définitions de cette partie sont tirées de **[1], chap 3.2**, les théorèmes principaux sont dus à Kaplansky (dans des versions bien plus générales) et tirées de **[3]** ou **[2]**.

Définition III.1

Soit (K, v) un corps valué. Soit γ un ordinal limite soit $u : \gamma \to K$, et soit $x \in K$.

On dit que u est **pseudocauchy** si $\exists \rho_0 < \gamma, \forall \rho_0 < \rho < \sigma < \lambda < \gamma, v(u_\lambda - u_\sigma) > v(u_\sigma - u_\rho)$.

On dit que x est une **pseudolimite** de u ou que u pseudoconverge vers x, et on écrit $u \rightsquigarrow x$ si $(v(u_\rho - x)_{\rho<\gamma}$ est éventuellement strictement croissante.

Propriétés

Les propriétés suivantes découlent directement des définitions d'une valuation et du caractère pseudocauchy. Soit $u : \gamma \to K$.

(i) : Si u est pseudocauchy, pour tout ordinal ρ_0 satisfaisant les conditions de la définition, on a $\forall \rho_0 < \sigma < \lambda < \gamma, v(u_\lambda - u_\sigma) = v(u_{\sigma+1} - u_\sigma)$.

(ii) : Si u est pseudocauchy, $v(u) := v \circ u$ est soit éventuellement strictement croissante (auquel cas $u \rightsquigarrow 0$), soit éventuellement constante.

(iii) : Si u admet une pseudolimite, alors u est pseudocauchy.

(iv) : Si a, b sont des pseudolimites de u, alors $v(a-b) > v(v(u_{\sigma+1}-u_\sigma)\ \forall \rho < \sigma < \lambda$ où ρ_0 respecte la condition de la définition du caractère pseudocauchy.

Proposition III.1 (Kaplansky)

Soit (K, v) un corps valué, et soit (L, w) une extension immédiate. Tout élément de $L - K$ est pseudolimite d'une suite pseudocauchy de (K, v) sans pseudolimite dans K.

$\star \star \star$

Soit $z \in K' - K$. On note V l'ensemble $\{v'(z - x) \mid x \in K\}$.

Montrons que V ne possède pas de maximum. Soit $\gamma \in S$. $\gamma \neq +\infty$ du fait que $z \notin K$.

On choisit $x \in K$ tel que $\gamma = v'(z-x)$. Puisque (K', v') (K, v) est immédiate, $vK = v'K'$, donc il existe $y \in K$ tel que $vy = v'(z-x)$, donc $v(\frac{z-x}{y}) = 0$.

Cela implique que $\frac{z-x}{y}$ est dans $K'^{\asymp 1}$, et on peut considérer $\frac{z-x}{y}v' \in K'v' = Kv$, donc il existe $t \in K^{\asymp 1}$ tel que $\frac{z-x}{y}v' = tv = tv'$.

On a donc $\frac{z-x-ty}{y}v' = 0$, donc $v'\frac{z-x-ty}{y} > 0$, donc $v'(z-(x+ty)) > v'(y) = \gamma$, avec $x+ty \in K$. On a donc trouvé un élément $v'(z-(x+ty))$ de V strictement supérieur à γ.

La cofinalité κ de $(V, <)$ est donc limite, et on dispose d'une κ-suite u d'éléments de K telle que $v'(z-u)$ est strictement croissante et cofinale dans V.

En particulier, u est pseudocauchy et elle pseudoconverge vers z.

Supposons que u admette une pseudolimite z' dans K. On a $v(z-z') > v'(z-u_\rho)$ $\forall \rho < \kappa$, ce qui contredit la cofinalité de $v'(z-u)$ dans V.

Ainsi, u est bien sans pseudolimite dans K, ce qui conclut la preuve.

$\star \star \star$

Lemme III.1

Soit $u : \gamma \to K$, et soit x une pseudolimite de u. Soit $P \in K[X] - K$.

On a $P(u) := P \circ u \rightsquigarrow P(x)$.

$\star \star$

On se place dans les conditions de l'énoncé.

Notons que pour $\rho < \gamma, P(u_\rho) - P(x) = \sum_{i \geq 1} P_{(i)}(x)(u_\rho - x)^i$.

Posons pour i entre 1 et n $\beta_i := v(P_{(i)}(x))$, et pour $\rho < \gamma, c_\rho := v(x-u_\rho)$, de sorte que $v(P_{(i)}(x)(u_\rho - x)^i) = \beta_i + i.\lambda_\rho$.

Montrons par induction qu'il existe i_0 entre 1 et $\deg(P)$ tel qu'éventuellement, on ait pour $i \neq i_0$, $\beta_i + i.\lambda_\rho > \beta_{i_0} + i_0.\lambda_\rho$. On le montre en général pour un ensemble d'indices i représentant des entiers naturels non nuls.

C'est vrai si $\deg(P) = 2$ (le cas $d = 1$ étant vrai par vacuité) : on a alors pour $\rho < \gamma$, et $j < i$, $\beta_i + i.\lambda_\rho - (\beta_j + j.\lambda_\rho) = \beta_i - \beta_j + (i-j).\lambda_\rho$ et λ_ρ étant strictement croissante à partir de $\rho_0 < \gamma$, on obtient le résultat en distinguant les cas $\exists \rho > \rho_0, (i-j).\lambda_\rho > \beta_j - \beta_i$, pour lequel $i_0 = j$, et celui où $\forall \rho > \rho_0, (i-j).\lambda_\rho \leq \beta_i - \beta_j$, pour lequel $i_0 = i$.

Supposant le résultat vrai jusqu'à un certain degré d, on obtient le résultat pour $d+1$ en appliquant le résultat à $\{i_1; ...; i_d\}$ et obtenant i_0, puis à $\{i_0; i_{d+1}\}$.

Soit dnc i_0 un tel indice. On a donc éventuellement $vP(u_\rho - x) = \beta_{i_0} + i_0.\lambda_\rho$, qui est strictement croissante car $i_0 > 0$ (P n'étant pas une constante) et $(\lambda_\rho)_{\rho_0 < \rho < \gamma}$ croît strictement.

C'est-à-dire que $P(u) \rightsquigarrow P(x)$.

⋆ ⋆

Corollaire

Si $u : \lambda \to K$ est pseudocauchy et $P \in K[X]$ est non constant, alors $P(u)$ est pseudocauchy.

⋆

Soit $\rho_0 < \lambda$ tel que $\rho_0 < \rho < \sigma < \gamma < \lambda, v(u_\gamma - u_\sigma) > v(u_\sigma - u_\rho)$. Il revient au même de le montrer pour la suite $(u_{\rho_0+\alpha})_{\rho_0+\alpha<\lambda}$, on peut donc supposer que $\rho_0 = 0$.

On considère un ultrafiltre non principal W sur λ et on étudie l'ultrapuissance $({}^*K, {}^*K^{\preceq 1}) = (K, +, ., 0, 1, K^{\preceq 1})^\lambda / W$.

C'est une extension élémentaire de (K, A), donc une extension de corps valué de K dans laquelle l'image ${}^*u$ de u par le plongement naturel $\varphi : K \longrightarrow {}^*K$ pseudoconverge vers la classe d'équivalence $u[W]$ de u modulo W.

En effet, soit $\rho_0 < \lambda$ tel que $\rho_0 < \rho < \sigma < \gamma < \lambda, v(u_\gamma - u_\sigma) > v(u_\sigma - u_\rho)$.

Soient $\rho_0 < \rho < \sigma < \lambda$.

On cherche à montrer que ${}^*v({}^*u_\sigma(\alpha) - u[W]) >^* v({}^*u_\rho - u[W])$, c'est-à-dire que $\frac{{}^*u_\sigma(\alpha) - u[W]}{{}^*u_\rho - u[W]}$ est dans l'idéal maximal de ${}^*A$, donc que c'est un élément non inversible de ${}^*A$.

Cela revient par définition d'un ultraproduit à montrer que l'ensemble $X := \{\alpha \in \lambda \mid \frac{u_\sigma - u_\alpha}{u_\rho - u_\alpha} \in A \wedge \frac{u_\rho - u_\alpha}{u_\sigma - u_\alpha} \notin A\}$ est dans W.

Il suffit pour cela de montrer qu'il contient tous les ordinaux de λ à partir de $\rho_0 + 1 = 1$ car $\lambda - \{0\} \in W$. Ceci est immédiat par définition de ρ_0.

Ainsi, (K, A) admet une extension (élémentaire) dans laquelle u est pseudoconvergente. D'après le lemme précédent, $\varphi(P)(u)$ y est également pseudoconvergente, donc pseudocauchy, donc $P(u)$ est pseudocauchy dans (K, A).

⋆

Définition III.2

Soit $u : \gamma \to K$ pseudocauchy dans (K, v).

-u est dite **de type algébrique** s'il existe $P \in K[X] - \{0\}$ tel que $P(u) \rightsquigarrow 0$. Dans ce cas, l'ensemble des éléments de $K[X]$ satisfaisant cela est un idéal dont on note Π_u l'unique générateur unitaire.

Π_u est appelé **polynôme minimal** de u sur (K, v).

-u est dite **de type transcendant** sinon.

Proptiété :

Le polynôme minimal d'une suite pseudocauchy u de type algébrique sur (K, v) est irréductible sur K.

En effet, supposons qu'il existe $Q, R \in K[X]$ non inversibles tels que $\Pi_u = QR$. Alors d'après le corollaire précédent, $Q(u), R(u)$ sont pseudocauchy. Si $v(Q(u))$ est éventuellement constante, alors puisque $v(\Pi_u(u)) = v(Q(u)) + v(R(u))$ est éventuellement strictement croissante, il en est de même pour $v(R(u))$ et donc $R(u) \rightsquigarrow 0$, donc $\Pi_u \mid R$ donc Π_u et R sont associés et Q est inversible : contradictoire.

Proposition III.2

Soit (K, v) un corps valué, et soit (K', v') une extension immédiate. Tout élément de $K' - K$ algébrique sur K est pseudolimite d'une suite pseudocauchy de (K, v) de type algébrique sans pseudolimite dans K.

$\star \star \star$

Soit $z \in K' - K$.

La **proposition III.1** fournit une suite pseudocauchy $u : \kappa \to K$ sans pseudolimite dans K qui pseudoconverge vers z.

Soit Π_z le polynôme minimal de z sur K.

Soit $\rho < \kappa$.

$\Pi_z(u_\rho) = \Pi_z(u_\rho) - \Pi_z(z) = (u_\rho - z)Q(u_\rho)$ pour un certain $Q \in K[a][X] = K(a)[X]$. (voir *expansion de Taylor* en partie I)

$v\Pi_z(u_\rho) = v(u_\rho - a) + vQ(u_\rho)$.

Le premier terme dans la somme de droite est éventuellement strictement croissant (en ρ) tandis que le second terme est éventuellement croissant, donc $v(\Pi_z(u_\rho))$ est éventuellement strictement croissante, c'est-à-dire que $\Pi_z(u) \rightsquigarrow 0$.

Donc u est de type algébrique, ce qui conclut la preuve.

$\star \star \star$

Théorème III.1

Soit (K, v) un corps valué, soit $u : \gamma \to K$ pseudocauchy de type transcendant.

(i) : Il existe une unique valuation w sur $K(X)$ prolongeant v telle que $u \rightsquigarrow X$ dans $(K(X), w)$.

(ii) : $(K(X), w)$ est une extension immédiate de (K, v)

(iii) : Si (K', v') est une extension de (K, v) et y est un élément de K' tel que $u \rightsquigarrow y$ dans (K', v'), alors y est transcendant sur K et l'isomorphisme naturel de corps $K(X) \to K(y)$ est un isomorphisme de corps valués

$\star \star \star$

(i) : On définit w sur $K[X]$. Le prolongement à $K(X)$ se faisant alors suivant $w(\frac{P}{Q}) = w(P) - w(Q)$.

Soit $P \in K[X] - \{0\}$. Puisque u est de type transcendant sur (K, v), $v(P(u))$ est éventuellement constante, et on définit $w(P)$ comme cette constante éventuelle. Il est clair que w prolonge v et satisfait $(V1)$ et $(V2)$ sur $K[X]$, donc sur $K(X)$.

Soit $\rho_0 < \gamma$ tel que $\forall \rho_0 < \sigma < \lambda < \gamma$, $v(u_\lambda - u\sigma) = v(u_{\sigma+1} - u_\sigma)$. Il existe $\rho_0 < \rho_1 < \gamma$ tel que $\forall \rho_1 < \rho < \gamma$, $v(u_\rho - u_\sigma) = w(X - u_\sigma)$ est constante.

Or pour ρ_1 choisi suffisamment grand, on a aussi $\forall \rho_1 \rho < \gamma$, $v(u_\rho - u_\sigma) = v(u_{\sigma+1} - u_\sigma)$.

Or on peut choisir ρ_1 tel que $(v(u_{\sigma+1} - u_\sigma))_{\rho_1 < \sigma < \gamma}$ est strictement croissante, donc $(w(X - u_\sigma))_{\sigma < \lambda}$ est éventuellement strictement croissante, c'est-à-dire que $u \rightsquigarrow X$

L'unicité de w découlera du (iii).

(ii) : Par définition, w est à valeurs dans vK, et par surjectivité de $v : K^\times \to vK$, on a $wK(X) = vK$.

Soit $f \in K(X)^{\preceq 1}$. On veut montrer qu'il existe $a \in K$ tel que $w(f - b) > 0$, ainsi on aura $fw = aw$. Notons qu'il suffit de le montrer pour $f \in K[X]^{\preceq 1}$.

En effet, en écrivant $f = \frac{P}{Q}$ avec $P, Q \in K[X]$, on a il existe $\alpha < \lambda$ tels que $w(P) = v(P(u_\alpha))$ et $w(Q) = v(Q(u_\alpha))$.

$f = \frac{P(u_\alpha)}{Q(u_\alpha)} \frac{Q(u_\alpha)}{Q} \frac{P}{P(u_\alpha)}$ où $\frac{P(u_\alpha)}{Q(u_\alpha)} \in K$ et $\frac{P}{P(u_\alpha)}, \frac{Q}{Q(u_\alpha)} \in K[X]^{\preceq 1}$.

On a donc pour $p, q \in K$ satisfaisant $pv, qv = \frac{P}{P(u_\alpha)} w, \frac{Q}{Q(u_\alpha)} w, fw = \frac{P(u_\alpha)}{Q(u_\alpha)} \frac{p}{q} w$ avec $\frac{P(u_\alpha)}{Q(u_\alpha)} \frac{p}{q} \in K$.

On suppose donc que f est un polynôme.

D'après le corollaire qui précède, $f(u)$ est pseudocauchy, donc il existe $\rho_2 < \lambda$ tel que $\forall \rho_2 < \rho < \sigma < \gamma < \lambda$, $v(f(u_\gamma) - f(u_\sigma)) > v(f(u_\sigma) - f(u_\rho))$.

Si ρ_2 est choisi suffisamment grand, on a aussi $v(f(u_\sigma)), v(f(u_\rho)) = wf = 0$ donc $v(f(u_\sigma) - f(u_\rho)) \geq 0$, donc $v(f(u_\gamma) - f(u_\sigma)) > 0$.

On fixe maintenant un tel ordinal $\sigma > \rho_2$. Il existe $\rho_3 > \rho_2$ tel que pour $\gamma > \rho_3$, $w(f - f(u_\sigma)) = v(f(u_\gamma) - f(u_\sigma))$ étant de valuation éventuellement constante.

On peut donc poser $a = f(u_\sigma) \in K^{\preceq 1}$, on a $w(f - a) > 0$, ce qui conclut la preuve que $(K(X), w)$ est une extension immédiate de (K, v).

(iii) : Justifions tout d'abord que dans la configuration de l'énoncé, y est transcendant sur K.

On suppose le contraire : soit $P \in K[X]$ qui annule y. Le **lemme II.1** affirme que $P(u) \rightsquigarrow P(y)$. Or $P(y) = 0$ donc u est de type algébrique sur K (dans K' donc dans K), ce qui est contradictoire.

y est donc bien transcendant, et on dispose d'un isomorphisme de corps $j : K(X) \to K(y)$.

Il reste à voir que pour $f(y) \in K(y)$, $v'(f(y)) = w(f)$. Il suffit de le montrer pour $f(y) \in K[y]$.

Or toujours d'après le **lemme II.1**, $f(u) \rightsquigarrow f(y)$ dans K' donc $v(f(u)-f(y))$ est éventuellement strictement croissante.

Soit $\rho < \lambda$ tel que $\forall \rho < \sigma < \lambda, wf = v(f(u_\sigma))$.

Si on avait $\forall \gamma > \rho, \exists \sigma > \gamma$, $vf(u_\sigma) \neq vf(y)$, on aurait $\forall \gamma > \rho, \exists \sigma > \gamma, v(f(u_\sigma) - f(y)) \in \{vf(u_\sigma); vf(y)\} = \{wf; v(f(y))\}$, ce qui contredirait la stricte croissance éventuelle de $v(f(u) - f(y))$.

Donc il existe $\gamma > \rho$ tel que $vf(y) = vf(u_\sigma) \forall \sigma > \gamma$. On a alors pour $\sigma > \gamma, vf(u_\sigma) = wf$, donc $wf = vf(y)$, ce qui montre que j est un isomorphisme de corps valués.

Cela montre également que w est l'unique valuation sur $K(X)$ à satisfaire les conditions du (i).

$\star \star \star$

Voici maintenant l'analogue du théorème précédent dans le cas de type algébrique :

Théorème III.2

Soit (K, v) un corps valué, soit $u : \gamma \to K$ pseudocauchy de type algébrique, soit a une racine de Π_u.

(i) : Il existe une unique valuation w sur $K[a]$ prolongeant v telle que $u \rightsquigarrow a$ dans $(K[a], w)$, et telle que

(ii) : $(K[a], w)$ est une extension immédiate de (K, v).

(iii) : Si (K', v') est une extension de K et $y \in K'$ est pseudolimite de u dans (K', v'), alors tout isomorphisme de corps $K[a] \to K(b)$ sur K envoyant a sur b est un isomorphisme de corps valués.

$\star \star \star$

(i) : On définit w sur $K[a] = K[X]/(\Pi_u)$ (Π_u étant d'après irréductible sur K) en passant par $K_{\deg(\Pi_u)}[X]$:

Soit $P \in K_{\deg(\Pi_u)}[X]$. Puisque Π_u est le polynôme minimal de u et $\deg(P) < \deg(\Pi_u)$, $\neg(P(u) \rightsquigarrow 0)$ et $v(P(u))$ est éventuellement constante ; on définit $w(\overline{P})$ comme cette constante éventuelle. Pour $x \in K[a]$, wx est définie comme la valuation de l'unique élément de x de degré strictement inférieur à $\deg(\Pi_u)$.

-Montrons que w est bien une valuation sur $K[a]$:

Soient $x, y = P(a), Q(a) \in K[a]$ avec $\deg(P), \deg(Q) < \deg(\Pi_u)$.

On considère la division euclidienne de PQ par Π_u : $PQ = S\Pi_u + R$.

Notons que par minimalité de Π_u, les suites $v(P(u)), v(Q(u))$ et $v(R(u))$ sont constantes à partir d'un certain rang commun ρ_0.

On note dans l'ordre p, q, r ces constantes.

Soit $\rho_0 < \sigma < \lambda$.

$v(PQ(u_\sigma) = v(S\Pi_u(u_\sigma) + R(u_\sigma)$, avec $v(PQ(u_\sigma) = v(P(u_\sigma)) + v(Q(u_\sigma)) = p + q$.

Supposons qu'on ait $r \neq p + q$. ALors pour $\rho_0 < \sigma < \lambda$, $v(S\Pi_u(u_\sigma)) \geq r$.

Or $v(S\Pi_u(u_\sigma)) = v(S(u_\sigma)) + v(\Pi_u(u_\sigma))$ où le premier terme est éventuellement croissant en σ, et le second est éventuellement strictement croissant en σ, donc $v(S\Pi_u(u_\sigma))$ croît éventuellement strictement et il existe $\rho_1 < \lambda$ tel que $\forall \rho_1 < \sigma < \lambda, v(S\Pi_u(u_\sigma)) > r$, d'où $\forall \rho_1 < \sigma < \lambda, p+q = v(S\Pi_u(u_\sigma)+R(u_\sigma)) = v(S\Pi_u(u_\sigma))$, ce qui est impossible car le terme de gauche est constant tandis que le terme de droite croît strictement.

Donc $p + q = r$, c'est-à-dire que $v(P(a)) + v(Q(a)) = v(P(a)Q(a))$.

Le second axiome des valuations est trivialement vérifié par w car $K[a] \in x \to P \in x \cap K_{\deg(\Pi_u)-1}[X]$ est un morphisme de groupes additifs.

La preuve dans le théorème précédent que $u \rightsquigarrow X$ peut être reproduite ici pour conclure que $u \rightsquigarrow a$.

L'unicité de w découlera du (iii).

(ii) : Ici encore, on peut reprendre la preuve du (ii) dans le théorème précédent dans le cas particulier de $f \in K[X]$ avec $f(a) \preceq 1$.

(iii) : De même, on peut reproduire la preuve du troisième point du théorème précédent.

$\star \star \star$

Il faut remarquer que les cas algébrique n'est pas vraiment analogique au cas transcendant. On ne peut pas affirmer par exemple que si b est une racine de Π_u dans K', alors l'isomorphisme canonique $K[a] \to K[b]$ préserve la valuation. On ne peut même pas assurer que $v'b$ soit égal à wa. Cette obstruction a des conséquences importantes que l'on mentionnera plus loin.

Les propositions et théorèmes précédents possèdent des corollaires important que l'on liste ici :

Corollaire 1

Un corps valué est algébriquement maximal si et seulement si ses suites pseudocauchy pseudoconvergent.

$\star$

L'implication gauche==> droite découle par contraposition du théorème précédent, l'autre découle par contraposition de la **proposition III.2**.

⋆

Corollaire 2

Tout corps valué admet une extension immédiate algébrique algébriquement maximale.

⋆

Soit (K, v) un corps valué. On définit par induction un système inductif d'extensions immédiates algébriques de K.

On pose $(K_0, v_0) = (K, v)$. Soit α un ordinal tel que les $(K_\beta, v_\beta), \beta < \alpha$ aient été définis et ne soient pas algébriquement maximaux.

Si $\alpha = \beta + 1$, (K_β, v_β) n'étant pas algébriquement maximal, il admet d'après le corollaire précédent une suite pseudocauchy de type algébrique sans pseudolimite, et on peut donc produire une extension immédiate et algébrique (K_α, v_α) comme de (K_β, v_β) en utilisant la construction du **théorème III.2**.

Si α est limite, on définit (K_α, v_α) comme la limite inductive de $((K_\beta, v_\beta))_{\beta<\alpha}$. Cette limite est bien une extension immédiate et algébrique de (K, v).

Le procédé soit s'arrêter car les extensions algébriques se plongent dans la clôture algébrique, de cardinal limité.

Donc il existe un ordinal α tel que (K_α, v_α) est algébriquement maximale ; et c'est une extension algébrique maximale de (K, v) par construction.

⋆

Corollaire 3

Un corps valué est maximal si et seulement si toutes ses suites pseudocauchy ont des pseudolimites.

⋆

L'implication droite ==> gauche découle par contraposition de la **proposition III.1** théorème précédent et de la définition de la maximalité.

L'autre se montre par l'absurde : si (K, v) est maximal et u est une suite pseudocauchy de (K, v) sans limite dans (K, v), u est de type transcendant et alors le **théorème III.1** produit une extension immmédiate propre de (K, v), ce qui est contradictoire ; sinon, u est de type algébrique et similairement le **théorème III.2** produit une extension immédiate propre de (K, v) : contradictoire. Donc u admet une pseudolimite dans K.

⋆

Corollaire 4

Tout corps valué admet une extension immédiate maximale.

⋆

On construit une chaîne d'extensions immédiates en ajoutant inductivement des pseudolimites au corps de départ (K, v) grâce aux points (i) des théorèmes **III.1 et III.2** (selon le type de la suite pseudocauchy sans limite considérée). Si le procédé s'arrête, c'est que toute suite pseudocauchy admet une pseudolimite, et donc d'après le corollaire précédent, que l'extension finale (K', v') est maximale. Il suffit donc de prouver que ce procédé doit s'arrêter.

Or, d'après la **proposition III.1**, tout élément de (K', v') est limite d'une suite pseudocauchy de (K, v) ou est lui-même dans K. Donc $|K'|$ est inférieur au cardinal de l'ensemble des suites pseudocauchy ou constantes de (K, v).

Un élément y de $K' - K$ étant fixé, on peut choisir comme suite pseudocauchy de limite y une suite u telle que $v'(u - y)$ croît strictement, et donc telle que le domaine de $v'(u - y)$, qui est celui de u se plonge dans $v'K' = vK$.

En particulier, le domaine de u est un ordinal strictement inférieur à $|\Gamma|^+$. Donc à tout élément y de $K' - K$, on peut associer un élément de $|K|^{|\Gamma|^+}$, ce qui prouve que $|K'| = |K' - K| + |K| \leq |K|^{|\Gamma|^+} + |K| = |K|^{|\Gamma|^+}$.

Donc le procédé doit s'arrêter avant $|K|^{|\Gamma|^+ +}$.

⋆

On peut se demander si les extensions immédiates ou immédiates algébriques sont nécessairement uniques à isomorphisme de corps valués près, de sorte que l'on puisse envisager une structure commune aux corps valués maximaux / algébriquement maximaux. Là aussi, il n'y a pas unicité en général, mais Kaplansky a trouvé une hypothèse générale dans laquelle tous ces problèmes sont résolus par la positive. Dans ce rapport, on ne considèrera pas cette hypothèse, mais plutôt le cas très particulier d'équicaractéristique nulle, pour lequel de nombreuses distinctions subtiles disparaissent.

On peut maintenant noter que les corps valués de séries de Hahn sont maximaux :

Proposition III.4

$(C((t^\Gamma)), \lambda, v)$ est une extension immédiate maximale de son sous-corps valué des fractions de séries formelles finies.

⋆ ⋆ ⋆

Il est sous entendu que C est un corps, Γ est un groupe ordonné et $\lambda : (\Gamma)^2 \to C^\times$ est un cocycle.

Commençons par montrer que $(C((t^\Gamma)), \lambda, v)$ est maximal. En vertu de l'équivalence donnée par le **corollaire 3** précédent, il suffit de montrer que les suites pseudocauchy de ce corps valué pseudoconvergent.

Soit $u : \lambda \to C((t^\Gamma))$ une telle suite. ON va montrer que u admet une pseudolimite.

Pour $\rho < \lambda$, on note $\gamma_\rho = v(u_{\rho+1} - u_\rho)$.

Quitte à considérer un segment final de u, on peut supposer que $\forall \rho < \sigma < \mu < \lambda, v(u_\mu - u_\sigma) = \gamma_\sigma > v(u_\sigma - u_\rho) = \gamma_\rho$.

Notons que $\bigsqcup_{\rho<\lambda} [\gamma_\rho; \gamma_{\rho+1}[\cap (u_{\rho+1} - u_\rho)^{-1}(C^\times)$ est bien ordonné en tant qu'union bien ordonnée strictement croissante pour l'ordre strict induit par$<$ sur les parties de Γ de parties bien ordonnées de $(\Gamma, <)$.

On peut donc poser $f := u_0 + \sum_{\rho<\lambda} \sum_{\gamma_\rho \leq \gamma < \gamma_{\rho+1}} (u_{\rho+1} - u_\rho)_\gamma t^\gamma \in C((t^\Gamma))$, et considérer pour tout $\sigma < \lambda$,

$f^\sigma := u_0 + \sum_{\rho<\sigma} \sum_{\gamma_\rho \leq \gamma < \gamma_{\rho+1}} (u_{\rho+1} - u_\rho)_\gamma t^\gamma \in C((t^\Gamma))$.

On peut montrer par induction que $\forall \sigma < \lambda$, $f^\sigma + \sum_{\gamma \geq \gamma_\sigma} (u_\sigma - u_0)_\gamma t^\gamma = u_\sigma$ si σ est limite, et $f^{\sigma+1} + \sum_{\gamma \geq \gamma_\sigma} (u_\sigma - u_0)_\gamma t^\gamma = u_{\sigma+1}$.

Ainsi $\forall \sigma < \lambda, v(u_\sigma - f) \geq \min(v(u_\sigma - f^\sigma), v(f^\sigma - f)) \geq \gamma_{\sigma-1}$, $\sigma - 1$ désignant le précédesseur de σ si σ est successeur, et σ lui-même sinon.

Deux cas peuvent se produire : $v(u_\sigma - f) > \gamma_\rho \ \forall \rho$ éventuellement, auquel cas f est une pseudolimite de u (voir remarque (iii) des propriétés des suites pseudocauchy), ou bien $\forall \rho < \lambda, \exists \sigma > \rho, v(u_\sigma - f) > v(u_\rho - f)$, donc $v(u-f)$ n'est pas ultimement constante. Or, $u - f$ est pseudocauchy puisque u l'est et f est constante, donc $v(u - f)$ est éventuellement strictement croissante, c'est-à-dire que f est pseudolimite de u.

Cela prouve que $(C((t^\Gamma)), \lambda, v)$ est maximal.

Il est clair que le groupe de valeurs de $(C((t^\Gamma)), \lambda, v)$ est Γ, qui est aussi le groupe de valeurs du sous-corps des fractions de séries formelles finies.

En identifiant C au sous-corps de $(C((t^\Gamma)), \lambda)$ des fonctions nulles sur $\Gamma - \{0\}$, on obtient un isomorphisme de C sur le corps résiduel de $(C((t^\Gamma)), \lambda, v)$.

Puisque C est également contenu dans le sous-corps des fractions de séries formelles finies, cela montre que ce sous-corps valué est de corps résiduel naturellement isomorphe à C.

Donc $(C((t^\Gamma)), \lambda, v)$ est une extension immédiate de ce sous-corps.

$\star \star \star$

Montrons maintenant que comme annoncé, il n'y a pas en général unicité d'une extension immédiate maximale.

Remarque

Il existe un corps valué de groupe de valeur $(\mathbb{Z}^2, <)$ (ordre lexicographique) et de corps résiduel $\mathbb{F}_2$ qui possède deux extensions immédiates maximales non isomorphes en tant que corps.

Notons que $\mathbb{Z}^2$ est isomorphe au groupe G de Grothendieck de $(\omega^2, \oplus)$ où $\oplus$ est la somme de Hessenberg. On identifie l'élément (m, n) de $\mathbb{Z}^2$ à $\omega.m \oplus n$.

On considère le corps valué de séries de Hahn $\mathbb{F}_2((t^G))$, et on note K son sous-corps valué des fractions rationnelles en les t^γ, $\gamma \in G$.

Notons tout d'abord que toute extension immédiate (K', v') de K telle contenant des pseudolimites pour chaque suite pseudocauchy $x : \omega \to K$ telle que $\forall n \in \omega, x_{n+1} - x_n \in \mathbb{N}$ est de cardinal supérieur ou égal à $2^{\aleph_0}$. En effet, soit $x \in \{0;1\}^{\mathbb{N}}$. La suite des $x_n := \sum_{k=0}^{n} x(k)t^k$ satisfait les conditions donc elle admet une limite $\phi(x)$ dans K'. Pour $x, y \in \{0;1\}^{\mathbb{N}}$, de $\varphi(x) = \varphi(y)$, on déduit par inégalité triangulaire pour v' que pour $n \in \mathbb{N}$,

$v'(x_n - y_n) = v'(x_n - \varphi(x) + \varphi(y) - y_n) \geq \min(v(x_n - x_{n+1}), v(y_n, y_{n+1})) = (n+1)$.

En particulier, $x(n) = y(n)$, puis $x = y$. Ainsi, ϕ est injective, ce qui montre que $|K'| \geq 2^{\aleph_0}$.

Si toute suite satisfaisant les conditions K était de type algébrique, alors en ajoutant selon le **théorème III.2** une limite pour chacune de ces suites, on obtiendrait une extension algébrique immédiate de cardinal supérieur ou égal à $2^{\aleph_0}$. Or toute extension algébrique de (K, v) est dénombrable car K est dénombrable.

Donc (K, v) admet une suite $x : \omega \to K$ pseudocauchy de type transcendant telle que $\forall n \in \omega, v(x_{n+1} - x_n) \in \mathbb{N}$.

Soit u la suite $t^{-\omega}x$. u est pseudocauchy de type transcendant sur K, et $\forall n \in \mathbb{N}, v(u_{n+1} - u_n) < 0$.

Soit a une pseudolimite de u dans $\mathbb{F}_2((t^G))$ (on en trouve d'après la proposition précédente).

On note P_0 le polynôme $X^2 + X \in K[X]$, nul sur $\mathbb{F}_2$. P_0 induit un morphisme de groupe sur $\mathbb{F}_2((t^G))$. Puisque u est pseudocauchy de type transcendant sur K, $P_0(u)$ aussi, et $P_0(a)$ est pseudolimite de $P(u)$ dans $\mathbb{F}_2((t^G))$.

Soit $n \in \mathbb{N}$. $v(P_0(u_{n+1}) - P_0(u_n)) = v((u_{n+1} + u_n)^2 - (u_{n+1} + u_n))$.

Puisque $\forall n \in \mathbb{N}, v(u_{n+1} - u_n) = v(u_{n+1} + u_n) < 0$, $v((u_{n+1} + u_n)^2) = 2v(u_{n+1} + u_n) < v(u_{n+1} + u_n)$ et donc $v(P_0(u_{n+1}) - P_0(u_n)) = 2v(u_{n+1} + u_n) < 0 = v1$.

Ainsi, $P_0(a) + 1$ est également une pseudolimite de $P_0(u)$ dans $\mathbb{F}_2((t^G))$. On note $L := K(P(a))$. On va montrer que L admet deux extensions immédiates maximales.

Puisque $P_0(a)$ et $P_0(a) + 1$ sont tous deux pseudolimites dans $\mathbb{F}_2((t^G))$ de $P_0(u)$ qui est de type transcendant sur K, l'automorphisme f de L sur K qui envoie $P_0(a)$ sur $P_0(a) + 1$ est un automorphisme de corps valué.

Notons que a est une racine de $P_0 + P_0(a) \in L[X]$. Donc $b := f(a)$ est racine de $P_0 + P_0(a) + 1$, et on dispose d'un isomorphisme de corps valués $L[a] \to L[b]$.

Soient M, M' deux extensions immédiates maximales respectives de $L[a]$ et $L[b]$.

M et M' sont donc deux extensions immédiates maximales de L. Supposons M et M' isomorphes sur L en tant que corps, soit j un tel isomorphisme.

$0 = j(0) = j(P_0(a) + P_0(a)) = j(P_0)(j(a)) + j(P_0(a)) = P_0(j(a)) + P_0(a)$, donc $P_0(j(a)) = P_0(a)$.

Donc $P_0(j(a) + b) = P_0(j(a)) + P_0(b) = P_0(a) + P_0(a) + 1 = 1$.

C'est-à-dire que $j(a)+b$ est racine dans M' de l'équation entière $X^2+X+1 = 0$ à coefficients dans l'anneau de valuation de M'. Ce dernier étant intégralement clos dans M', il contient $j(a) + b$, et en passant au corps résiduel, cela produit une racine de $X^2 + X + 1$ dans $\mathbb{F}_2$, ce qui est contradictoire. Donc M et M' ne sont pas isomorphes en tant que corps sur L, ce qui conclut la preuve.

Cette preuve est largement inspirée de **[2], p.318, §5**.

IV - Corps valués henseliens

La notion que l'on présente ici est à la fois centrale en théorie des corps valués et facilement manipulable dans des contextes divers comme la géométrie algébrique, la théorie des corps ordonnés, la théorie des modèles. Elle possède également des spécifications aux structures de corps différentiels valués que l'on ne rencontrera cependant pas dans le rapport.

Les résultats de cette partie sont tirés de **[1], chap 3.3**.

Définition IV.1 : corps valués henseliens

Un corps valué (K, v) est dit **henselien** s'il vérifie la condition suivante :

$\forall P \in K^{\preceq 1}[X], \forall a \in K^{\preceq 1}$, si $P(a) \prec 1$ et $P'(a) \asymp 1$ alors il existe $x \in av$ tel que $P(x) = 0$.

La condition $P(a) \prec 1$ signifie que $P(a)v = 0$ dans le corps résiduel, c'est-à-dire que av est une racine de la projection dans Kv du polynôme P, aussi notée Pv. $P'(a) \asymp 1$ signifie que av est racine simple de Pv, ainsi le caractère henselien traduit le fait que les équations polynomiales ayant une solution singulière dans le corps résiduel ont une solution dans le corps tout entier.

Proposition IV.1

Dans la configuration précédente, la racine x de P dans av si elle existe est unique.

$\star \star \star$

Soit $x \in av$ tel que $P(x) = 0$.

Soit $\varepsilon \prec 1$. L'expansion de Taylor en x donne :

$P(x + \varepsilon) = P(x) + P'(x)\varepsilon + (\sum_{i \geq 0} P_{(i+2)}(x)\varepsilon^i)\varepsilon^2$ où $y := \sum_{i \geq 0} P_{(i+2)}(x)\varepsilon^i \preceq 1$.

Notons que $P(x) = 0$ et $P'(x)v = P(a)v \neq 0$ donc $P'(x)$ est inversible. Ainsi, on a :

$P(x + \varepsilon) = P'(x)\varepsilon + y\varepsilon^2 = P'(x)\varepsilon(1 + P'(x)^{-1}y\varepsilon)$ où $P'(x)^{-1}y\varepsilon \prec 1$ donc $(1 + P'(x)^{-1}y\varepsilon) \asymp 1$.

En particulier, $P(x + \varepsilon)$ s'annule si et seulement si $\varepsilon = 0$, donc sur av, P ne s'annule qu'en x.

$\star \star \star$

Lemme IV.1

Soit (K, v) un corps valué, soient $P \in K^{\preceq 1}[X]$ et $a \in K^{\preceq 1}$ tels que :

-$P(a) \prec 1$

-$P'(a) \asymp 1$

-P ne s'annule pas sur av.

Il existe une suite $(u_\alpha)_{\alpha < \gamma}$ pseudocauchy d'éléments de av sans pseudolimite dans K telle que $(P(u_\alpha))_{\alpha < \gamma} \rightsquigarrow 0$.

$\star \star$

Notons que pour $x \in K$, on a $P(a+x) = \sum_{i\geq 0} P_{(i)}(a)x^i = P(a) + xP'(a) + \sum_{i\geq 2} P^{(i)}(a)x^i$.

Ainsi, en posant $b = a - \frac{P(a)}{P'(a)}$, on a $P(b) = P(a)^2(\sum_{i\geq 0} \frac{P_{(i+2)}(a)}{P'(a)^{i+2}}x^i)$ où $\sum_{i\geq 0} \frac{P_{(i+2)}(a)}{P'(a)^{i+2}}x^i \preceq 1$.

Donc $P(b) \preceq P(a)^2$, où $P(a)$ est non nul car P ne s'annule pas sur av, donc $v(P(b)) \geq 2v(P(a)) > 0$.

On a également $v(b-a) = v(-\frac{P(a)}{P'(a)}) = v(P(a)) - v(P'(a)) = v(P(a)) > 0$. Cela implique en outre $b - a \prec 1$ donc $b \in av$ donc $(P(b)v, P'(b)v) = (P(a)v, P'(a)v)$ (car $P \in K^{\preceq 1}[X]$).

Ainsi, $P(b) \prec 1$ et $P'(b) \asymp 1$. C'est-à-dire que b satisfait les mêmes conditions que a par rapport à P, et on peut donc itérer cette construction.

On construit ainsi une suite $(u_\rho)_{\rho<\lambda}$ de av telle que $\forall \rho < \sigma < \lambda, v(u_\sigma - u_\rho) = v(P(u_\rho)) > 0$, $v(u_\sigma) \geq 2v(u_\rho) > 0$, $P(u_\sigma) \prec 1$ et $P'(u_\sigma) \asymp 1$.

-On pose $u_0 = a, u_1 = b$.

Soit β un ordinal tel que $(u_\rho)_{\rho<\beta}$ est construite.

-Si β est successeur d'un ordinal α, on pose $u_\beta := u_\alpha - \frac{P(u_\alpha)}{P'(u_\alpha)}$. Les conditions $P(u_\beta) \prec 1$ et $P'(u_\beta) \asymp 1$, $u_\beta \in av$ sont respectées par construction.

On a pour $\rho \leq \alpha < \beta$. Si $\rho = \alpha$ alors $v(u_\beta - u\rho) = v(P(u_\rho))$ par construction.

Sinon, $v(u_\beta - u_\rho) = v(u_\beta - u_\alpha + u_\alpha - u_\rho)$ où $v(u_\beta - u_\alpha) = v(P(u_\alpha)) \geq 2v(P(u_\rho)) > v(P(u_\rho)) = v(u_\alpha - u_\rho)$, donc $v(u_\beta - u_\rho) = v(u_\alpha - u_\rho) = v(P(u_\rho))$.

Il est clair que $v(P_(u_\beta)) \geq 2v(P(u_\rho))$. Ainsi, $(u_\rho)_{\rho<\beta+1}$ est bien construite.

-Si β est limite, alors $(u_\rho)_{\rho<\beta}$ est pseudocauchy. En effet, pour $\rho < \sigma < \gamma < \beta$, on a $v(u_\gamma - u_\sigma) = v(P(u_\sigma)) \geq 2v(P(u_\rho)) > v(P(u_\rho)) = v(u_\sigma - u_\rho)$.

Si $(u_\rho)_\beta$ n'admet pas de pseudolimite dans K alors le lemme est prouvé.

Sinon, on note u_β une pseudolimite de cette suite. $P(u_\rho) \underset{\rho<\beta}{\rightsquigarrow} P(u_\beta)$ donc par stricte-croissance de $(v(P(u_\rho)))_{\rho<\beta}$, on a $v(P(u_\beta)) \geq 2v(P(u_{\rho+1})) > v(P(u_\rho))\ \forall \rho < \beta$.

Pour $\rho < \beta$, on a de même que précédemment $v(u_\beta - u_\rho) = v(u_{\rho+1} - u_\rho) = v(P(u_\rho))$, ce qui implique que $u_\beta \in av$, puis que $P(u_\beta) \prec 1$ et $P'(u_\beta) \asymp 1$.

Ainsi, la suite $(u_\rho)_{\rho<\beta+1}$ est construite.

Par stricte croissance de $(v(P(u_\rho))_{\rho<\gamma}$ dans vK, la construction doit s'arrêter avant $|vK|^+$, et donc on dispose d'un certain ordinal limite γ tel que $(u_\rho)_{\rho<\gamma}$ est une suite pseudocauchy de av sans limite dans K telle que par construction, $(P(u_\rho))_{\rho<\gamma} \rightsquigarrow 0$.

$\star\ \star$

Théorème IV.1

Tout corps valué algébriquement maximal est henselien.

$\star \star \star$

Soit (K, v) algébriquement maximal. Soient $P \in K^{\preceq 1}[X], a \in K^{\preceq 1}$ tels que $Pv(av) = 0$ et $P'v(av) \neq 0$.

On a donc $P(a) \prec 1$ et $P'(a) \asymp 1$.

On suppose que P ne s'annule pas sur av. On peut appliquer le lemme précédent pour déduire l'existence d'une suite $(u_\rho)_{\rho<\gamma}$ pseudocauchy de av sans limite dans K et annulée par P.

Mais alors $(u_\rho)_{\rho<\gamma}$ est algébrique sur (K, v), donc elle admet d'après le **théorème III.2** une pseudolimite dans une extension algébrique immédiate de (K, v), qui est propre du fait que P ne s'annule pas sur av : cela contredit le caractère algébriquement maximal de (K, v).

Donc P s'annule sur av : (K, v) est henselien.

$\star \star \star$

Corollaire

Tout corps valué maximal est henselien, tout corps valué algébriquement clos est henselien.

On va maintenant montrer la réciproque dans le cas d'équicaractéristique nulle.

Lemme IV.2

Soit (K, v) henselien.

Soient $P \in K[X]$ et $a \in K$. On pose $\gamma := v(P(a)) - v(P'(a))$ (éventuellement, $\gamma = +\infty$). On suppose que $P'(a) \neq 0$ et $P(a) = 0$ ou $(P'(a) \neq 0$ et $\forall i \in \{2; ... \deg(P)\}$, $vP(a) < vP_{(i)}(a) + i.\gamma$.

On dit que P est en **configuration de Hensel** en a

Alors il existe un unique élément $b \in K$ tel que $vb \geq \gamma$ et $P(a + b) = 0$. De plus, $vb = \gamma$.

$\star \star \star$

-Si $P(a) = 0$, $b = 0$ fonctionne et est unique car alors $\gamma = +\infty$.

-Sinon, soit $g = \frac{P(a)}{P'(a)}$, et $Q := \frac{P((a+gX)}{P(a)}$.

$Q = 1 + X + \sum_{i \geq 2} P_{(i)}(a) g^i X^i$.

Pour $i \in \{2; ...; \deg(P)\}$, on a $v\frac{P_{(i)}(a)g^i}{P(a)} = vP_{(i)}(a) + i.\gamma - v(P(a)) > 0$.

On en déduit que $Q \in K^{\preceq 1}$, $Qv = X + 1$. Et (K, v) étant henselien, que Q admet une unique racine x dans $K^{\preceq 1}$.

$b := ug$ satisfait $P(a + b) = P(a)Q(u) = 0$ et $vb = vu + vg = 0 + \gamma = \gamma$.

De plus, pour $b' \in K$ tel que $P(a+b')=0$ et $vb' \geq \gamma$, on a $Q(\frac{b}{g}) = \frac{P(a+b)}{P(a)} = 0$ où $v\frac{b'}{g} \geq \gamma - \gamma = 0$ donc $\frac{b'}{g} \in K^{\preceq 1}$ et par unicité de la racine de Q dans $K^{\preceq 1}$, $\frac{b'}{g} = u$, donc $b' = b$, ce qui conclut la preuve.

$\star \star \star$

Lemme IV.3

Soit (K,v) un corps valué *d'équicaractéristique nulle*, soit $u : \lambda \to K$ une suite pseudocauchy admettant une pseudolimite a dans K.

Pour $\rho < \lambda$, on pose $\gamma_\rho := v(a-u_\rho)$. Soit d un nombre naturel, soit $P \in K_d[X]$ qui annule u et tel que pour $1 \leq i \leq d, P_{(i)}(u) \not\rightsquigarrow 0$.

Pour $2 \leq i \leq d$, on a éventuellement $vP(u_\rho) = v(P(u_\rho) - P(a)) = vP'(a) + \gamma_\rho < v(P_{(i)}(a) + \gamma_\rho)$.

$\star \star$

La preuve du **lemme III.1** appliquée à P fournit l'existence d'un unique entier $1 \leq i_0 \leq d$ tel que pour tout $1 \leq i \neq i_0 \leq d$,

$v(P(u_\rho) - P(a)) = vP_{(i_0)}(a) + i_0.\gamma_\rho < vP_{(i)}(a) + i.\gamma_\rho$ éventuellement.

Puisque $P(u) \rightsquigarrow 0$, $vP(u_\rho) = v(P(u_\rho) - P(a))$ éventuellement, ce qui donne pour $1 \leq i \neq i_0 \leq d$,

$vP(u_\rho) = vP_{(i_0)}(a) + i_0.\gamma_\rho < vP_{(i)}(a) + i.\gamma_\rho$ éventuellement.

Montrons que $i_0 = 1$. Soit $i > 1$. Il suffit de montrer que $vP'(a) + \gamma_\rho \leq vP_{(i)}(a) + i.\gamma_\rho$ éventuellement.

La preuve du **lemme III.1** appliquée à P' montre que pour $j \geq 1$, $v(P'(u_\rho) - P'(a)) \leq vP'_{(j)}(a) + j.\gamma_\rho$ éventuellement.

De même, puisqu'éventuellement $vP'(a) = vP'(u_\rho)$, on obtient $vP'(a) \leq vP'_{(j)}(a) + j.\gamma_\rho$ éventuellement.

(K,v) étant de caractéristique nulle, on a $P'_{(j)} = \frac{P'^{(j)}}{j!} = (j+1)\frac{P^{(j+1)}}{(j+1)!} = (j+1)P_{(j+1)}$.

Kv étant de caractéristique nulle, $v(j+1) = 0$, d'où $vP'(a) \leq vP_{(j+1)}(a) + j.\gamma_\rho$ éventuellement.

Puisque $i > 1$, on peut appliquer ceci à $j = i-1$ pour obtenir $vP'(a) + \gamma_\rho \leq vP_{(i)}(a) + i.\gamma_\rho$ éventuellement, ce qui conclut la preuve.

$\star \star$

Proposition IV.2

Soit (K,v) un corps valué *d'équicaractéristique nulle*, soit $u : \lambda \to K$ une suite pseudocauchy.

Pour $\rho < \lambda$, on pose $\gamma_\rho := v(a-u_\rho)$. Soit $P \in K[X]$ qui annule u et tel que pour $1 \leq i, P_{(i)}(u) \not\rightsquigarrow 0$.

Alors P est éventuellement en configuration de Hensel en u_ρ, et dans toute extension henselienne de K, il existe une unique racine de P pseudolimite de u.

$\star\star\star$

Soit (K', v') une extension de (K, v) possédant une pseudolimite a de P (voir le corollaire du **lemme III.1**). On a éventuellement $v'P_{(i)}(u_\rho) = v'P_{(i)}(a)$, donc le lemme précédent appliqué dans (K', v') montre que P est éventuellement en configuration de Hensel en u_ρ.

Soit (L, w) admet une extension henselienne (K, v).

Quitte à considérer un segment final de u, on peut supposer que $(\gamma_\rho)_{\rho<\lambda}$ est strictement croissante, que pour $\rho < \sigma < \lambda, v(u_\sigma - u_\rho) = \gamma_\rho$ et que $P'(u_\rho) \neq 0\ \forall \rho < \lambda$.

D'après les deux lemmes précédents, on peut également supposer que pour tout $\rho < \lambda$, il existe un unique élément b_ρ de L tel que $P(b_\rho) = 0$ et $w(u_\rho - b_\rho) = wP(u_\rho) - wP'(u_\rho)$.

D'après le lemme précédent, on peut également supposer que $\forall \rho < \lambda, wP(u_\rho) - wP'(u_\rho) = \gamma_\rho$, et donc $w(u_\rho - b_\rho) = \gamma_\rho$.

Par unicité des b_ρ, on a $b_\sigma = b_\rho$ pour $\sigma > \rho$. Ainsi, tous les b_ρ sont égaux à b_0 et l'égalité $w(u_\rho - b_\rho) = \gamma_\rho$ montre que b_0 est pseudolimite de u.

$\star\star\star$

Théorème IV.2

Un corps valué d'équicaractéristique nulle est henselien si et seulement s'il est algébriquement maximal.

$\star\star\star\star$

Le sens indirect est un cas particulier du **théorème IV.1**.

Montrons la réciproque.

Soit (K, v) un corps valué henselien, et soit $u : \lambda \to K$ pseudocauchy de type algébrique sur K.

(K, v) étant d'équicaractéristique nulle, pour $1 \leq i \leq \deg(\Pi_u)$, on a $-\infty < \deg(\Pi_{u(i)}) < \deg(\Pi_u)$ donc $\Pi_{u(i)}(u) \not\to 0$.

D'après la proposition précédente, (K, v) étant sa propre extension henselienne, Π_u est éventuellement en configuration de Hensel en u_ρ et il existe une unique pseudolimite a de u dans K qui est racine de Π_u.

En particulier, u admet une pseudolimite dans K. D'après le **corollaire 1 du théorème III.2**, K est algébriquement maximal.

$\star\star\star\star$

Comme nous l'avons suggéré, un corps valué peut admettre deux extensions immédiates algébriquement maximales non isomorphes. Le théorème qui suit

montre que la situation est bien plus rigide lorsque l'on affaiblit la condition de maximalité algébrique et qu'on la remplace par le caractère henselien.

Théorème IV.3

Soit (K, A) un corps valué. Il existe une extension henselienne (E, B) de (K, A) telle que tout plongement de (K, A) dans un corps valué henselien (L, V) se prolonge de manière unique en un plongement $(E, B) \longrightarrow (L, V)$.

Une telle extension est appelée **henselisé** de (K, A).

$\star \star \star \star$

Définition

Soit $\widetilde{K}$ une clôture algébrique de K. On choisit un anneau de valuation $\widetilde{A}$ de $\widetilde{K}$ qui domine A.

$(\widetilde{K}, \widetilde{A})$ est henselien car algébriquement clos, ainsi on peut considérer l'intersection E des sous-extensions henseliennes de K dans $\widetilde{K}$.

On pose $B = E \cap \widetilde{K}$. Il s'agit de montrer que (E, B) est un henselisé de (K, A).

Caractère henselien

Soit $P \in B[X]$, soit $a \in B$ tels que $P(a) \in m_B$ et $P'(a) \in B^\times$.

$(\widetilde{K}, \widetilde{A})$ étant henselien, P admet une unique racine b dans $a + m_{\widetilde{A}}$.

Soit $(K', K' \cap \widetilde{A})$ une extension henselienne de (K, A) dans $(\widetilde{K}, \widetilde{A})$.

De même, $B \subset K \cap \widetilde{A}$, donc P admet une racine b' dans $a + m_{K' \cap \widetilde{A}}$.

Mais alors $b' \in a + m_{\widetilde{A}}$, donc $b' = b$.

C'est-à-dire que b est dans K'. On en déduit que $b \in B$, et donc que $b \in a + m_B$, ce qui prouve que (E, B) est henselien.

Existence d'un prolongement

Il suffit de montrer que si (L, V) une extension henselienne de (K, A), il existe un plongement $(E, B) \longrightarrow (K, A)$ sur K. Quitte à considérer la clôture algébrique de K dans L, qui est henselienne par transitivité du caractère algébrique d'une extension, on peut supposer que L est algébrique sur K.

Soit $\widetilde{L}$ une clôture algébrique de L, et $\widetilde{V}$ un anneau de valuation sur $\widetilde{L}$ qui domine V.

D'après le corollaire de la **proposition II.4**, puisque $\widetilde{K}$ et $\widetilde{L}$ sont isomorphes en tant que clôtures réelles de K, il existe un isomorphisme $\sigma : (\widetilde{K}, \widetilde{A}) \longrightarrow ((\widetilde{L}, \widetilde{V})$ sur K.

$\sigma(E)$ est la plus petite sous-extension henselienne de K dans $\widetilde{L}$, donc en particulier, $\sigma(E) \subset L$.

Donc $\varphi := \sigma|_E$ est un plongement de corps valués $(E, B) \longrightarrow (L, V)$ sur K.

Unicité du prolongement

Soit $j : (E, B) \longrightarrow (L, V)$ un plongement sur K. On veut montrer que $j = \varphi$.

Posons $F := \{a \in E \mid j(a) = \varphi(a)\}$.

F est un sous-corps de E qui contient K. Il suffit donc de montrer que $(F, F \cap B)$ est henselien pour conclure que $F = E$ donc $j = \varphi$.

Soit $P \in F \cap B[X]$, soit $a \in F \cap B$ tels que $P(a) \in m_{F\cap B}$ et $P'(a) \in (F \cap B)^\times$.

(E, B) étant henselien, P admet une unique racine b dans $a + m_B$.

(L, V) étant henselien, $j(P)$ et $\varphi(P)$ admettent d'uniques racines c, d dans $j(a) + m_V, \varphi(a) + m_V$. Puisque $j(P)(j(b)) = 0 = \varphi(P)(\varphi(b))$ et $j(b), \varphi(b) \in j(a) + m_V, \varphi(a) + m_V$, on a $c, v = j(b), \varphi(b)$.

Or $j(P) = \varphi(P)$ car $P \in F[X]$, et $j(a) = \varphi(a)$ car $a \in F$, donc $c = d$, c'est-à-dire $j(b) = \varphi(b) : b \in F$.

Ainsi $b \in a + m_{F\cap B}$, ce qui montre que $(F, F \cap B)$ est henselien et conclut la preuve.

$\star \star \star \star$

Propriétés :

-Puisqu'un henselisé satisfait une propriété universelle, il est unique à unique isomorphisme sur (K, A) près, et on peut parler de l'henselisé de (K, A).

-Le **théorème IV.1** permet de déduire que l'henselisé d'un corps valué est un sous-corps valué de toutes ses extensions algébriquement maximales, et puisqu'en particulier tout corps valué admet une extension immédiate algébriquement maximale, que l'henselisé est une extension immédiate. Par ailleurs

-L'équivalence donnée par **théorème IV.2** montre que dans le cas d'équicaractéristique nulle, un henselisé est tout simplement une extension immédiate algébriquement maximale, et que la propriété universelle s'applique si l'on remplace "henselienne" par "algébriquement maximale".On parle alors de clôture algébriquement maximale.

V - Un théorème de structure

Le but de cette partie est de démontrer un théorème de structure pour les corps valués maximaux d'équicaractéristique nulle.

On travaillera donc principalement en équicaractéristique nulle.

Le théorème dans une version plus générale se trouve dans **[2], Theorem 6, p317**. Les preuves sont ici inspirées de **[1]**, **[2]** et **[3]**.

Proposition V.1

Deux extensions immédiates maximales d'un même corps valué d'équicaractéristique nulle sont isomorphes sur K.

$\star \star \star$

Soit (K, A) valué d'équicaractéristique nulle, soient (L, V), (F, B) deux extensions immédiates maximales de K.

Soit X l'ensemble des triplets (L', F', j) où L', F' sont des sous-extensions de K respectivement dans L, F, et j est un isomorphisme $(L', L' \cap V) \longrightarrow (F', F' \cap B)$ sur K.

On munit X de l'inclusion triple $(\subset, \subset, \subset)$.

X contient (K, K, id_K) donc il n'est pas vide.

X est stable par unions de chaînes, donc d'après le lemme de Zorn, X admet un élément maximal (L_0, F_0, j_0).

Supposons que $L_0 \neq L$.

(L, V) est maximal donc algébriquement maximal, donc henselien.

-Si $(L_0, L_0 \cap V)$ n'est pas henselien, alors sa clôture henselienne L_h (plongée de manière unique dans (L, V)) dans (L, V) est une extension propre.

D'après le **théorème IV.3**, j_0 se prolonge en un isomorphisme de corps valués $j_h : L_h \to F_h$, F_h étant la clôture henselienne de F_0 dans (F, B).

On a alors $(L_0, F_0, j_0) < (L_h, F_h, j_h)$, ce qui est contradictoire.

Ainsi, L_0 est henselien.

-Soit $x \in L - L_0$.

Notons que $(L_0, L_0 \cap V)$ est d'équicaractéristique nulle, donc d'après le **théorème III.2**, il est algébriquement maximal.

L étant une extension immédiate de (K, A), c'est une extension immédiate de $(L_0, L_0 \cap V)$, donc d'après la **proposition III.1**, x est pseudolimite d'une suite pseudocauchy u de $(L_0, L_0 \cap V)$. D'après le **corollaire 3 du théorème III.2**, $(L_0, L_0 \cap V)$ n'est pas maximal.

Notons que $(L_0, L_0 \cap V)$ est d'équicaractéristique nulle, donc d'après le **théorème III.2**, il est algébriquement maximal ; ainsi, u est de type transcendant.

$j_0(u)$ est donc de type transcendant sur F_0, et par maximalité de (F, B), elle admet une pseudolimite y dans F. Le **théorème III.1** affirme alors que y est transcendant sur F_0 et que l'on peut prolonger j_0 en un isomorphisme $(L_0(x), L_0(x) \cap V) \longrightarrow (F_0(y), F_0(y) \cap B)$, ce qui contredit encore une fois la maximalité de (L_0, F_0, j_0).

Donc $L_0 = L$, de même $F_0 = F$: finalement (L, V) et (F, B) sont isomorphes sur K via j_0.

$\star \star \star$

Cette rigidité permet de parler de la clôture maximale d'un corps valué d'équicaractéristique nulle, qui n'est alors qu'une extension immédiate maximale. Il faut prendre garde tout de même au fait qu'en général, plusieurs clôtures maximales peuvent exister, comme le montre la remarque de la fin de la partie III.

Par ailleurs, même dans le cas d'équicaractéristique nulle, la clôture maximale ne possède pas la propriété universelle initiale. En fait, la preuve précédente permet de produire plusieurs isomorphismes sur (K, v) entre deux clôtures maximales de (K, v) : il suffit étant données les premières extensions $E(x), E(y)$ de l'henselisé de K dans L, F de considérer les isomorphismes $j_0, j_1 : K(x) \to K(y)$ envoyant respectivement x sur y et x sur $y+1$. Le lemme de Zorn produit alors un élément maximal (L, F, i_0) prolongeant j_0 et un autre (L, F, i_1) prolongeant j_1, et les deux isomorphismes sont bien distincts.

On veut montrer que les corps valués maximaux d'équicaractéristique nulle sont semblables aux corps valués de séries de Hahn. Dans ces derniers, on trouve en le sous-corps des constantes un sous-corps isomorphe à leur corps résiduel via l'application résidu (on parle d'un relèvement du corps résiduel), et un ensemble de monômes qui à cocycle près définit une section de la valuation. Il s'agit donc de mettre en évidence ces deux propriétés dans les corps valués maximaux d'équicaractéristique nulle.

Lemme V.1

Soit (K, v) un corps valué admettant un sous-corps maximal C de $K^{\preceq 1}$
(i) : C est algébriquement clos relativement à K.
(i) : Kv/Cv est algébrique.

$\star \star \star$

(i) : $K^{\preceq 1}$ est intégralement clos dans K, et il contient une clôture algébrique de C dans K. Par maximalité de C comme sous-corps de $K^{\preceq 1}$, C est algébriquement clos dans K.

(ii) : Supposons qu'il existe $y = xv \in Kv$ transcendant sur Cv.

$C[x]$ se plonge dans $Kv[y]$. En effet, pour $P \in C[X]$ non nul, Pv est non nul ($C \cap K^{\prec 1} = \{0\}$ car C est stable par inversion, et donc $cd(Pv) \neq 0$), et en particulier, Pv n'annule pas y, donc $P(x)v \neq 0$.

C'est-à-dire que $\forall Q(x) \in C[x], v(Q(x)) = 0$. Donc $\forall Q_1(x), Q_2(x) \in C[x], Q_2(x) \neq 0$, $v(\frac{Q_1(x)}{Q_2(x)}) = 0$, et donc $C(x) \subset K^{\preceq 1}$. Or C est un sous-corps propre de $C(x)$,

ce qui contredit la maximalité de C.

Ainsi, Cv est algébriquement clos dans Kv.

$\star\star$

On en déduit l'existence de relèvements pour les corps valués d'équicaractéristique nulle ordonnés et henseliens.

Proposition V.2

Si (K,v) est henselien d'équicaractéristique nulle, alors $K^{\preceq 1}$ admet un sous-corps maximal, et tout sous-corps maximal de $K^{\preceq 1}$ est un relèvement de Kv.

$\star\star\star$

Notons tout d'abord que (K,v) étant dans les deux cas d'équicaractéristique nulle, $K^{\preceq 1}$ admet un sous-corps isomorphe à $\mathbb{Q}$ et par Zorn, il admet un sous corps maximal. On en fixe un que l'on note C.

Soit $y = xv \in Kv$.

D'après le **lemme V.1**, y possède un polynôme minimal $\Pi_y \in Cv[X]$. Π_y est séparé car irréductible en caractéristique nulle.

Soit P un relèvement de Π_y dans $C[X]$.

y est racine simple de $Pv = \Pi_y$ donc par henseliannité de (K,v), P admet une racine $x' \in x + K^{\prec 1} \subset K^{\preceq 1}$.

C étant algébriquement clos dans $K^{\preceq 1}$, $x' \in C$, et donc $y \in Cv$.

Donc $Cv = Kv$: C est un relèvement de Kv.

$\star\star\star$

Définition V.1

Soit (K,v) un corps valué. Un **groupe monomial** de (K,v) est un sous-groupe de $(K^\times,\times)$ isomorphe à vK.

De manière équivalente, c'est l'image d'une section de la valuation v vu comme un morphisme de groupes $(K^\times,\times) \to (vK,+)$.

Proposition V.3

Soit (K,v) un corps valué. Soit G un sous-groupe divisible de $K^\times$ tel que $vG = vK$. G contient un sous-groupe monomial de (K,v).

$\star\star\star$

Notons que l'on dispose de la suite exacte courte suivante :

$0 \longrightarrow G \cap K^{\preceq 1} \xrightarrow{\subseteq} G \xrightarrow{v} vK \longrightarrow 0$.

$G \cap K^{\preceq 1}$ est divisible : pour $n \in \mathbb{N}, g \in G \cap K^{\preceq 1}$, $\exists \delta \in G, \delta^n = g$ et $v(\delta) = \frac{1}{n}.v(g) \geq 0$ donc $\delta \in G \cap K^{\preceq 1}$.

G étant divisible, $G \cap K^{\preceq 1}$ est divisible, donc d'après la **proposition I.1**, il est injectif dans la catégorie des groupes abéliens.

Ainsi, en appliquant la définition de l'injectivité dans une catégorie abélienne avec $A = B = G \cap K^{\preceq 1}$ et $C = G$, on obtient une section de l'inclusion $G \cap K^{\preceq 1} \hookrightarrow G$, la suite est scindée, et on en déduit l'existence d'une section de $v : G \to vK$, dont l'image est un groupe monomial de (K, v) inclus dans G.

$\star \star \star$

En général, la preuve du lemme étant non constructive, on ne dispose pas d'un groupe monomial explicite pour (K, v). On peut noter qu'en vertu de cette proposition les corps réels clos valués et les corps algébriquement clos valués admettent un groupe monomial.

Ce n'est pas nécessairement le cas pour les corps valués henseliens, cependant on peut leur trouver un groupe monomial "à cocycle près" :

Proposition V.4

Soit (K, v) henselien d'équicaractéristique nulle.

On fixe un relèvement C, algébriquement clos dans K, de son corps résiduel.

Il existe un cocycle $\lambda : (vK)^2 \longrightarrow C^\times$ et une application $t : \Gamma \to C^\times$ tels que $v \circ t = id_\Gamma$ et $\forall \alpha, \beta \in \Gamma, t^\alpha t^\beta = \lambda(\alpha, \beta) t^{\alpha + beta}$.

$\star \star \star$

On se donne une base rationnellement indépendante B de vK. (**proposition I.2**)

-Pour chaque élément γ de B, on fixe t^γ dans $v^{-1}(\{\gamma\})$.

-Pour $\alpha = \sum_i x_i \gamma_i \in vK$, combinaison linéaire à coefficients entiers des $\gamma_i \in B$, on pose $t^\alpha := \prod_i (t^{\gamma_i})^{x_i}$.

-Soit $\alpha = \sum_i \frac{x_i}{y_i} \gamma_i \in vK$, combinaison linéaire à coefficients rationnels des $\gamma_i \in B$. On note $r = \bigvee_i y_i$, de sorte que $\alpha = \frac{1}{r}.(r.\alpha)$ où $r.\alpha$ est une combinaison linéaire à coefficients entiers des γ_i. On dispose ainsi de $t^{r.\alpha}$.

Soit $z \in K$ tel que $\alpha = vz$. $vz^r = r.\alpha = vt^{r.\alpha}$ donc $v\frac{z^r}{t^{r.\alpha}} = 0$.

Ainsi, $\exists a \in C^\times$ tel que $av = \frac{z^r}{t^{r.\alpha}} v$.

Soit $P = \frac{z^r}{at^{r.\alpha}} X^r - 1 \in K^{\preceq 1}[X]$.

$Pv = X^r - 1$ admet la racine simple 1. (K, v) étant henselien, P admet une racine b dans $K^{\preceq 1}$.

On pose $t^\alpha := zb$, de sorte que $(t^\alpha)^r = at^{r.\alpha}$.

Soient $\alpha, \beta \in vK$. On fixe des entiers r, s, u tels que $r.\alpha, s.\beta, u.(\alpha+\beta)$ sont des combinaisons linéaires à coefficients entiers d'éléments de B.

Il existe $a, b, c \in C$ tels que $(t^\alpha)^r = at^{r.\alpha}$, $(t^\beta)^s = bt^{s.\beta}$ et $(t^{\alpha+\beta})^u = ct^{u.(\alpha+\beta)}$.

Donc $(\frac{t^\alpha t^\beta}{t^{\alpha+\beta}})^{rsu} = a^{su}b^{ru}c^{-rs} \in C$.

C étant algébriquement clos dans K, $\frac{t^\alpha t^\beta}{t^{\alpha+\beta}} \in C$.

On définit donc un cocycle satisfaisant les conditions en posant pour $(\alpha, \beta) \in (vK)^2$, $\lambda(\alpha, \beta) := \frac{t^\alpha t^\beta}{t^{\alpha+\beta}} v$.

Par construction, on a bien $v \circ t = id_\Gamma$.

$\star \star \star$

Voici enfin le théorème de structure :

Théorème V.1

(i) : Soit (K, v) valué maximal d'équicaractéristique nulle. Il existe un cocycle $\lambda : (\Gamma)^2 \to Kv^\times$ et une application $t : vK \to (Kv)^\times$ tels que $v \circ t = id_{vK}$ et (K, v) est naturellement isomorphe au corps valué des séries de Hahn $(Kv((t^{vK})), \lambda, w)$.

(ii) : Si de plus (K, v) admet un groupe monomial, alors on peut choisir $\lambda \equiv 1$.

$\star \star \star \star$

(i) (K, v) étant maximal, il est algébriquement maximal donc henselien. D'après la **proposition V.3**, on peut choisir un relèvement C de Kv et d'après la **proposition V.4**, on peut choisir un cocycle λ

(K, v) est une extension immédiate de son sous-corps valué F engendré par $t(vK)$ et C, car celui-ci contient C ainsi que les $t^\alpha, \alpha \in vK$ dont les valuations épuisent vK.

On a vu avec la **proposition III.4** que $(C((t^{vK})), \lambda, w)$ est également une extension immédiate maximale de ce corps valué (à isomorphisme près), donc d'après la **proposition V.1**, ces deux corps valués sont isomorphes sur F. C'est ce que l'on entend par "naturellement isomorphe" ; il faut faire attention cependant au fait que les existences de λ et t sont des résultats non constructifs en général.

C étant naturellement isomorphe à Kv, on obtient le résultat tel qu'énoncé.

(ii) : Si de plus (K, v) admet un sous-groupe monomial, alors la section t correspondante permet de choisir $\lambda \equiv 1$.

$\star \star \star \star$

VI - Algorithme de Newton

Dans toute cette partie, on fixe un corps valué (K, v), et un polynôme $P = \sum_{i=1}^{r} a_i X^i \in K[X]$ avec $a_r \neq 0$. On notera $\Gamma := vK$, $A := K^{\preceq 1}$ et $k := Kv$.

On fixe une partie $\mathcal{M}$ de $K^\times$ telle que la restriction de $v : \mathcal{M} \to \Gamma$ est bijective, et on note s sa réciproque. Les éléments de $\mathcal{M}$ seront appelés monômes.

On va présenter un algorithme appelé **algorithme de Newton** permettant de déterminer les racines de P dans K en utilisant la valuation pour ramener la difficulté de trouver les racines dans le corps résiduel. Cet algorithme n'est donc utile que si le corps résiduel possède des propriétés algébriques permettant d'y résoudre certaines équations polynômiales. Les résultats jusqu'au **lemme VI.4** figurent à quelques détails près dans **[1], chap 3.7**. L'algorithme à proprement parler est une façon comme une autre de les mettre en pratique.

Le dernier paragraphe est une application de cet algorithme à une équation simple.

Définition VI.1

Soit $Q = \sum_{i=1}^{n} q_i X^i \in K[X]$ non nul. Soit $x \in K$

-On note δ_Q et on appelle **monôme dominant** de Q l'élément $s(\min(\{va_i \mid \leq i \leq n\}))$.

-Par construction, $\frac{1}{\delta_Q} Q \in A[X]$. On note $D_Q := \frac{1}{\delta_Q} Qv \in k[X]$.

-On note $Q_{+x} := Q(X + x)$, et $Q_{\times x} := Q(xX)$.

-On note $mul(Q)$ et on appelle **multiplicité** de Q en 0 la plus grande puissance de X qui divise Q.

-On note $ddeg(Q)$ et on appelle **degré dominant** de Q le degré de D_Q.

-On note $dmul(Q)$ et on appelle **multiplicité dominante** de Q la multiplicité de D_Q en 0.

Quelques remarques :

-D_Q n'est jamais nul.

-On a $Q_{+x} = \sum_{i=0}^{n} Q_{(i)}(x)X^i$, et $Q_{\times x} = \sum_{i=0}^{n} (q_i x^i)X^i$. En particulier, $\deg(Q_{+x}), \deg(Q_{\times x}) = \deg(Q)$ et $mul(Q_{\times x}) = mul(Q)$.

-$0 \leq ddeg(Q) \leq \deg(Q)$ et $mul(Q) \leq dmul(Q) \leq \deg(Q)$.

Lemme VI.1

Soient $\mathfrak{m} \prec \mathfrak{n} \in \mathcal{M}$.

On q $dmul P_{\times \mathfrak{m}} \leq ddeg(P_{\times \mathfrak{m}}) \leq dmul(P_{\times \mathfrak{n}}) \leq ddeg(P_{\times \mathfrak{n}})$.

$\star\ \star$

On a toujours $mul(Q) \leq \deg(Q)$ si Q est un polynôme non nul, il suffit donc de montrer que $ddeg(P_{\times \mathfrak{m}}) \leq dmul(P_{\times \mathfrak{n}})$.

On note $d = dmul(P_{\times \mathfrak{n}})$. Soit $i > d$.

Si on avait $va_i\mathfrak{n}^i < va_d\mathfrak{n}^d$, on aurait $\delta_{P_{\times n}} \succeq a_i\mathfrak{n}^i \succ a_d\mathfrak{n}^d$ donc le coefficient de degré d de $\frac{1}{\delta_{P_{\times \mathfrak{n}}}} P_{\times \mathfrak{n}}$ serait dans m_A, et donc son résidu serait nul.

Mais alors, par définition de d, les coefficients jusqu'au degré d de $D_{P_{\times \mathfrak{n}}}$ seraient nuls ce qui contredirait la définition de d.

Donc $a_i\mathfrak{n}^i \preceq a_d\mathfrak{n}^d$.

On a donc $a_i\mathfrak{m}^i = (a_i\mathfrak{n}^i)\frac{\mathfrak{m}^i}{\mathfrak{n}^i}$, et puisque $\frac{\mathfrak{m}^i}{\mathfrak{n}^i} \prec 1$ et $i >$d, on obtient $a_i\mathfrak{m}^i \prec (a_i\mathfrak{n}^i)\frac{\mathfrak{m}^d}{\mathfrak{n}^d} \preceq (a_d\mathfrak{n}^d)\frac{\mathfrak{m}^d}{\mathfrak{n}^d} = a_d\mathfrak{m}^d$.

Pour la même raison que précédemment, le coefficient de degré i de $D_{P_{\times \mathfrak{m}}}$ est nul. Puisque c'est vrai pour tout $i > d$, on a $ddeg(P_{\times \mathfrak{m}}) \leq d$.

$\star\ \star$

Définition VI.2

Un **zéro approché** de P est un élément $y \in K$ tel que $vP(y) > \min(\{va_iy^i \mid 0 \leq i \leq r\})$.

Un **monôme spécial** de P est un élément $\mathfrak{m} \in \mathfrak{M}$ tel que $D_{P_{\times \mathfrak{m}}}$ possède au moins deux coefficients non nuls.

Proposition VI.1

(i) : Si $y \in K$ est un zéro approché de P, alors y est non nul et $\mathfrak{m} := s(vy)$ est un monôme spécial de P et $\frac{y}{\mathfrak{m}}v$ est un zéro de $D_{P_{\times \mathfrak{m}}}$.

(ii) : Si $z \sim y$, alors z est également un zéro approché de P.

(iii) : Toute racine non nulle P en est un zéro approché.

$\star\ \star\ \star$

Soit $y \in K$ un zéro approché de P

(i) : Puisque $vP(0) = va_0$ et $\min(\{va_i 0^i \mid 0 \leq i \leq r\}) = va_0$, 0 n'est pas un zéro approché de P, donc y est non nul.

On peut donc considérer $\mathfrak{m} := s(vy)$. $v\mathfrak{m} = vy$ par définition de s donc $\frac{y}{\mathfrak{m}} \in A$ et on peut considérer son résidu.

$D_{P_{\times \mathfrak{m}}}(\frac{y}{\mathfrak{m}}v) = \sum_{i=0}^{r} \frac{a_i \mathfrak{m}^i y^i}{\delta_{P_{\times \mathfrak{m}}} \mathfrak{m}^i} v = \sum_{i=0}^{r} \frac{a_i y^i}{\delta_{P_{\times \mathfrak{m}}}} v = \frac{1}{\delta_{P_{\times \mathfrak{m}}}} P(y)v.$

Or $v\frac{1}{\delta_{P_{\times \mathfrak{m}}}} P(y) = vP(y) - v(s(\min(\{va_j \mathfrak{m}^j \mid 0 \leq j \leq r\}))) = vP(y) - \min(\{va_j \mathfrak{m}^j \mid 0 \leq j \leq r\}) = vP(y) - \min(\{va_j y^j \mid 0 \leq j \leq r\}) > 0$ par définition de la qualité de zéro approché.

On peut noter ici qu'il y a équivalence entre le fait que y soit zéro approché et que y soit non nul, avec $\frac{y}{s(vy)}v$ racine de $D_{P_{\times s(vy)}}$.

Donc $\frac{1}{\delta_{P_{\times \mathfrak{m}}}} P(y)v = 0$: $\frac{y}{\mathfrak{m}}v$ est racine de $D_{P_{\times \mathfrak{m}}}$.

(ii) : Soit $z \sim y$. z n'est donc pas nul.

$vz = vy$ donc $s(vy) = \mathfrak{m}$. De plus, $v(\frac{z}{s(vz)} - \frac{y}{s(vy)}) = v(z - y) - vz > 0$ par définition de l'équivalence forte, donc $\frac{z}{s(vz)}v = \frac{y}{s(vy)}v$ est une racine de $D_{P_{\times s(vz)}}$, ce qui montre d'après l'équivalence mentionnée dans la preuve du (i) que z est un zéro approché de P.

(iii) : Si $P(z) = 0$ et $z \neq 0$, alors $vP(z) = +\infty > va_n z^n$, donc z est un zéro approché de P.

$\star \star \star$

On cherche donc les racines non nulles de P parmi ses zéros approchés. L'outil géométrique que l'on va maintenant construire permet entre autre de localiser "graphiquement" les zéros approchés d'un polynôme.

Définition VI.3 : Diagramme de Newton

On considère l'enveloppe divisible $\mathbb{Q}\Gamma$ de Γ.

On voit $\mathbb{N} \times \mathbb{Q}\Gamma$ comme un ensemble de points.

Pour $\beta \in \mathbb{Q}\Gamma$, on note L_β l'application $\mathbb{N} \times \mathbb{Q}\Gamma \to \mathbb{N} \times \mathbb{Q}\Gamma$ donnée par $L_\beta(i, \gamma) = \gamma + i.\beta$.

-On appelle **droite** de $\mathbb{N} \times \mathbb{Q}\Gamma$ une partie L de $\mathbb{N} \times \mathbb{Q}\Gamma$ telle qu'il existe $(\beta, \delta) \in \mathbb{Q}\Gamma \times \Gamma$ tel que $L = L_\beta^{-1}(\{\delta\})$.

Une droite étant donnée, les paramètres β, δ correspondants sont déterminés, on les appelle respectivement **antipente** et **ordonnée à l'origine** de L, et on note $L = L_{\beta,\delta}$.

-Un point (i, γ) de $\mathbb{N} \times \mathbb{Q}\Gamma$ est **au dessus de** la droite $L_{\beta,\delta}$ si $L_\beta(i, \gamma) > \delta$, **en dessous de** $L_{\beta,\delta}$ si $L_\beta(i, \gamma) > \delta$, **sur** $L_{\beta,\delta}$ si $L_\beta(i, \gamma) = \delta$.

-Le diagramme de Newton de P est la partie $\mathcal{N}(P) := \{(i, va_i) \mid 0 \leq i \leq r\}$ de $\mathbb{N} \times \mathbb{Q}\Gamma$.

-Une **arête** de $\mathcal{N}(P)$ est une droite de $\mathbb{N} \times \mathbb{Q}\Gamma$ contenant deux points de $\mathcal{N}(P)$, et telle que tous les points de $\mathcal{N}(P)$ sont au dessus de ou sur L.

-Une antipente de $\mathcal{N}(P)$ est un élément de Γ qui est l'antipente d'une arête de $\mathcal{N}(P)$.

-L'abscisse gauche (resp. droite) d'une arête L de $\mathcal{N}(P)$ est le plus petit entier (resp. plus grand entier) $0 \leq i \leq r$ tel que $(i, va_i) \in L$. On les notes g_L et d_L.

Convexité du diagramme

(i) : Deux arêtes distinctes de $\mathcal{N}(P)$ ont des antipentes différentes.

En effet, soit $\beta \in \mathbb{Q}\Gamma$ une antipente commune aux arêtes $L_{\beta,\delta}$ et $L_{\beta,\delta'}$ de $\mathcal{N}(P)$.

Soit (i, va_i) un point de $L_{\beta,\delta}$. (i, va_i) est au dessus de ou sur $L_{\beta,\delta'}$ donc $va_i + i.\beta = \delta \geq \delta'$.

De même, $\delta' \geq \delta$, donc $\delta = \delta'$ et $L_{\beta,\delta} = L_{\beta,\delta'}$.

(ii) : Si L, L' sont deux arêtes de $\mathcal{N}(P)$ d'antipentes respectives $\beta < \beta'$, alors $d_{L'} \leq g_L$, c'est-à-dire que l'antipente diminue de gauche à droite, ou encore que la pente augmente de gauche à droite, ce qui revient en conjonction avec (i) à dire que la figure formée par les arêtes de $\mathcal{N}(P)$ est convexe.

En effet, si $(i, va_i) \in L$ et $(j, va_j) \in L'$, en notant δ, δ' les ordonnées à l'origine, on a :

$va_i + i.\beta = \delta$

$va_j + j.\beta' = \delta'$

$va_i + i.\beta' \geq \delta'$

$va_j + j.\beta \geq \delta$.

Donc $va_i + i.\beta \leq va_j + j.\beta$ et $va_j + j.\beta' \leq va_i + i.\beta' \geq \delta'$, d'où :

$(i-j).\beta \leq va_j - va_i \leq (i-j).\beta'$, puis $0 \leq (i-j).(\beta' - \beta)$ où $\beta' - \beta > 0$.

On en déduit que $(i-j) \geq 0$, donc $j \leq i$, et en particulier, $d_{L'} \leq g_L$.

Voici un exemple de diagramme de Newton. Il s'agit de celui de

$P_0 := \frac{1+t}{t^2+1}X^6 - \frac{3}{t-1}X^5 + 2tX^4 - (t+2)X^3 + \frac{t^2+t+1}{t+1}X^2 + \frac{1}{t^4-3t^2+1}X - \frac{7t^2-3}{2t^6+t^5+1}$.

dans $K = \mathbb{R}(t)[X]$, $v\frac{P(t)}{Q(t)} := \deg(Q) - \deg(P)$. ($\Gamma = \mathbb{Z}$ et $k = \mathbb{R}$).

Les points représentent les points de $\mathcal{N}(P_0)$, les segments représentent les arêtes de $\mathcal{N}(P_0)$. Elles sont ici au nombre de 3, et les antipentes correspondantes, qui sont les opposés des pentes géométriques de ces portions de droites, valent $\frac{3}{2}, 0$ et 1 de gauche à droite. A noter que la première n'appartient pas à Γ ; nous verrons que c'est une obstruction à ce que P_0 admette un grand nombre de racines dans K.

Le lien entre le diagramme de Newton et les zéros approchés est étudié dans la proposition suivante. Tout d'abord, notons les faits suivants :

-Si $L = L_{\beta,\delta}$ est une arête de $\mathcal{N}(P)$, alors tous les points de $\mathcal{N}(P)$ sont au dessus de ou sur L, donc $\delta \leq \min_i va_i + i.\beta$.

De plus, L contient un point de $\mathcal{N}(P)$ donc $\delta = \min_i va_i + i.\beta$.

-Si $\beta \in \Gamma$, alors $\beta = vs(\beta)$ donc $\delta = \min_i va_i + i.\beta = \min_i va_i s(\beta)^i = v\delta_{P_{\times s(\beta)}}$.

On note P_β le polynôme $Q_{P_{\times s(\beta)}}$ de $k[X]$, de sorte que $Q_{P_{\times s(\beta)}} = \frac{1}{\delta_{P_{\times s(\beta)}}} P_{\times s(\beta)} v = \frac{1}{s(\delta)} P_{\times s(\beta)} v$.

Proposition VI.2

(i) : L'antipente β d'une droite L est dans Γ, alors L est une arête de $\mathcal{N}(P)$ si et seulement si $s(\beta)$ est un monôme spécial de P. Dans ce cas, $g_L = mul(P_\beta)$ et $d_L = \deg(P_\beta)$.

(ii) : Si $y \in K$ est un zéro approché de P, alors vy est une antipente de $\mathcal{N}(P)$, et $\frac{y}{s(vy)}v$ est une racine de P_{vy}.

(iii) : Si $\beta \in \Gamma$ est une antipente de $\mathcal{N}(P)$, et $c \in k$ est une racine non nulle de P_β, alors P admet un zéro approché y unique à équivalence près à respecter $vy = \beta$ et $\frac{y}{s(\beta)}v = c$.

$\star\star\star$

(i) : Il suffit de remarquer que les indices des coefficients non nuls de P_β sont les abscisses des points de L dans $\mathcal{N}(P)$.

(ii) : Soit y un zéro approché de P. vy est dans Γ, et comme on l'a vu dans la proposition précédente, $\frac{y}{s(vy)}v$ est une racine de P_{vy} qui admet au moins deux coefficients non nuls, disons d'indices j_0 et j_1.

On a alors $v\delta_{P_{\times s(vy)}} = \min_i va_i + i.vy = va_{j_0} + j_0.vy = va_{j_1} + j_1.vy$, ce qui signifie que $L_{vy, v\delta_{P_{\times s(vy)}}}$ est une arête de $\mathcal{N}(P)$, donc vy est une antipente de $\mathcal{N}(P)$.

Il ne reste plus noter que la droite passant (i, va_i) et (j, va_j) est une arête de $\mathcal{N}(P)$ d'antipente vy par définition de P_{vy}, donc vy est une antipente de $\mathcal{N}(P)$.

(iii) : Soit $\mathfrak{m} := s(\beta)$. Soit $x \in c$. On pose $y = \mathfrak{m}x$, de sorte que $\frac{y}{\mathfrak{m}}v = c$.

On a déjà vu que $D_{P_{\times \mathfrak{m}}}(\frac{y}{\mathfrak{m}}v) = 0$ impliquait que y était zéro approché de P.

Or ici $P_\beta(c) = P_\beta(\frac{y}{\mathfrak{m}}v) = D_{P_{\times \mathfrak{m}}}(\frac{y}{\mathfrak{m}}v)$.

Donc y est zéro approché de P. Soit y' un zéro approché de P tel que $vy' = \beta = vy$ et $\frac{vy'}{s(\beta)}v = c$.

Il existe donc $x' \in c$ tel que $y = \mathfrak{m}x'$.

$v(y-y') = v(\mathfrak{m}(x-x')) = v(\mathfrak{m}) + v(x-x')$ où $x - x' \in m_A$ donc $v(x-x') > 0$.

Ainsi, $v(y-y') > v(\mathfrak{m}) = v(\mathfrak{m}) + vx$ car $c \neq 0$ dans k donc $vx = 0$.

$v(y-y') > v(\mathfrak{m}x) = vy : y \sim y'$.

$\star\star\star$

Corollaire

P admet au plus $\deg(P)$ zéros approchés à équivalence près.

$\star$

Soit Z l'ensemble des classes d'équivalence forte de zéros approchés de P.

D'après (ii) et (iii), l'application qui à un élément de Z associe la valuation commune de ses éléments a pour image l'ensemble G des antipentes de $\mathcal{N}(P)$ dans Γ.

Pour chaque antipente β de $\mathcal{N}(P)$, il y a d'après (ii) et (iii) autant d'éléments de Z de valuation β que de racines de P_β dans $k^\times$.

Or, puisque $mul(P_\beta) = g_L$ et $\deg(P_\beta) = d_L$ où L est l'arête de $\mathcal{N}(P)$ d'antipente β, ce nombre de racines non nulles est inférieur ou égal à $d_L - g_L$.

Ainsi, en notant $L_1, ..., L_{|G|}$ les arêtes de $\mathcal{N}(P)$ d'antipente dans Γ ordonnées par antipente strictement décroissante, on a $|Z| \leq \sum_{p=1}^{|G|} d_{L_p} - g_{L_p}$.

Pour tout $1 \leq p < |G|$, $g_{L_{p+1}} \geq d_{L_p}$, donc $|Z| \leq \sum_{p=0}^{|G|-1} d_{L_{p+1}} - d_{L_p} \leq d_{L_{|G|}} - d_{L_1} \leq r - 0 = r$.

$\star$

Définition VI.4

-Une partie non vide $\mathcal{E}$ de $K^\times$ est dite $\preceq$-fermée, si $\forall x \preceq y \in K^\times, y \in E \rightarrow x \in E$.

-Une **équation asymptotique** est la donnée d'un polynôme non nul à coefficients dans K et d'une partie $\preceq$-fermée de $K^\times$.

-Le **degré dominant** $ddeg(E)$ de l'équation asymptotique $E := (Q, \mathcal{E})$ est 0 si les antipentes de $\mathcal{N}(Q)$ sont majorées strictement par $v\mathcal{E}$.

Sinon, on note $\beta(E)$ la plus petite antipente de $\mathcal{N}(Q)$ telle qu'il existe $x \in \mathcal{E}$ tel que $vx \leq \beta(E)$, L_E l'arête correspondante, et on pose $ddeg(E) = d_{L_E}$.

D'après le point (i) de la proposition précédente, si $\beta(E) \in \Gamma$, on a $d_{L_E} = \deg(P_{\beta(E)})$.

-Enfin, on note $ddeg_{\mathcal{E}}(Q) := \max(\{ddeg(D_{Q\times\mathfrak{m}}) \mid \mathfrak{m} \in \mathcal{E} \cap \mathcal{M}\})$.

-Une **solution** de E est un zéro de Q dans $\mathcal{E}$, une **solution approchée** de E est un zéro approché de Q dans $\mathcal{E}$.

Soit $\mathfrak{m} \in \mathcal{M}$. On a $mul(P) = mul(P_{\times\mathfrak{m}}) \leq dmul(P_{\times\mathfrak{m}}) \leq ddeg(P_{\times\mathfrak{m}}) \leq \deg(P)$, donc $mul(P) \leq ddeg_{\mathcal{E}}(P) \leq \deg(P)$.

La relation entre $ddeg(E)$ et $ddeg_{\mathcal{E}}(P)$ peut-être précisée :

Lemme VI.2

Si le degré dominant de E est nul, alors E n'admet aucune solution approchée, et $ddeg_{\mathcal{E}}(P) = mul(P)$.

Sinon, $mul(P) < ddeg_{\mathcal{E}}(P) = ddeg(E)$.

$\star\star$

Soit $(\widetilde{K}, \widetilde{\preceq})$ une extension algébriquement close de $(K, \preceq)$. On prolonge s en une application $\widetilde{s}$ du groupe de valeur de $(\widetilde{K}, \widetilde{\preceq})$ dans son groupe unité telle que $v \circ \widetilde{s} \circ \widetilde{v}$ soit l'identité sur le groupe de valeur, et on considère $\widetilde{\mathcal{M}} := Im(\widetilde{s})$. On pose aussi $\widetilde{\mathcal{E}} := \{x \in \widetilde{K}^\times \mid \exists y \in \mathcal{E}, x \widetilde{\preceq} y\}$; qui est une partie $\widetilde{\preceq}$-fermée de $(\widetilde{K}, \widetilde{\preceq})$.

$\widetilde{E} := (P, \widetilde{\mathcal{E}})$ est alors une équation asymptotique sur $(\widetilde{K}, \widetilde{\preceq})$. La définition de $\widetilde{\mathcal{E}}$ impose que $ddeg(\widetilde{E}) = ddeg(E)$. Conjointe au **lemme VI.1**, elle implique également que $ddeg_{\widetilde{\mathcal{E}}}(P) = ddeg_{\mathcal{E}}(P)$. Bien sûr, la multiplicité de P en zéro est conservée par extension quelconque. On peut donc supposer que K est algébriquement clos, ce qui impose trivialement que Γ est divisible, et c'est ce que l'on fait dans la suite.

Supposons que $y \in \mathcal{E}$ est un zéro approché de P. Alors vy est une antipente de $\mathcal{N}(P)$, donc $ddeg(E)$ est l'abscisse droite d'une arête de $\mathcal{N}(P)$, qui est strictement supérieure à l'abscisse gauche de la même arête, donc non nulle. Ainsi une équation asymptotique de degré dominant nul n'admet aucune solution approchée.

Soient $m := mul(P), d := ddeg_{\mathcal{E}}(P)$.

Supposons $m < d$. Soit $\mathfrak{m} \in \mathcal{M}$ tel que $d = ddeg(P_{\times \mathfrak{m}})$.

On ne peut pas avoir $va_m \mathfrak{m}^m < va_d \mathfrak{m}^d$ sinon le coefficient de degré d de $D_{P_{\times \mathfrak{m}}}$ serait nul et ce polynôme serait donc de degré distinct de d.

On a donc $va_m + m.v\mathfrak{m} \geq va_d + d.v\mathfrak{m}$.

m étant la multiplicité de P en zéro, c'est la plus petite abscisse des points de $\mathcal{N}(P)$, donc l'abscisse gauche de l'arête L de $\mathcal{N}(P)$ de plus grande antipente.

Cette antipente doit donc être plus grande que $v\mathfrak{m}$, ce qui montre que $ddeg(E) \geq d_L > 0$. Cela montre la première inégalité par contraposition.

Supposons maintenant que $ddeg(E) > 0$. Puisque $mul(P)$ est la plus petite abscisse de points de $\mathcal{N}(P)$ et que $ddeg(E)$ est une abscisse droite d'une arête de $\mathcal{N}(P)$ (on utilise ici le fait que Γ étant divisible, $\beta(E)$ appartient nécessairement à Γ), $ddeg(E) > mul(P)$.

Il reste donc à montrer que $ddeg(E) \geq ddeg_{\mathcal{E}}(P)$.

Supposons le contraire. On dispose alors d'un élément $\mathfrak{m}$ de $\mathcal{E} \cap \mathcal{M}$ tel que $i := ddeg(P_{\times \mathfrak{m}}) > ddeg(E) =: d$.

Par l'argument habituel, $va_d + d.v\mathfrak{m} \geq va_i + i.v\mathfrak{m}$.

d est l'abscisse droite de L_E, donc L_E contient (d, va_d) mais pas (i, va_i), et donc $va_i + i.\beta(E) > va_d + d.\beta(E)$.

Soit L la droite passant par (d, va_d) et (i, va_i). Son antipente β vaut donc $\frac{1}{i-d}(va_d - va_i)$, et satisfait donc d'après les inégalités précédentes $v\mathfrak{m} \leq \beta < \beta(E)$.

L'arête de $\mathcal{N}(P)$ ayant d pour abscisse gauche a une antipente β' supérieure à β, donc à $v\mathfrak{m}$ puisque (i, va_i) est sur ou au dessus de cette arête.

Par décroissance stricte des antipentes lorsqu'on se déplace vers la droite dans le diagramme de Newton, $\beta' < \beta(E)$, et donc β' invalide la maximalité de $\beta(E)$ à majorer un vx pour $x \in \mathcal{E}$: contradictoire.

Donc $ddeg(E) = ddeg_{\mathcal{E}}(P)$.

$\star\ \star$

Le degré dominant est un indicateur de la *complexité* d'une équation asymptotique. L'équation est sans solution (car sans solution approchée) s'il est nul, et sinon, cet entier donne le nombre maximal à équivalence près de solutions approchées d'une valuation donnée.

La suite de la théorie de l'algorithme de Newton s'intéresse aux cas intermédiaires, et la proposition suivante considère celui de degré dominant égal à 1 :

Proposition VI.3

Une équation asymptotique de degré dominant 1 admet une unique solution dans toute extension henselienne de (K, v).

$\star\ \star\ \star$

On peut supposer (K, v) henselien.

$(0, va_0)$ est sur l'arête de $\mathcal{N}(P)$ d'antipente $\beta(E)$ puisque son abscisse droite est 1.

On a donc $va_{ddeg(E)} + ddeg(E).\beta(E) = va_1 + \beta(E) = va_0 \in \Gamma$, donc $\beta(E) \in \Gamma$.

Soit $\mathfrak{m} := s(\beta(E))$; soit $\delta := \delta_{P_{\times\mathfrak{m}}}$.

$\delta^{-1}P_{\times\mathfrak{m}}v = P_{\beta(E)}$, avec $\deg(P_{\beta(E)}) = ddeg(E) = 1$.

Donc $\delta^{-1}P_{\times\mathfrak{m}}v$ admet une unique racine dans k. Cette racine est non nulle car $P_{\beta(E)}$ possède deux coefficients non nuls.

(K, v) étant henselien, $\delta^{-1}P_{\times\mathfrak{m}}$, et donc $P_{\times\mathfrak{m}}$ admettent une unique racine y dans $K^{\preceq 1}$.

$vy = 0$ et $\mathfrak{m}y$ est une racine de P de valuation $\beta(E)$.

Toute racine de P est de valuation supérieure ou égale à $\beta(E)$, et puisque $ddeg(E) = 1$, une telle racine ne peut avoir de valuation strictement supérieure, sinon $\mathcal{N}(P)$ admettrait une arête strictement à gauche de celle passant par $(0, va_0)$ et $(1, va_1)$, ce qui est absurde.

Donc toute racine de P est de valuation $\beta(E)$, et par unicité dans la propriété de Hensel, elle vaut $\mathfrak{m}y$.

$\star\ \star\ \star$

Dans toute la suite, (K, v) est supposé d'équicaractéristique nulle

Définition VI.5

Soit $E = (Q, \mathcal{E})$ une équation asymptotique. Un **raffinement** de E est une équation asymptotique de la forme $(Q_{+f}, \mathcal{E}')$ où f est une solution approchée de E ou $f = 0$, et $\mathcal{E}'$ est une partie $\preceq$ fermée de $\mathcal{E}$.

Remarque :

Si x est une solution du raffinement $(P_{+f}, \mathcal{E}')$ de $(P, \mathcal{E})$ et $x + f \neq 0$, alors $x + f$ est une solution de $(Q, \mathcal{E})$.

De plus, si x est une solution approchée de $(P_{+f}, \mathcal{E}')$ et $x \not\sim -f$, alors $x + f$ est une solution approchée de $(Q, \mathcal{E})$.

En effet, si $x \not\sim -f$ alors $v(x + f) \leq vx, vy$, et :

$vP(x+f) = vP_{+f}(x) > \min_i vb_i x^i$ où $\forall 0 \leq i \leq r, b_i = \frac{P^{(i)}(f)}{i!} = \sum_{j=1}^{n} \binom{j}{i} a_j f^{j-i}$.

$vP(x + f) > \min_i \min_{j \geq i} a_j x^i f^{j-i} \geq \min_i \min_{j \geq i} va_j + i.vx + (j - i).vf \geq va_j + i.v(x + f) + (j - i).v(x + f) = \min_i \min_{j \geq i} va_j(x + f)^j = \min_i va_j(x + f)^j$.

On va s'intéresser à un type particulier de raffinement d'une équation asymptotique $E = (P, \mathcal{E})$. Il s'agit de $E_{+f} := (P_{+f}, \{x \in K^\times \mid x \prec f\})$ où f est une solution approchée de E.

On note alors $\mathcal{E}_{\prec f} = \{x \in K^\times \mid x \prec f\}$ et $ddeg_{\prec f}(P) := ddeg_{\mathcal{E}_{\prec f}}(P)$.

La remarque précédente implique que les solutions approchées de E_{+f} sont exactement les translatés par $-f$ des solutions approchées de E. Les solutions de E_{+f} sont les translatés par $-f$ des solutions non nulles de E.

Lemme VI.3

Soit f une solution approchée de E. On note $\beta := vf$, $\mathfrak{m} := s(\beta)$, et μ la multiplicité en $c := \frac{f}{\mathfrak{m}} v$ de P_β.

On note enfin pour $i \in \{0; ...; r\}$, $b_i := \frac{P^{(i)}(f)}{i!}$.

On a :

(i) : $b_\mu \neq 0$, et les points de $\mathcal{N}(P_{+f})$ d'abscisse strictement inférieure à μ sont au dessus de la droite passant par (μ, vb_μ) d'antipente β, et les autres sont sur ou au dessus d'elle.

(ii) : S'il existe $i < \mu$ tel que $b_i = 0$, alors $ddeg(E_{+f}) = 0$.

(iii) : Sinon, $ddeg(E) = \mu$.

$\star\star$

Soit $\delta := \delta_{P_{\times \mathfrak{m}}}$, soit $\alpha = v\delta$. Soit $Q := \delta^{-1} P_{\times \mathfrak{m}}$.

$P_\beta = Qv$.

Pour $i \in \{0; ...; r\}$, $Q^{(i)}(\frac{f}{\mathfrak{m}}) = \mathfrak{m}^i\delta^{-1}P^{(i)}_{\times\mathfrak{m}}(\frac{f}{\mathfrak{m}}) = \mathfrak{m}^i\delta^{-1}P^{(i)}(f) = \mathfrak{m}^i\delta^{-1}b_i i!$.

Donc $vb_i = v\frac{Q^{(i)}(\frac{f}{\mathfrak{m}})\delta}{\mathfrak{m}^i i!} = vQ^{(i)}(\frac{f}{\mathfrak{m}})\delta - i.\beta$.

Or, si $i < \mu$, $Q^{(i)}(\frac{f}{\mathfrak{m}})v = P^{(i)}_\beta(c) = 0$, et $Q^{(\mu)}(\frac{f}{\mathfrak{m}})v = P^{(\mu)}_\beta(c) \neq 0$.

On a donc pour $i < \mu$, $vb_i > \alpha - i.\beta$, et $vb_\mu = \alpha - \mu.\beta$. Cette dernière égalité montre que b_μ n'est pas nul.

Enfin, en général, $vb_i \geq \alpha - i.\beta$.

Donc si (i, vb_i) est un point de $\mathcal{N}(P)$, si $i < \mu$, on a $vb_i + i.\beta > \alpha = vb_\mu + \mu.\beta$, et si $i \geq \mu$, $vb_i + i.\beta \geq vb_\mu + \mu.\beta$, ce qui prouve (i).

On en déduit également que pour $0 \neq x \prec f$ et $\mu < j \leq r$, $vb_\mu x^\mu = \alpha - \mu.\beta + \mu.vx = \alpha + \mu.(vx - \beta) < \alpha + j.(vx - \beta) = vb_j x^j$, ce qui montre par l'argument classique que $ddeg(E_{+f}) = ddeg_\prec f(P_{+f}) \leq \mu$ si $ddeg(E_{+f}) > 0$, et bien sûr cette inégalité est vraie dans le cas de degré dominant nul.

Supposons que pour tout $i < \mu$, on ait $b_i = 0$. D'après (i), la plus grande antipente de $\mathcal{N}(P_{+f})$ (qui est alors celle de l'arête passant par (μ, vb_μ)) est inférieure ou égale à β, et donc toutes les antipentes de $\mathcal{N}(P_{+f})$ sont strictement majorées par chaque élément de $v(\{y \in K^\times \mid y \prec f\})$, donc $ddeg(E) = 0$.

Supposons au contraire qu'il existe $i < \mu$ tel que $b_i \neq 0$. Soit L la ligne passant par (μ, vb_μ) et un point (i, vb_i) avec $b_i \neq 0$ d'antipente minimum.

D'après les inégalités précédentes, son antipente β' est strictement supérieure à β. Tous les points de $\mathcal{N}(P_{+f})$ d'abscisse stritement supérieure à μ sont sur ou au dessus de L, donc c'est une arête de $\mathcal{N}(P_{+f})$, et d'après (i), son abscisse droite $d_L = \mu$ est par minimalité de β' le degré dominant de E_{+f}, ce qui prouve (iii).

$\star\ \star$

Lemme VI.4

On suppose (K, v) henselien. Soit $E = (P, \mathcal{E})$ de degré dominant $d \geq 1$ tel que $\beta(E) \in \Gamma$ et $P_{\beta(E)}$ admet un zéro de multiplicité d.

(i) : $P^{(d-1)}$ admet un unique zéro $f \in \mathcal{E}$.

(ii) : $vf = \beta(E)$ et f est une solution approchée de E unique à équivalence près parmi les solutions approchées de E.

(iii) : Si $ddeg(E_{+f}) = d$ et $\beta(E_{+f}) \in \Gamma$, alors $P_{\beta(E_{+f})}$ n'a aucun zéro de multiplicité d.

$\star\ \star$

Puisque $\beta(E) \in \Gamma$, on a $\deg(P_{\beta(E)}) = d$ et il existe donc $c_1 \in k^\times$ tel que $P_{\beta(E)} = c_1(X - c_0)^d$ où c_0 est le zéro de $P_{\beta(E)}$ de multiplicité d.

Puisque $ddeg(E) > 0$, d'après le **lemme VI.2** $mul(P) < d$, donc c_0 est non nul.

On pose $\mathfrak{m} := s(\beta(E))$, $\delta := \delta_{P_{\times \mathfrak{m}}}$, et $Q := \delta^{-1} P_{\times \mathfrak{m}}$.

$Q^{(d-1)} = \delta^{-1}\mathfrak{m}^{d-1} {P^{(d-1)}}_{\times \mathfrak{m}}$.

Or $Q^{(d-1)}v = Qv^{(d-1)} = {P_{\beta(E)}}^{(d-1)} = c_1 d!(X - c_0)$ (car l'application résidu commute avec les dérivations sur $K^{\preceq 1}[X]$ et $k[X]$)

On en déduit que $\beta(E)$ est une antipente de $\mathcal{N}(P^{(d-1)})$, donc $ddeg(P^{(d-1)}, \mathcal{E}) > 0$, et donc $ddeg(P^{(d-1)}, \mathcal{E}) = ddeg_{\mathcal{E}}(P^{(d-1)})$.

Or $ddeg_{\mathcal{E}}(P^{(d-1)}) = \max(\{\mathfrak{n} \in \mathcal{E} \cap \mathcal{M} \mid ddeg(P^{(d-1)}_{\times \mathfrak{n}})\}) = \max(\{ddeg(P_{\times \mathfrak{n}}) - (d-1) \mid \mathfrak{n} \in \mathcal{E} \cap \mathcal{M}\}) = d - (d-1) = 1$.

Donc $ddeg(P^{(d-1)}, \mathcal{E}) = 1$ et d'après la **proposition VI.2**, $P^{(d-1)}$ admet une unique racine $f = \mathfrak{m}g$ dans $\mathcal{E}$, où g est l'unique racine de $Q^{(d-1)}$ dans $K^{\preceq 1}$. Cela prouve (1).

On a $0 = Q^{(d-1)}(g)v = P_\beta(gv)$, donc $gv = c_0$, donc $vf = \beta(E)$ et $\frac{f}{\mathfrak{m}}v = c_0$, qui est une racine de $P_{\beta(E)}$ dans $k^\times$, donc f est une solution approchée de (E).

Soit x une solution approchée de (E). $P_{\beta(E)}(0) = (-1)^d c_1 {c_0}^d \neq 0$, donc $mul(P_\beta)$, qui est l'abscisse de l'arête de $\mathcal{N}(P)$ d'antipente $\beta(E)$, est nulle. Donc $\beta(E)$ est la plus grande antipente de $\mathcal{N}(P)$, et la seule à satisfaire $\exists n \in \mathcal{E} \cap \mathcal{M}$, $v\mathfrak{n} \leq \beta(E)$. vx étant une de ces antipentes (voir **proposition VI.1**), $vx = \beta(E)$.

Puisque $P_{\beta(E)}$ admet c_0 pour unique racine, $x \sim f$. (voir **proposition VI.1**) Cela prouve (ii).

Supposons que $ddeg(E_{+f}) = d$, que $\beta(E_{+f}) \in \Gamma$, et que $P_{\beta(E_{+f})}$ admet une racine de multiplicité d.

Alors d'après (i) appliqué à E_{+f}, ${P_{+f}}^{(d-1)}$ admet un unique zéro $0 \neq g \prec f$.

On a ${P_{+f}}^{(d-1)}(g) = {P^{(d-1)}}_{+f}(g) = P^{(d-1)}(f+g)$ où $f + g \neq f$, donc $f + g \neq \mathcal{E}$ par unicité de f dans (i).

Or $v(f+g) = vf$, donc par $\preceq$-fermeture de $\mathcal{E}$, $f + g$ est nécessairement nul, ce qui contredit $g \prec f$.

Donc $P_{\beta(E_{+f})}$ n'admet pas de racine de multiplicité d.

$\star\star$

Tous ces résultats nous permettent de produire un algorithme de résolution d'une équation polynomiale dans un corps valué henselien d'équicaractéristique nulle.

On suppose ici que (K, v) est henselien d'équicaractéristique nulle.

On cherche à résoudre l'équation asymptotique $E := (P, K^\times)$. On va mettre en place un algorithme à proprement parler pour résoudre asymptotiquement cette équation, ainsi qu'une méthode théorique pour la résoudre totalement.

Algorithme de Newton (fini)

La description qui suit de l'algorithme est inductive :

On pose $E_0 = E$; pour chaque antipente β de $\mathcal{N}(P)$ dans Γ, on construit la séquence initiale $(E, \beta, 0)$.

Supposons données une séquence finie $\beta_0 < ... < \beta_n$ d'éléments de Γ, une séquence finie $f_0 \succ ... \succ f_n$ de d'éléments de $K^\times$, et une suite finie d'équations asymptotiques $E_0 = (P_0, \mathcal{E}_0), ..., E_n = (P_n, \mathcal{E}_n)$ telles que :

(i) : Pour $0 \leq i \leq n$, β_i est une antipente de $\mathcal{N}(P_i)$ dans $\Gamma \cap v\mathcal{E}_i$

(ii) : Pour $0 \leq i \leq n-1$, f_{i+1} est une solution approchée de E_i d'antipente β_i

(iii) : Pour $0 \leq i \leq n-1$ $E_{i+1} = (P_{i+1}, \{x \in K^\times \mid x \prec f_i\})$ est une équation asymptotique dont les solutions (resp solutions approchées) sont exactement les translatés par $-f_i$ des solutions (resp solutions approchées) de E_i.

On prolonge ou pas ces suites en préservant ces conditions de la manière suivante :

-Si $ddeg(E_n) = 0$ et 0 est une racine de P_n, on ne prolonge pas σ, et on pose $f(e) := f_0 + ... + f_n$. $f(e)$ est alors une solution de E. ($f(e) \neq 0$ car $f_n \prec ... \prec f_0$.)

-Si $ddeg(E_n) = 0$ et 0 n'est pas une racine de P_n, on ne prolonge pas les séquences.

Notons qu'alors E_n n'admet aucune solution approchée, donc a fortiori aucune solution non nulle, et donc aucune solution. D'après (iii), E n'admet aucune solution.

-Si $ddeg(E_n) \geq 1$, pour toute antipente $\beta \geq \beta(E)$ de $\mathcal{N}(P_n)$ dans Γ, on choisit en résolvant $P_\beta = 0$ dans k une liste complète $f_{\beta,0}, ..., f_{\beta,p}$ de solutions approchées E_n deux-à-deux non équivalentes.

Pour chaque $0 \leq i \leq p$, on prolonge les suites en ajoutant β,$f_{\beta,i}$, $E_{n+f_{\beta,i}}$ dans le cas noté **a** traité par le **lemme VI.3** avec $\mu < ddeg(E_n)$, et en leur ajoutant $\beta = \beta(E_n), f_{\beta,i}, (P_{n+f_{\beta,i}}^{(ddeg(E_n)-1)}, \{x \in K^\times \mid x \prec f_{\beta,i}\})$ dans le cas **b** spécifiquement traité par le **lemme VI.4**.

Il est clair par définition que les conditions (i) et (ii) sont préservées par prolongement. Pour ce qui est de la troisième, elle provient dans le cas **a** directement de la remarque succédant la **définition VI.4** et du fait que pour $x \prec f \in K^\times, x + f \neq 0 \to x \not\sim -f$.

Dans le cas **b**, le point (*ii*) du **lemme VI.4** montre que les équations satisfont bien (*iii*).

L'algorithme se termine-t-il ?

Une façon classique de prouver la terminaison d'un algorithme récursif est d'exhiber une application strictement décroissante par sauts du nombre de récursions dans un ensemble bien fondé. Dans les paragraphes qui suivent, on entend montrer que le degré dominant des équations asymptotiques d'indices finals dans les séquences de prolongements est une telle application. Cependant ce n'est parfois que pour un nombre infini de récursions (ordinal infini) que le degré dominant décroît. Il faudra donc proposer une méthode de prolongation transfinie des séquences produites par l'algorithme fini.

Le **lemme VI.3** montre que les degré dominants des équations asymptotiques d'indices finals dans les séquences de prolongements sont décroissants largement.

On prétend qu'à chaque fois que l'on prolonge deux fois successivement les suites, le degré dominant des équations asymptotiques d'indices finals qui sont strictement supérieurs à 1 sont abaissés d'au moins 1.

En effet, si toutes les solutions approchées f de E_n pour une antipente quelconque $\beta \in \Gamma$ de $\mathcal{N}(P_n)$ sont tels que $\frac{f}{s(\beta)}v$ est de multiplicité strictement inférieure à $ddeg(E_n)$, les degrés dominants des équations asymptotiques obtenues par prolongement sont égaux d'après le **lemme VI.3** à ces multiplicités, et sont donc strictement inférieurs à $ddeg(E_n)$.

Si E_n admet une solution approchée f pour laquelle la multiplicité est égale à $ddeg(E_n)$, l'antipente correspondante est nécessairement égale à $\beta(E_n)$.

Si cette antipente est dans Γ, on peut chercher la racine de P_n correspondante parmi les racines de ${P_n}^{(d-1)}$ dans E_n, et puisque $d > 1$, $ddeg(E_{n+1}) = ddeg_{\prec f}({P_n}^{(d-1)}) = ddeg_{\prec f}(P_n) - (d-1) \leq ddeg(E_n) - (d-1) \leq ddeg(E_n) - 1$. (on applique ici également le **lemme VI.1**).

Donc en un temps fini, on finit par abaisser les degrés dominants jusqu'à 1 ou 0.

Il reste à traiter le cas spécial du degré dominant 1. Notons qu'en vertu du **lemme VI.4**, on pourrait se contenter de remplacer l'instruction de l'algorithme dans le cas d'existence d'un zéro approché de multiplicité associée égale au degré dominant en cours par "choisir l'unique racine de P_n dans $\mathcal{E}_n$", cependant ce n'est pas algorithmiquement satisfaisant : il n'y a pas de moyen simple en général de trouver une telle racine exacte même lorsque le degré dominant est 1, car le degré de P_n peut être très grand.

Le cas spécial de degré dominant égal à 1 doit par conséquent être traité à part.

Cas spécial de degré dominant égal à 1 et "algorithme transfini"

Si $ddeg(E_n) = 1$ pour un certain entier naturel correspondant à une séquence de prolongements $(\beta_0, ..., \beta_n, f_0, ..., f_n, E_0, ..., E_n)$, il y a deux possibilités :

-Il n'existe pas de suite infinie indexée par $\mathbb{N}$ de prolongements de la séquence considérée. On est donc retombé sur le cas $ddeg(E) = 0$ au bout d'applications de l'algorithme fini un nombre fini de fois.

-Il en existe une, on considère la concaténation de ces prolongements à partir de n : $\beta_n, ..., \beta_m, ...$; $f_n, ..., f_m, ...$; $E_n, ..., E_m, ...$

Alors la suite $u := p \longmapsto f_{n+1} + ... + f_p$ est pseudocauchy dans (K, v) d'après la relation $f_p \prec ... \prec f_n$.

De plus, P_n est un polynôme annulateur de u.

En effet, pour $n \leq p \in \mathbb{N}, P_{p+1} = P_{+f_p}$ (on est en effet dans le second cas de prolongement pour $ddeg(P) = 1$).

Donc $vP_n(u_{p+1}) = vP_p(f_{p+1}) > \min_i vq_{p,i}{f_{p+1}}^i$ où $P_p = \sum_i q_{p,i}X^i$.

Puisque les degrés dominants à partir de n sont égaux à 1, et que vf_{p+1} est égal à $\beta(E_p)$ dans ce cas, on a $\min_i vq_{p,i}{f_{p+1}}^i = \min_i vq_{p,i} + i.\beta(E_p) = vq_{p,0} = vq_{p,1}f_{p+1} = vq_{p,1} + \beta(E_p)$.

En particulier, $vP_n(u_{p+1}) > vq_{p,0} = vP_p(0) = vP_n(u_p)$.

Donc u est de type algébrique sur (K, v). Ce dernier étant henselien d'équicaratéristique nulle, il est algébriquement maximal, et donc u admet une pseudolimite $u_{1,0}$ dans (K, v).

On peut répéter l'algorithme fini en considérant comme statut initial celui pour lequel $\beta_{1,0}$ est une antipente de $P_{n+u_{1,0}}$, en posant $f_{1,0} = 0$, et en prolongeant la suite des équations avec $E_{1,0} := (P_{n+u_{1,0}}, \{x \in K^\times \mid \forall p \in \mathbb{N}, x \prec u_{p+1} - u_p\})$. Notons que puisque $a_1 \sim f_{n+1}$, est un zéro approché de P_n et $\{x \in K^\times \mid \forall p \in \mathbb{N}, x \prec u_{p+1} - u_p\} \subset \mathcal{E}_{\prec f_n}$, le **lemme VI.1** permet de déduire que $ddeg(E_{1,0}) \leq ddeg(E_n) = 1$.

On appelle étape transfinie 1, étape fine 0 cet état de prolongement de la séquence initiale. On passe alors (en supposant que le degré dominant se maintienne à 1) en utilisant l'algorithme fini à l'étape transfinie 1, étape finie 1 produisant une suite u_1, puis étape transfinie 1, étape finie 2, et ainsi de suite, jusqu'à atteindre une nouvelle étape transfinie 2 produisant un prolongement u_2 de u_1, et ainsi de suite. Notons qu'à toutes les étapes transfinies $m \in \mathbb{N}^*$, étapes finies 0, u_m est pseudocauchy dans (K, v) annulée par $P_{1,0}$, satisfait les conditions (i), (ii) et (iii) de l'algorithme aux étapes finies, et la généralisation de la condition (iii) au transfini à toutes les étapes transfinies m, étapes finies 0, à savoir que les solutions approchées (resp solutions non nulles) de $E_{m,0}$ sont les translatés par $u_{m',0} - u_{m,0}$ de celles de $E_{m,0}$.

On cherche maintenant à définir inductivement un prolongement d'étape transfinie $\lambda \in Ord$ quelconque, et d'étape finie $p \in \mathbb{N}$ quelconque tant le maintient à 1 du degré dominant le permet. Soient λ, p de tels ensembles.

On suppose que pour $\rho < \lambda$, les prolongements d'étape transfinie ρ ont été définis, que les équations asymptotiques à partir de l'étape transfinie 1 sont de

degré dominant 1, et que les conditions suivantes sont vérifiées :

-La suite $u_\rho : \omega.\rho + p \to K^\times$ définie par $u_\alpha = 0$ si $\alpha < \omega$, si $\alpha = \omega.\mu + p$, $1 \leq \mu \leq \lambda$ et $p \in \mathbb{N}$ par $u_{\alpha+1} - u_\alpha = f_{\mu,p+1}$, et u_α est la de pseudolimite de $u_\gamma)_{\gamma<\alpha}$ telle que $E_{\mu,0} = (P_{(1,0)_{+u_\alpha}}, \bigcap_{\gamma<\alpha} \mathcal{E}_{\prec u_{\gamma+1}-u_\gamma})$ si α est limite ($p = 0$), est pseudocauchy à partir de ω annulée par $P_{1,0}$.

-Les solutions approchées (resp solutions non nulles) de $E_{\rho,0}$ sont les translatés par $u_{\sigma,0} - u_{\rho_0}$ des solutions approchées (resp solutions non nulles) de $E_{\sigma,0}$, dès que $\omega < \sigma < \rho < \lambda$ sont des ordinaux limites.

Ainsi, l'union de ces suites (qui sont incluses les unes dans les autres car les pseudolimites et les solutions approchées sont fixées par les prolongements) est pseudocauchy dans (K, v) annulée par $P_{(1,0)}$, donc elle admet une pseudolimite $a_{\lambda,0}$ dans K.

On prolonge la suite en posant $E_{\lambda,0} := (P_{(1,0)_{+u_{\lambda,0}}}, \{x \in K^\times \mid \forall \alpha < \lambda, x \prec u_{\alpha+1} - u_\alpha\})$, en posant $f_{\lambda,0} = 0$ et en choisissant $\beta_{\lambda,0}$ parmi les antipentes de $P_{(1,0)_{+u_{\lambda,0}}}$ dans $\Gamma \cap \{x \in K^\times \mid \forall \alpha < \lambda, x \prec u_{\alpha+1} - u_\alpha\}$ (il n'en existe qu'une, puisque pour les mêmes raisons que dans le cas d'étape transfinie d'indice fini, $ddeg(E_{\lambda,0}) = 1$),

Il reste à voir que la condition (iii) généralisée au transfini est satisfaite. Il suffit de voir que l'équivalence tient entre les solutions de $E_{\lambda,0}$ et $E_{1,0}$, ce qui est immédiat par définition et du fait que les solutions approchées à ces équations asymptotiques sont uniques à équivalence près, puisque les degrés dominants sont égaux à 1.

A noter que le nombre d'étapes transfinies est limité car à l'étape transfinie λ, on a un plongement $(\omega.\lambda, \in) \to (\Gamma, <)$ donné par $\omega.\rho + p \longmapsto \beta_{\rho,p}$.

Ainsi, les indices des étapes transfinies sont majorés, et le prolongement finit par abaisser au bout de l'étape transfinie λ pour un certain ordinal λ le degré dominant de 1 à 0 à moins que l'algorithme fini ne l'ait déjà fait. A ce moment là, 0 est nécessairement racine de $P_{\lambda,0}$ puisque ce dernier admet une unique racine et qu'il n'admet aucun zéro approché (donc en particulier aucune racine non nulle). Ainsi, $P(u_{1,0} + u_{\lambda,0}) = P_{1,0}(u_{\lambda,0}) = P_{\lambda,0}(0) = 0$, on pose alors $f(e) = u_{0,1} + u_{\lambda,0}$, (e) étant la suite correspondante.

Théorème VI.1

Les racines non nulles de P sont les $f(e)$.

⋆ ⋆ ⋆ ⋆

Il s'agit de s'en convaincre en reprenant les éléments précédents et en remarquant que toute racine non nulle d'un polynôme est un zéro approché de ce polynôme.

⋆ ⋆ ⋆ ⋆

Cette méthode et les méthodes de même genre permettent de démontrer d'importants résultats comme le théorème de Newton-Puiseux concernant la paramétrisation locale des courbes algébriques par des éléments de $\mathbb{C}((t^{\frac{1}{n}.\mathbb{Z}}))$ pour certaines valeurs entières de n.

L'algorithme permet également dans certains cas de développer asymptotiquement avec une précision arbitraire des solutions d'équations polynomiales, voire de trouver des solutions exactes. Un des tours de force des auteurs de est de proposé un algorithme permettant de réaliser la même chose pour des équations différentielles polynomiales, de la forme $P(y) = 0$ où $P \in K[id, \partial, \partial^2, ..., \partial^n, ...]$ est un polynôme différentiel à une variable, ∂ étant une dérivation formelle sur le corps valué K, se comportant abstraitement comme l'opérateur de dérivation sur un ensemble de fonctions dérivables.

Il faut cependant noter plusieurs limites de cet algorithme.

-L'utilité de l'outil géométrique qu'est le diagramme de Newton d'un polynôme présuppose la possibilité de représenter dans de bonnes proportions les points et les segments de $\mathbb{N} \times \mathbb{Q}\Gamma$, ce qui n'est systématiquement possible que lorsque $(\Gamma, +, <)$ est archimédien. On lui préfèrera dans ce cas calcul algorithmique des antipentes, qui est certes de complexité quadratique.

-Etant donnée une antipente β, la résolution exacte de $P_\beta = 0$ dans k n'est pas nécessairement évidente. Une résolution approchée doit être suffisamment précise pour qu'aucun terme de n'apparaisse en trop dans le développement du polynôme même avec un coefficient de valuation nulle négligeable (par au sens d'une norme sur le corps résiduel), et inversement.

-Si (K, v) n'est pas d'équicaractéristique nulle, l'algorithme ne termine pas correctement pour tout prolongement choisi. Par exemple, la résolution de $Q := X^2 + X + t$ dans $\mathbb{F}_2((t^{\mathbb{Z}}))$ selon l'algorithme fournit seulement la solution de valuation 1 $a := \sum_{n \in \mathbb{N}} t^{2^n}$ et pas son conjugué $a + 1$ de valuation nulle, en effet, du fait que $Q_{+1} = Q$, on a $ddeg(Q_{+1}, \{x \in K^\times \mid vx > 0\}) = 0$ avec $Q_{+1}(0) \neq 0$.

-Le choix d'une pseudolimite dans le cas de l'algorithme transfini n'est possible que si la suite pseudocauchy correspondante peut être appréhendée synthétiquement. Bien sur, l'itération seule de l'algorithme ne permet pas de produire des développements asymptotiques de taille transfinie.

En tout état de cause, la configuration optimale pour produire le plus facilement possible le plus de racines de P est de se placer dans un corps valué d'équicaractéristique nulle algébriquement clos de groupe de valeurs archimédien, comme par exemple $\mathbb{C}((t^{\mathbb{Q}}))$.

Applications

On va ici illustrer l'algorithme fini et sur l'exemples suivants :
$P = X^4 - t^3X^3 + 2X^2 - 2t^2X - 5t$ dans $K = \mathbb{C}((t^{\mathbb{Z}}))$.
(L'ensemble de monômes étant l'ensemble des $t^n, n \in \mathbb{Z}$)

On commence par tracer le diagramme de Newton de P :

(1,2,0,3,0)

On a bien $ddeg(E_0) = \deg(P) = 4 > 0$.
On identifie deux antipentes $\alpha = \frac{1}{2}$, et $\beta = 0$; seule β est dans $\mathbb{Z}$.
Il faut donc commencer par résoudre $P_\beta = X^4 + 2X^2 = 0$ dans $\mathbb{C}$.
Les racines non nulles sont $c_+, c_- = \sqrt{2}i, -\sqrt{2}i$, de multiplicités $1 < ddeg(E_0)$, avec zéro approchés associés $f_+, f_- = \sqrt{2}i, -\sqrt{2}i$; donc l'algorithme fini produit les deux raffinements :
$P_{+f_+} = X^4 + (4\sqrt{2}i - t^3)X^3 - (10 + 3\sqrt{2}it^3)X^2 - (4\sqrt{2}i + 2t^2 - 6t^3)X - 5t - 2\sqrt{2}it^2 + 2\sqrt{2}it^3 = 0$ dans $\mathcal{E}_{\prec 1}$ et
$P_{+f_-} = X^4 - (4\sqrt{2}i + t^3)X^3 - (10 - 3\sqrt{2}it^3)X^2 + (4\sqrt{2}iX - 2t^2 + 6t^3)X - 5t + 2\sqrt{2}it^2 - 2\sqrt{2}it^3 = 0$ dans $\mathcal{E}_{\prec 1}$.
Ces deux polynômes ont le même diagramme de Newton, exposé ci-dessous :

(1,0,0,0,0)

Ce diagramme possède deux antipentes $\beta_1 = 1$ et $\beta_2 = 0$, toutes deux dans Γ, mais seule β_1 est dans $v(\mathcal{E}_{\prec 1})$, donc les deux raffinements $E_{+,1}$ et $E_{-,1}$ sont de degré dominant 1.

Notons que d'après le **lemme VI.4**,et le **théorème VI.1** P_A possède exactement deux racines non nulles, donc deux racines, x_+, x_- dans K, et ces deux racines sont égales à $\pm\sqrt{2}i+y_+$ où y_+ est l'unique racine de $P_{A_{+\sqrt{2}i}}$ dans $E_{A,+,1}$.

Les équations résiduelles correspondant à β_1 sont $-4\sqrt{2}iX - 5 = 0$ pour $E_{+,1}$ et $4\sqrt{2}iX - 5 = 0$ pour $E_{-,1}$.

On en déduit les solutions approchées $f_{+1} = \frac{-5\sqrt{2}i}{8}t, f_{-1} = -\frac{5\sqrt{2}i}{8}t$ des raffinements.

Puisque les degrés dominants sont 1, l'algorithme produit les deux raffinements $E_{+,2} = (P_{+\sqrt{2}i+\frac{5\sqrt{2}i}{8}t}, \mathcal{E}_{\prec t})$ et $E_{-,2} = (P_{-\sqrt{2}i-\frac{5\sqrt{2}i}{8}t}, \mathcal{E}_{\prec t})$, que l'on explicitera pas du fait de leur longueur. (les calculs sont faits sur un logiciel de calcul formel)

Les deux polynômes ont encore le même diagramme de Newton :

(2,0,0,0,0)

Ce diagramme admet les antipentes 2 et 0, seule 2 appartient à $v(\mathcal{E}_{\prec t})$, et le degré dominant est encore 0.

En répétant le même principe, on trouve $x_+ \sim \sqrt{2}i+\frac{5}{8}\sqrt{2}it+(\frac{125}{16}\sqrt{2}i+\frac{1}{2})t^2$, et $x_- \sim -\sqrt{2}i - \frac{5}{8}\sqrt{2}it + (\frac{125}{16}\sqrt{2}i - \frac{1}{2})t^2$.

Il faut ensuite répéter l'algorithme suffisamment de fois pour vérifier que P_A admet une solution qui est une somme finie de monômes en t ou si les deux solutions sont de taille infinie.

Un moyen de prédire le résultat est de conjecturer une expression ou une relation récursive pour les coefficients dans les développements asymptotiques.

On peut avoir une idée avec cet exemple de comment trouver autour de $Y = 0$ une paramétrisation analytique de la forme $(t, f(t))$ de la courbe algébrique $V(X^4 - X^3Y^3 + 2X^2 - 2Y^2X - 5Y)$ associée à $P = X^4 - t^3X^3 + 2X^2 - 2t^2X - 5t$ comme le stipule le théorème de Newton-Puiseux, et même comprendre pourquoi en général les solutions existent dans $\mathbb{C}((t^{\frac{1}{n}\cdot\mathbb{Z}}))$ pour un certain n : il suffit que n soit le *p.p.c.m.* de dénominateurs des antipentes apparues dans l'itération de l'algorithme avant que le degré dominant n'atteigne 1.

Bibliographie

[1] : M. Aschenbrenner, L. van den Dries, J. van der Hoeven, *Real Differential Algebra and Model Theory of Transseries*, http ://arxiv.org/abs/1509.02588v1 (2015).

[2] : I. Kaplansky, *Maximal fields with valuation I*, Duke Mathematical Journal **9** (1942), 303-321.

[3] : K. Pal, *A note on immediate extensions of valued fields A la Kaplansky*,http ://homepage.usask.ca/ kop704/Papers/Kaplansky.pdf