

Université PARIS DIDEROT-PARIS VII
UFR de Mathématiques
École Doctorale de Sciences Mathématiques de Paris Centre (ED386)

THÈSE

en vue de l'obtention du
DOCTORAT de l'UNIVERSITÉ Paris VII
Spécialité : Mathématiques

Modules Valués

en vue d'applications à la théorie des corps valués de caractéristique positive

présentée par **Gönenç Onay**

soutenue publiquement le 1er Décembre 2011

Directrices:

Françoise Delon
Françoise Point

Rapporteurs:

Lou van den Dries
Thomas Scanlon

Jury:

Elisabeth Bouscaren
Françoise Delon
Françoise Point
Mike Prest
Patrick Simonetta
Frank Wagner

Table des matières

Remerciements	iii
Introduction	v
1 Préliminaires	1
1.1 Élimination des quantificateurs pour les modules	1
1.2 Espaces ultramétriques et valuations	2
1.2.1 Groupes valués	2
1.2.2 Corps valués	3
1.3 Anneau des polynômes tordus et polynômes additifs	4
2 R-modules divisibles	7
2.1 Généralités	7
2.2 Complétions de la théorie des R -modules divisibles	9
2.3 Cas des corps	14
3 $K[t; \varphi]$-modules K-trivialement valués : K agit en préservant la valuation	15
3.1 Modules K -trivialement valués	16
3.2 Modules K -trivialement valués divisibles et henséliens	18
3.3 Un principe d’Ax-Kochen et Ershov	21
4 $K[t; \varphi]$-modules valués : K agit par translations sur la valuation	27
4.1 R -chaînes	27
4.2 Modules valués dans une R -chaîne	32
4.3 Extensions de modules valués	33

4.4	Modules valués henséliens	40
4.5	Modules valués résiduellement divisibles	48
4.6	Un principe d’Ax-Kochen et Ershov	53
4.7	Unicité de l’extension immédiate maximale des modules résiduellement divisibles	60
4.8	Un théorème de structure	62
5	$K[t; \varphi]$-modules C-minimaux	67
5.1	Cas fortement minimal	69
5.2	Interlude : conséquences de la C-minimalité	70
5.3	Cas d’une valuation non triviale et K -triviale	70
5.4	Cas d’une valuation non K -triviale	74
6	Modules avec une filtration valuationnelle	77
6.1	La cas parfait	77
6.2	Le $\varphi(K)$ -espace vectoriel K	78
6.3	R -modules filtrés	80
6.4	Matrices sur $K[t; \varphi]$	81
6.5	Élimination des quantificateurs au voisinage de 0	82

Remerciements

Je veux commencer par remercier mes deux directrices : Françoise Delon et Françoise Point. Je remercie Françoise Point pour m'avoir proposé ce sujet fort intéressant ainsi que pour sa présence, ses compétences et sa compréhension mêmes pendant les moments les plus difficiles. Je remercie Françoise Delon avec qui tout échange d'idées mathématique et non mathématique m'a été un grand plaisir. J'espère, grâce à ses efforts formateurs, avoir un peu acquis son agréable manière de la fusion du formalisme avec l'intuition.

Je remercie mes rapporteurs Lou van den Dries et Thomas Scanlon qui ont lu très attentivement cette thèse dans relativement peu de temps. Je dois aussi un grand merci aux membres du jury : Elisabeth Bouscaren, Mike Prest, Patrick Simonetta et Frank Wagner qui ont accepté de se présenter dans ma soutenance organisée dans un temps très limité.

Je remercie tous mes enseignants des mathématiques qui ont certainement indirectement contribué à cette thèse. En commençant par ma maîtresse Meliha Denizli dont son introduction des notions ensemblistes à l'école normale (tout à fait ordinaire) primaire de la rue Gazimuhtar-pasa m'a fourni une base solide jusqu'au niveau License ; sans oublier M. Michael Eisermann à Grenoble et ses travaux dirigés en théorie de Galois et tous ceux qui m'ont appris la logique et la théorie des modèles à Paris 7 : en particulier René Cori, Gabriel Sabbagh, Patrick Simonetta et Zoé Chatzidakis.

Je veux remercier tous mes amis du bureau des thésards. Même si ma présence y était réduite, j'ai apprécié grandement leur gentillesse et leur collaboration. Je me permets de citer juste quelques noms avec lesquels j'ai partagé davantage de temps : Fares, Avenilde, Victor, Karim, David, Rémi, Yann, Pablo et Ana. Un grand merci également au premier mathématicien que j'ai rencontré à Paris, Clément dont l'amitié a toujours compté pour moi.

Cette partie des remerciements resterait incomplète si j'oubliais l'UFR de Mathématique de l'Université Mimar Sinan qui m'accueille depuis quelques mois en m'offrant des très bonnes conditions de travail.

Je remercie mes amis David Rouquet, Marc, Ewaryst, Amandine, Pascale, Henri, Franck, Marion et Martin Hils qui, pendant différents moments de cette thèse, ont partagé mes bonheurs, mes douleurs, mon appartement, leurs appartements, mes idées et mes sentiments intimes.

Je remercie le clan gsl de Paris et d'Europe : en commençant par le XIIIe : Eren, Emre, Kemal, Zeynepsu, Maydo, Orkun, puis le capitaine Bekir d'Allemagne, et puis Nilda et Mine, plus au nord Volkan, Derya, Umut et Lale, le couple (bientôt le triplet) exceptionnel Mitare et Burcu, les deux göziçi Levent et Kaan, l'ancien attaquant Nantais Eylem et sa copine Clémence, Rasim, le pionnier du mouvement sgciste parisien et son épouse Dorothee, Zeren et Emre Abi,

et enfin le maître chocolatier Aylin.

Voici maintenant un grand homme, une grosse tête (dont une petite partie héritée suffit pour accomplir une thèse) mais surtout un grand cœur qui je ne sais comment remercier : mon père Irfan. Un cœur qui, très récemment, a été malheureusement envahi par des plaques d'athéromes. Mais c'est aussi un cœur qui résiste, qui résistera pour partager sa profondeur avec son entourage comme il a fait avec moi durant toute ma vie. Je ne sais non plus comment remercier les deux autres membres de ma petite famille : ma mère Hülya et ma sœur Gözde. Elles m'ont fait toujours sentir leur soutien même de très loin, ce qui a toujours importé dans toutes mes réussites.

Enfin je veux remercier une personne en l'absence de laquelle cette thèse aurait quand même vu sa fin, la théorie des modèles aurait continué son développement, mais je n'aurais eu peut-être qu'elle, cette thèse, mais pas elle, et qu'une vie certainement moins intéressante et moins belle. Başak, je te remercie.

Introduction

Dans cette thèse nous nous proposons d'étudier les R -modules munis d'une distance ultramétrique, où R est un anneau euclidien à droite. Les exemples motivants viennent de la théorie des corps valués en caractéristique positive. De fait, tout corps K de caractéristique $p > 0$ porte canoniquement une structure de module sur son anneau de polynômes additifs, cet anneau est l'ensemble des polynômes de la forme $\sum_i a_i X^{p^i}$.

Les polynômes additifs apparaissent cruciallement dans la théorie des corps surtout depuis l'étude des extensions d'Artin-Schreier, et en théorie des valuations depuis le fameux article de Kaplansky : Maximal fields with valuations. Les polynômes additifs ont été également considérés en théorie des modèles des corps valués par plusieurs mathématiciens du domaine. Notons en particulier Franz-Viktor Kuhlmann (cf. [Kul]), Lou van den Dries et son étudiant Thomas Rohwer, qui a montré que la théorie du corps $\mathbb{F}_p((t))$ sur son anneau de polynômes additifs est modèle-complète dans le langage des modules muni d'un prédicat pour $\mathbb{F}_p[[t]]$ (cf. [Ro]). Le chapitre 6 de cette thèse reprend l'étude de ce cas.

Contenu de la thèse

Le chapitre 1, préliminaires, présente les objets essentiels de notre étude et leurs propriétés, notamment l'anneau $R := K[t; \varphi]$, où K est un corps et φ un endomorphisme de $(K, +, \times, 1, 0)$.

Dans le chapitre 2, nous étudions les R -modules divisibles. Ce sont exactement les R -modules injectifs par le fait que, dans R , tout idéal à droite est principal. On montre l'élimination des quantificateurs pour leurs théories dans le langage des R -modules (cf. le lemme 2.2.1), et on décrit leurs complétions (cf. le corollaire 2.2.21) en établissant que leurs invariants de Baur et Monk sont déterminés par le cardinal des annulateurs des éléments premiers de R .

Au chapitre 3, on introduit la notion de module valué dans le cas simple où les constantes provenant de K^\times agissent en préservant la valuation. On axiomatise les modules valués comme des structures à deux sortes, un R -module M et un ensemble totalement ordonné Δ muni d'une fonction strictement croissante, liés par une valuation du groupe additif $v : M \rightarrow \Delta$. Les modèles usuels dans cette situation sont les corps valués de caractéristique $p > 0$, vus comme modules sur l'anneau des polynômes additifs à coefficients dans un sous-corps valué trivialement. On introduira une propriété analogue à celle exprimée par le lemme de Hensel dans le cas des corps valués (cf. définition 3.2.1). En particulier tout corps de caractéristique positive muni d'une valuation henselienne au sens classique sera henselien en tant que R -module. On constatera tout de suite que l'analogue de la notion d'algébriquement clos, la divisibilité, n'implique pas la propriété de Hensel pour les modules (cf. la proposition 3.2.9).

On considérera alors les modules valués henséliens et divisibles, pour lesquels on établira un résultat de type Ax-Kochen et Ershov (cf. les théorèmes 3.3.8, 3.3.9 et 3.3.10).

Le chapitre 4 généralise les définitions et les techniques provenant du chapitre 3 au cas où K n'agit plus en préservant la valuation. Cette fois, l'ensemble totalement ordonné Δ est muni d'une action de K , qui induit sur K une valuation v_K , et d'une action de R , qui prolonge celle de K . Cela nous amène à étudier dans un premier temps les structures qu'on appelle des R -chaînes. Celles-ci sont une adaptation et/ou généralisation de la situation suivante. Soit (L, v) un corps valué et R l'anneau des polynômes additifs sur L . A un polynôme $F(X) = \sum_i a_i X^{p^i} \in R$ on peut associer la fonction

$$f_F : v(L) \rightarrow v(L), \gamma \mapsto \min_i \{p^i \gamma + v(a_i)\};$$

alors $v(L)$ muni de l'ordre et de ces fonctions est une R -chaîne. Le graphe d'une telle fonction est obtenu en mettant bout à bout des segments des droites $(\gamma, i\gamma + v(a_i))$, pris dans l'ordre décroissant des exposants i . Par l'inégalité ultramétrique, pour chaque polynôme F comme ci-dessus, il existe un sous-ensemble fini $SP(F)$ de $v(L)$ tel que, pour tout $x \in L$ dont la valuation est dans $v(L) \setminus SP(F)$, on a $v(F(x)) = f_F(v(x))$. En fait, les éléments de $SP(F)$ sont les abscisses des points d'intersection des droites $(\gamma, p^i \gamma + v(a_i))_\gamma$ et $(\gamma, p^j \gamma + v(a_j))_\gamma$ pour $i \neq j$. Si $\gamma \in SP(F)$ et $x \in L$ de valuation γ vérifient $v(F(x)) \neq \min_i \{p^i \gamma + v(a_i)\}$, alors on appellera γ un « saut » de F et x un élément « irrégulier » pour F . Par exemple, le seul saut du polynôme d'Artin-Schreier $X^p - X$ est 0. En termes de modules valués, on appellera irrégulier pour $r \in R$ tout élément x tel que $v(x.r) > v(x) \cdot r$, où l'action à droite $\cdot r$ est l'analogue de la fonction f_F ci-dessus. Il crucial pour nos intérêts d'avoir le plus d'informations possible sur le comportement des points irréguliers pour r . Pour cela, étant donnés r et un élément x irrégulier pour r , le mieux que l'on peut espérer c'est d'avoir un autre élément y tel que $y.r = x.r$ et y régulier pour r , i.e. $v(y.r) = v(y) \cdot r$. On verra qu'un corps (L, v) de caractéristique $p > 0$ (vu comme $L[t; x \mapsto x^p]$ -module valué) satisfait cette propriété si, et seulement si, c'est un corps de Kaplansky algébriquement maximal (cf. le théorème 4.5.12 avec le corollaire 4.3.20).

Ces propriétés sont également nécessaires pour avoir un résultat de type Ax-Kochen et Ershov dans le langage des R -modules valués. En effet, si K est le corps des séries de Puiseux en la variable Y sur un corps fini, on remarque que deux extensions algébriquement maximales de K , dont l'une contient une racine de $X^p - X - 1 - (1/Y)$ et l'autre n'en contient pas, ne sont pas élémentairement équivalentes dans le langage des purs R -modules (cf. 4.3.23). Pourtant, d'après les résultats de F.-V. Kuhlmann, on sait qu'elles le sont dans le langage des corps. Cela montre que le langage des modules ne permet d'avoir des résultats aussi forts. En effet, le langage des modules, du fait qu'il contient un symbole de fonction pour chaque polynôme additif, permet d'exprimer sans paramètre des propriétés qui dépendent des coefficients de ces polynômes. On montre alors le résultat d'Ax-Kochen et Ershov pour les modules valués dits « affinement maximaux et résiduellement divisibles » (cf. théorème 4.6.3), et on termine ce chapitre en établissant un résultat de structure des corps de Kaplansky maximaux vu comme modules valués (cf. théorème 4.8.4).

Le chapitre 5 permet d'établir les conséquences des résultats qui précèdent du point de vue de la C -minimalité. Comme on l'a constaté dans le chapitre 4, il y a une valuation v_K induite sur K par son action sur Δ . On va séparer deux cas. Si v_K est non triviale on verra que les modules valués C -minimaux sont exactement ceux qui sont affinement maximaux, résiduellement divisibles et qui possèdent une chaîne o -minimale. Si v_K est triviale, il découle du chapitre 3 que les modules henséliens, divisibles et avec une chaîne o -minimale sont C -minimaux. On verra qu'il y en a d'autres, par exemple l'anneau des séries de Puiseux sur un

corps fini \mathbb{F}_q comme module valué sur l'anneau des polynômes additifs à coefficients dans \mathbb{F}_q (cf. le corollaire 5.3.3).

Enfin au chapitre 6, on examine les modules que l'on appelle filtrés, comme des structures additives à une seule sorte munies des prédicats unaires $(P_\delta)_\delta$ indexés par une R -chaîne Δ , dont les interprétations naturelles dans les modules valués sont les boules centrées en 0. On met en place un système d'axiomes dont les modèles sont en particulier les corps valués henséliens (K, v) , non parfaits et tels que $[K : K^p]$ est fini ; notre langage sera alors enrichi des fonctions $(\lambda_i)_{0 \leq i < p}$, l'interprétation de λ_i étant dans ce cas la fonction qui à un $x \in K$, associe la racine p -ième du i -ème coefficient de x dans une base fixée $(\alpha_i)_i$ du K^p -espace vectoriel K . Alors, dans cette théorie, on montre grâce à une propriété analogue au lemme de Hensel, ce que nous appelons une élimination de quantificateur au voisinage de 0 : étant donnée une formule p.p. $\phi(x_1, \dots, x_n)$ dans le langage des R -module enrichi des prédicats P_δ , pour un certain produit cartésien $V := P_{\delta_1} \times \dots \times P_{\delta_n}$, l'intersection $\phi \cap V$ est définissable sans quantificateurs dans le langage avec les fonctions λ_i (cf. proposition 6.5.2).

Chapitre 1

Préliminaires

Ce chapitre consiste en une brève présentation des concepts et résultats de base sur la théorie des modèles des modules, sur la théorie des valuations et sur les anneaux d'Ore. En particulier, on présente l'anneau $K[t, \varphi]$, pour K un corps et $\varphi \in \text{End}(K, +, \times)$; c'est cet anneau sur lequel nos modules seront définis durant les chapitres 2 à 6.

Noter que les définitions 1.3.2 et 1.3.4 sont propres à cette thèse et seront utilisés couramment dans les chapitres qui suivent.

Les ouvrages de base auxquels l'on s'est référé sont [Co] pour la théorie des anneaux d'Ore, [Ho] pour la théorie des modèles des modules, et [Ef] pour la théorie des valuations.

Sauf mention du contraire, tout anneau sera unitaire et tout module sera un module à droite. Quand M est un module sur un anneau A , on notera $m.a$ la multiplication par le scalaire $a \in A$, de l'élément $m \in M$.

1.1 Élimination des quantificateurs pour les modules

Rappelons quelques propriétés modèles-théoriques des modules. Soit U un anneau et L_U le langage des U -modules, i.e. le langage des groupes abéliens enrichi d'un symbole de fonction unaire r pour chaque éléments de U , qui sera interprété comme la multiplication par ce scalaire. Une formule dite primitive positive (p.p.) d'un langage de premier ordre n'est qu'une formule de la forme $\exists y_1, \dots, y_n \psi$, où ψ est une conjonction de formules atomiques. Les formules primitives positives de L_U sont les formules existentielles de la forme :

$$\exists y_1, \dots, \exists y_m \bigwedge_i \left(\sum_{j=1}^l x_j \cdot r_{i,j} - \sum_{k=1}^m y_k \cdot q_{i,k} \right) = 0,$$

qu'on peut aussi écrire comme :

$$\exists y_1, \dots, \exists y_m ((x_1, \dots, x_l).B - (y_1, \dots, y_m).A) = 0$$

où $A = (r_{i,j})$ et $B = (q_{i,k})$ sont des matrices à coefficients dans U .

Définition 1.1.1. Soit M un module sur un anneau U , quelconque. Chaque formule p.p à

une variable libre définit un sous-groupe de M . Pour deux telles formules p.p. $\psi(x)$ et $\phi(x)$ et pour chaque $m \in \mathbb{N}$, on peut construire un énoncé $\text{Inv}(\phi, \psi, m)$ tel que

$$M \models \text{Inv}(\phi, \psi, m) \quad \text{si et seulement si} \quad \left| \frac{\phi(M)}{\phi(M) \cap \psi(M)} \right| \leq m.$$

Un énoncé de type $\text{Inv}(\phi, \psi, m)$ s'appelle énoncé invariant.

Dans le chapitre 6 on utilisera le théorème de Baur-Monk, qui s'énonce comme suit :

Théorème 1.1.2 (Baur-Monk). *Soit U un anneau, $L_U = \{0, +, -, (r)_{r \in U}\}$ le langage des U -modules et T la L_U -théorie des U -modules à droite. Alors toute formule $\phi(x_1, \dots, x_n)$ de L_U est équivalente modulo T à une combinaison booléenne de formules p.p. et d'énoncés invariants.*

PREUVE. Voir [Ho], p.655 corollaire A.1.2. ■

Remarque 1.1.3. Comme il est discuté dans [Ho] p. 655 juste après le corollaire A.1.2., le résultat ci-dessus est aussi satisfait quand on enrichit le langage L_U , avec des prédicats unaires $(P_i)_{i \in I}$, interprétés comme des sous-groupes.

1.2 Espaces ultramétriques et valuations

1.2.1 Groupes valués

Définition 1.2.1. Un ensemble E accompagné d'une chaîne $(\Delta, \leq, 0)$ où 0 est un élément minimal, et d'une fonction $d : E^2 \rightarrow \Delta$, satisfaisant $d(x, y) = 0$ si et seulement si $x = y$, $d(x, y) = d(y, x)$ pour tout $(x, y) \in E^2$ et vérifiant pour tous x, y, z l'inégalité ultramétrique

$$d(x, z) \leq \max\{d(x, y), d(y, z)\} \tag{1.1}$$

est appelé un espace ultramétrique.

Définition 1.2.2. On appellera groupe valué une structure à deux sortes $\mathcal{G} = (G, \Delta, +, 0, <, v, \infty)$, telle que $(G, +, 0)$ est un groupe abélien, $(\Delta, <)$ une chaîne ayant un plus grand élément ∞ et $v : G \rightarrow \Delta$ une fonction surjective vérifiant

1. $\forall x \ v(x) = v(-x)$,
2. $\forall x \forall y \ v(x - y) \geq \min\{v(x), v(y)\}$,
3. $v(x) = \infty \iff x = 0$.

Pour $(a, \gamma) \in G \times \Delta$, on appelle boule ouverte (respectivement boule fermée) de centre a et de rayon γ , l'ensemble $B(a, \gamma) := \{x \in G \mid v(x - a) > \gamma\}$ (respectivement l'ensemble $B[a, \delta] := \{x \in G \mid v(x - a) \geq \delta\}$).

Par la suite, on notera (G, v) un groupe valué.

Remarque 1.2.3. Tout groupe valué (G, v) induit canoniquement une structure d'espace ultramétrique quand on définit $d(x, y) := v(x - y)$ et qu'on prend la chaîne Δ munie de l'ordre inverse.

Soit (G, v) un groupe valué. L'application $(x, y) \mapsto v(x - y)$ induit une topologie dont une base est donnée par les boules ouvertes. On a : pour tous $a, b \in G$ et $\gamma \in \Delta$, $a \in B(b, \gamma)$ si et seulement si $B(a, \gamma) = B(b, \gamma)$. Il en résulte qu'une boule ouverte est également fermée.

Présentation équivalente : Soit $(I, <)$ un ensemble totalement ordonné avec un maximum ∞ , G un groupe abélien et $(G_i)_{i \in I}$ une chaîne de sous-groupes de G d'intersection triviale, telle que $G_i \subset G_j$ si et seulement si $i \geq j$, et que, pour tout $x \in G$, il existe un plus grand $i \in I$ pour lequel $x \in G_i$. Alors en particulier $G_\infty = \{0\}$ et la fonction $v : G \rightarrow I$, définie par l'équivalence

$$v(x) = i \Leftrightarrow x \in G_i \setminus \left(\bigcup_{j > i} G_j \right),$$

est une valuation sur G .

Notation 1.2.4. Soit $\mathcal{G} = (G, \Delta)$ un groupe valué. On désignera la boule fermée (respectivement ouverte) de centre 0 et de rayon γ , par $G_{\geq \gamma}$ (respectivement par $G_{> \gamma}$). Notons que ces boules sont des sous-groupes de G . Par ailleurs, on note $G_\gamma(a)$ le quotient de la boule fermée centrée en a et de rayon γ , par la relation d'équivalence : $v(x - y) > \gamma$. En particulier $G_\gamma(0)$ est le quotient $G_{\geq \gamma}/G_{> \gamma}$.

Remarque 1.2.5. Puisque les boules ouvertes (respectivement fermées) de même rayon sont en bijection par translation, pour tous $a \in G$ et $\gamma \in \Delta$, $|G_\gamma(a)| = |G_\gamma(0)|$.

Définition 1.2.6. Soit (E, d) un espace ultramétrique. On appelle suite pseudo-Cauchy une suite $(a_\lambda)_{\lambda \in \Lambda}$ de E , indexée par un ordinal limite Λ , et telle que, pour $\rho < \mu < \delta$ dans Λ tous suffisamment grands, on a

$$d(a_\delta, a_\mu) < d(a_\mu, a_\rho). \quad (1.2)$$

On dit qu'un élément $a \in E$ est limite de la suite pseudo-Cauchy $(a_\rho)_\rho$ si $d(a, a_\rho) = d(a_{\rho+1}, a_\rho)$ pour ρ suffisamment grand.

Remarque 1.2.7. Nous redéfinirons et parlerons davantage des suites pseudo-Cauchy dans le chapitre 4, section « extensions de modules valués », la définition ci-dessus est donnée pour la compréhension de la suite des ces préliminaires.

1.2.2 Corps valués

Définition 1.2.8. Soit K un corps. Si $(K, +)$ est muni d'une structure de groupe valué avec v tel que $v(K) \setminus \{\infty\}$ est un groupe abélien ordonné et que la restriction de v à K^\times est un morphisme de groupe, on dit que K est un corps valué et on le note (K, v) .

Remarque 1.2.9. On peut étendre l'addition à $v(K)$ en posant $\infty + \infty = \infty + \gamma = \gamma + \infty = \infty$.

Rappelons quelques résultats concernant les corps valués. Soit (K, v) un corps valué. On vérifie que l'ensemble des éléments de valuation ≥ 0 forment un anneau, \mathcal{O}_K , que l'on appelle l'anneau de valuation de K . On dit que v est triviale sur K si $\mathcal{O}_K = K$. Les éléments de valuation nulle de K sont exactement les inversibles de \mathcal{O}_K , on note leur ensemble U . Alors $\mathcal{M}_K := \mathcal{O}_K \setminus U$ est un idéal maximal de \mathcal{O}_K , \mathcal{O}_K est un anneau local, et $k_K := \mathcal{O}_K/\mathcal{M}_K$ est un corps que l'on appellera le corps résiduel de (K, v) . Si le corps K est de caractéristique $p > 0$, alors il en va de même pour k_K . Par ailleurs, il existe des corps valués de caractéristique 0 dont la caractéristique résiduelle est $p > 0$, par exemple le corps \mathbb{Q}_p des nombres p -adiques muni de la valuation p -adique. En résumé : $(\text{car } K, \text{car } k_K) \in \{(0, 0), (0, p), (p, p)\}$.

Une extension (L, w) de (K, v) est une extension de corps, telle que la restriction de w à K est v . On dit que c'est une extension immédiate si $v(K) = v(L)$ et $k_K = k_L$, c'est-à-dire si les inclusions canoniques $v(K) \subset v(L)$ et $k_K \subset k_L$ sont surjectives. On appelle alors maximal un corps valué qui n'a pas d'extension immédiate propre. On a le théorème suivant de Kaplansky ([Ka]).

Théorème 1.2.10. *Un corps valué (K, v) est maximal si, et seulement si, chaque suite pseudo-Cauchy admet une limite dans (K, v) .*

Finalement, on donne la définition d'un corps valué hensélien. Noter qu'il existe plusieurs définitions équivalentes dans la littérature (cf. [Ef] par exemple).

Définition 1.2.11. Soit $P(X) = X^n a_n + \dots + a_0 \in \mathcal{O}_K[X]$. Une racine résiduelle de P est une racine (dans k_K) de $\bar{P} := X^n \bar{a}_n + \dots + \bar{a}_0$, avec $\bar{a}_i = a_i/M_K$. On dit que le corps valué (K, v) est hensélien si tout polynôme unitaire $P \in \mathcal{O}_K[X]$ admettant une racine résiduelle simple $\bar{b} \in k_K$ admet une racine $a \in \mathcal{O}_K$ telle que $\bar{a} = \bar{b}$.

Le lemme suivant caractérise également les corps valués henséliens. Le point c . ci-dessous dit que l'image d'un polynôme non nul de $X\mathcal{O}_K[X] \setminus X^2\mathcal{O}_K[X]$ contient tout élément de valuation suffisamment grande. C'est cette approche qu'on va adapter quand on définira les modules valués henséliens (cf. chapitre 3 et 4, définitions 3.1.8 et 4.4.7).

Lemme 1.2.12. *Les assertions suivantes sont équivalentes :*

- a. (K, v) est hensélien.
- b. Si $P \in \mathcal{O}_K[X]$ et $a \in \mathcal{O}_K$ sont tels que $v(P(a)) > v(P'(a))$ et $v(P'(a)) = 0$, alors il existe une racine $b \in K$ de P telle que $v(a - b) > 0$.
- c. Si $P \in \mathcal{O}_K[X]$ est tel que $v(P(0)) > 2v(P'(0))$, alors P a une racine $b \in K$ telle que $v(P(0)) - v(P'(0)) = v(b)$.

PREUVE. Toutes ces assertions sont des conséquences immédiates du théorème 18.1.2 dans [Ef]. ■

On note également :

Théorème 1.2.13. *Tout corps valué (K, v) admet une plus petite extension hensélienne. De telles extensions sont algébriques, séparables et immédiates. Elles sont toutes K -isomorphes. En particulier, les corps valués maximaux sont henséliens.*

1.3 Anneau des polynômes tordus et polynômes additifs

Soit K un corps commutatif de caractéristique $p \neq 0$. On appelle polynôme additif un élément P de $K[X]$ tel que, dans toute extension $L \supset K$, pour tous $x, y \in L$, $P(x + y) = P(x) + P(y)$. Par exemple le polynôme d'Artin-Schreier est additif. On peut montrer que tout tel polynôme s'écrit comme $\sum_{i=0}^n X^{p^i} a_i$. Ces polynômes ont été introduits et étudiés par O. Ore dans l'article [Ore].

De manière plus générale, soit K un corps commutatif et φ un endomorphisme de $(K, +, \cdot)$. On construit l'anneau R comme l'anneau engendré par les éléments de K et par un symbole t , et satisfaisant la relation $at = t\varphi(a)$, i.e. $R := K\langle t; at = t\varphi(a), a \in K \rangle$. Tout élément f de R s'écrit de façon unique comme $\sum_{i \in I} t^i a_i$ avec I fini, et $a_i \neq 0$; l'entier $\max I$ est noté $\deg(f)$. On appellera parfois aussi polynôme un élément de R . Il est facile de voir que R est euclidien à gauche avec la fonction \deg . De plus, si φ est un automorphisme, alors R est aussi euclidien à droite. On notera également cet anneau $K[t; \varphi]$. Pour plus de détails on renvoie à [Co], à la proposition 2.1.1.

Par ailleurs K se plonge dans l'anneau des endomorphismes de $(K, +)$ par $a \mapsto m_a$ avec $m_a : y \mapsto ay$. Si, $f, g \in \text{End}(K, +)$, désignons par le composé $f \circ g$ l'application $x \mapsto g(f(x))$. Avec cette notation : $m_a \circ \varphi = \varphi \circ m_{\varphi(a)}$. Considérons l'ensemble constitué des sommes finies $\sum_{i=0}^n \varphi^i \circ m_{a_i}$. Cet ensemble est le sous-anneau R' de $\text{End}(K, +)$ engendré par les m_a et φ . Ainsi le morphisme d'anneau $R \rightarrow R'$, $t^d a_d + \dots a_0 \mapsto \varphi^d \circ m_{a_d} + \dots + m_{a_0}$ est surjectif et R' est un quotient de R .

Sauf mention du contraire durant tout le reste de ce texte K désignera un corps abstrait, et φ un endomorphisme de $(K, +, \times, 0, 1)$. Remarquons que K est toujours un $K[t; \varphi]$ -module, en interprétant $x.t$ par $\varphi(x)$. Quand K est de caractéristique $p > 0$, K hérite donc canoniquement d'une structure de $K[t; x \mapsto x^p]$ -module. Ainsi, dans cette thèse, l'expression $K[t; x \mapsto x^p]$ -module désignera toujours une extension (de corps) de K , où on interprète $x.t$ par x^p .

Notons tout de suite une propriété liant les polynôme additifs et les polynômes usuels :

Théorème 1.3.1. *Si K est un corps de caractéristique $p > 0$, alors, tout polynôme de $K[X]$ divise un polynôme additif.*

PREUVE. C'est le théorème 1 dans [Ore], chapitre 3. ■

Définition 1.3.2. On dit qu'un polynôme $q = \sum_{i=0}^n t^i a_i \in R$ est séparable si $a_0 \neq 0$. On dit qu'un élément $q \in R \setminus K$ est premier s'il est séparable et s'il n'existe pas $q_1, q_2 \in R \setminus K$, tels que $q = q_1 q_2$. On notera R_{sep} le sous-ensemble des éléments séparables.

Remarque 1.3.3. Par l'algorithme d'Euclide à droite tout élément $q \neq 0$ de R s'écrit comme $t^n p_1 \dots p_k$, où les p_i sont premiers. En particulier tout élément de R s'écrit de manière unique comme $t^n r'$ avec r' séparable.

Définition 1.3.4. Soit $r \in R \setminus \{0\}$ que l'on écrit comme $t^n r'$ avec r' séparable. On appelle cet entier n le **degré d'inséparabilité** de r , et on le note $\text{deg}_{is}(r)$. Alors on note $\text{deg}_s(r) := \text{deg}(r) - n$, et on l'appelle le **degré de séparabilité** de r .

Notation 1.3.5. Soit $0 \neq q = \sum_{i=0}^n t^i a_i \in R$. Alors $qt^n = t^n \sum_{i=0}^n t^i \varphi^n(a_i)$ et on pose $q^{\varphi^n} := \sum_{i=0}^n t^i \varphi^n(a_i)$.

Définition 1.3.6. On dira qu'un anneau est d'Ore à droite s'il est intègre et si tous $a, b \in R \setminus \{0\}$ ont un multiple commun, i.e. $aR \cap bR \neq 0$.

Proposition 1.3.7. 1. *Tout anneau d'Ore (à droite) admet un corps de fraction.*

2. *L'anneau R étant principal à droite, est en particulier d'Ore. De plus, étant donnés deux élément non nuls a, b de R , il existe un plus petit (au sens de la relation de divisibilité sur R) multiple commun de a et b , que l'on notera $\text{ppcm}(a, b)$; de même il existe un plus petit diviseur commun de a et b , qui sera noté $\text{pgcd}(a, b)$.*

PREUVE. Pour 1. voir [Co] (corollary 1.3.3 & proposition 1.3.4). Un anneau L qui est d'Ore à droite admet un unique corps de fractions, qui est égal au quotient de $L \times L \setminus \{0\}$ par la relation d'équivalence \mathfrak{R} suivante :

$$(a, b) \mathfrak{R} (a', b') \quad \text{s'il existe } u, v \in L \setminus \{0\} \text{ tels que } au = a'v, bu = b'v.$$

1. Dans l'article [Ore], ce qui est appelé « p -polynomial» n'est rien d'autre qu'un polynôme additif; cela étant, surtout depuis l'article [Ka] plusieurs auteurs appellent p -polynôme une somme de la forme $F + a$, où F est un polynôme additif et a une constante.

L'existence du ppcm et du pgcd découle du fait R est euclidien. ■

Notation 1.3.8. Durant tout ce texte, sauf mention du contraire, on notera D le corps de fractions de l'anneau R .

Chapitre 2

R -modules divisibles

Soit comme précédemment K un corps, φ un endomorphisme de K , $K_0 = \text{Fix}(\varphi)$, $R = K[t; \varphi]$ et $D = \text{Frac}(R)$. Dans ce qui suit on considérera toujours des R -modules à droite.

Dans ce chapitre on rappellera d'abord les généralités sur les modules sur un anneau intègre et principal à droite (i.e. tout idéal à droite est principal), ce qui est le cas de R . Sur un tel anneau, les modules divisibles sont exactement les modules injectifs (voir 2.1.3). Ensuite, on établit l'élimination des quantificateurs pour la théorie des R -modules divisibles (voir 2.2.1). Puis on considère les R -modules divisibles où t n'a pas torsion. On montre que les invariants de Baur et Monk de tels modules M sont de la forme $|\text{ann}_M(r)/\text{ann}_M(q)|$, où $r, q \in R \setminus \{0\}$ et $\text{ann}_M(q)$ désigne l'ensemble $\{x \in M \mid x.q = 0\}$. Ce dernier résultat est montré d'abord avec l'hypothèse que chaque r premier a une torsion non nul (voir 2.2.7), puis en omettant cette hypothèse (voir 2.2.10). Cela permet de décrire les complétions de la théorie des R -modules sans t -torsion (voir 2.2.21). Enfin, on donne les conséquences sur les corps de caractéristique $p > 0$ vus comme modules sur un anneau de polynômes additifs. Notons que les $K[t; \varphi]$ -modules divisibles ont été aussi étudiés dans [HrPo] dans le cas où φ est un automorphisme de K . Ici, on suppose seulement que φ est un endomorphisme de $(K, +, \times, 0, 1)$.

Notons que dans les chapitres 3 et 4, les classes des R -modules valués pour lesquelles on établit des principes d'Ax, Kochen et Ershov sont des sous-classes des R -modules divisibles. Dans le chapitre 5, on verra que les R -modules divisibles M , où pour chaque $r \in R \setminus \{0\}$, $\text{ann}_M(r)$ est fini, sont fortement minimaux.

2.1 Généralités

Définition 2.1.1. On dit qu'un R -module M est divisible si, pour tout $r \in R \setminus \{0\}$, pour tout $x \in M$, il existe $y \in M$ tel que $x = y.r$.

Lemme 2.1.2. *Tout R -module divisible sans torsion porte une unique structure de D -espace vectoriel. En conséquence tout isomorphisme de R -module entre deux tels modules induit un isomorphisme de D -espace vectoriel.*

PREUVE. Soit N un R -module divisible sans torsion, $x \in N$ et $q', q \in R$, $q \neq 0$. On définit $x.(q'/q)$ comme $y \in N$ tel que $y.q = x.q'$. Un tel y existe et est uniquement déterminé car N

est sans torsion. La deuxième assertion découle de cette construction. ■

Lemme 2.1.3. 1. *Un module divisible sur un anneau tel que tout idéal à droite est principal est injectif, et un module injectif sur un anneau intègre est divisible. En particulier pour tout R -module M , M est divisible si et seulement s'il est injectif.*

2. *Tout module A se plonge dans un module injectif; il existe des modules injectifs contenant A et minimaux pour l'ordre de plongement; de plus, de tels modules sont isomorphes au-dessus de A . On les appelle enveloppes injectives de A .*

3. *Si N est un module injectif et $A \subset N$ un sous-module, alors il existe des sous-modules injectifs de N , contenant A et minimaux pour l'inclusion : ce sont exactement les extensions essentielles maximales (pour l'inclusion) de A , c'est-à-dire les extensions $E \supset A$ maximales pour la propriété*

$$\ll X \cap A = 0 \Rightarrow X = 0, \text{ pour tout sous-module } X \subset E \gg.$$

4. *Si $B \supset A$ est une enveloppe injective d'un module A et $x \in B \setminus \{0\}$, alors il existe $r \in R \setminus \{0\}$ tel que $x.r \in A \setminus \{0\}$.*

PREUVE. On renvoie à [Ja] (p. 156-164). La dernière assertion est l'exercice 3. de la page 164. ■

Observation 2.1.4. 1. Ainsi on réservera l'expression «clôture divisible de A » pour celles des enveloppes injectives qui contiennent A .

2. Quand on considérera des «modules valués» (cf. chapitre 3-5), on verra que les différentes clôtures divisibles ne sont en général ni isomorphes ni même élémentairement équivalentes en tant que modules valués.

Notation 2.1.5. Soit M un R -module. On note M_{tor} l'ensemble $\{x \in M \mid \text{il existe } r \in R \setminus \{0\} \text{ tel que } x.r = 0\}$. On dit qu'un sous-module A de M est sans torsion si $A \cap M_{tor} = \{0\}$.

Lemme 2.1.6. *Si M est un R -module divisible alors M_{tor} est un sous-module divisible de M .*

PREUVE. R étant un anneau d'Ore, M_{tor} est un sous-module (cf. [DDP1] proposition 3.5). De plus, si $0 \neq x \in M_{tor}$, avec $q \in R \setminus \{0\}$ tel que $x.q = 0$ alors, pour tout $r \in R \setminus \{0\}$ et pour tout $y \in M$ tel que $y.r = x$, on a $y.rq = 0$. En conséquence $y \in M_{tor}$, ce qui montre que M_{tor} est divisible. ■

Corollaire 2.1.7 (des lemmes 2.1.3 et 2.1.6). *Le sous-module de torsion d'un R -module divisible y est facteur direct. Par conséquent si A et B sont deux R -modules divisibles qui ne sont pas de torsion, alors ils sont élémentairement équivalents si et seulement si $A_{tor} \cong B_{tor}$.*

PREUVE. Par le lemme 2.1.6 le sous-module de torsion d'un module divisible est divisible et donc par le lemme 2.1.3 il est facteur direct. Il vient $A = A_{tor} \oplus A'$ et $B = B_{tor} \oplus B'$. Dans ce cas A' et B' sont des D -espaces vectoriels par le lemme 2.1.2. Ils sont tous les deux non-nuls par hypothèse. Donc ils sont infinis car R est infini. Par conséquent ils sont élémentairement équivalents. La conclusion découle alors du théorème de Feferman-Vaught (cf. par exemple [Ho] section 9.6 pour ce théorème). ■

2.2 Complétions de la théorie des R -modules divisibles

Proposition 2.2.1. *Toute formule p.p. est équivalente modulo la théorie des R -modules divisibles à une conjonction de formules atomiques. En conséquence, les p.p. formules à une seule variable libre ne définissent que les annulateurs des éléments de R .*

PREUVE. Soit $\phi(x_1, \dots, x_n)$ une p.p. formule, que l'on écrit sous la forme :

$$\exists y_1, \dots, y_k \bar{y}.A = \bar{x}.B,$$

où A (respectivement B) est une $k \times m$ matrice (respectivement $n \times m$) à coefficients dans R . Par la proposition 6.1 de [DDP1], il existe des matrices inversibles P et Q , avec P à coefficients dans $\{0, 1\}$, telles que $A' := PAQ$ est de la forme $(A_1, 0)$, où A_1 est une $k \times l$ matrice triangulaire inférieure dont chaque élément sur la diagonale est non nul, et 0 est la $k \times (m - l)$ matrice nulle. Donc ϕ est équivalente à la formule :

$$\exists y_1, \dots, y_k \bar{y}.PAQ = \bar{x}.BQ.$$

Alors, quitte à remplacer A par A' et B par BQ , on peut supposer que A est de la forme $(A_1, 0)$ décrite ci-dessus. Il vient que ϕ est de la forme $\phi_1(\bar{x}, \bar{y}) \wedge \phi_2(\bar{x})$, où ϕ_1 s'écrit comme

$$\exists \bar{y} \bar{y}.A_1 = \left(\sum_{i=1}^n x_i.b_{i,1}, \dots, \sum_{i=1}^n x_i.b_{i,l} \right).$$

et ϕ_2 comme

$$\left(\sum_{i=1}^n x_i.b_{i,l+1}, \dots, \sum_{i=1}^n x_i.b_{i,m} \right) = (0, \dots, 0).$$

Puisque tout modèle de $T_{R,d}$ est divisible et que les éléments diagonaux de A_1 sont tous non-nuls, $T_{R,d} \models \forall \bar{x} \phi_1(\bar{x})$. D'où ϕ est équivalente à ϕ_2 . En particulier, si x représente une seule variable, on a : $\phi(x) \longleftrightarrow \bigwedge_{j=l+1}^m x.b_{1,j} = 0 \longleftrightarrow x.\text{pgcd}(b_{1,l+1}, \dots, b_{1,m}) = 0$. \blacksquare

Corollaire 2.2.2. *Toute complétion de $T_{R,d}$ élimine les quantificateurs.*

PREUVE. Soit T_c est une telle complétion. Par le théorème 1.1.2 toute formule est équivalente modulo T_c , à une combinaison booléenne de formules p.p. Le résultat découle donc du lemme précédent. \blacksquare

Définition 2.2.3. Soit M un R -module. On désignera par $\text{ann}_M(r)$ l'ensemble $\{x \in M \mid x.r = 0\}$.

Remarque 2.2.4. L'ensemble $\text{ann}_M(r)$ est un K_0 -espace vectoriel (rappelons que K_0 désigne $\text{Fix}(\varphi)$).

Soit $T_{R,d}$ la théorie des R -modules divisibles sans t -torsion, i.e. dans lesquels l'application $x \mapsto x.t$ est injective. Sauf mention contraire dans ce qui suit, M désignera un modèle de $T_{R,d}$. Dans un premier temps, on considère la théorie $T' = T_{R,d} \cup \{\exists y \ y \neq 0 \wedge y.q = 0; q \in$

R, q premier}. Cela exprime donc que, dans tout modèle de T' , pour tout élément q de R qui n'est pas un monôme, $\text{ann}_M(q)$ contient un élément non-nul.

Observons d'abord un résultat essentiel :

Lemme 2.2.5. *Soit M un R -module, $A \subset M$ un sous-module de M et $x \in M \setminus A$ tel que $x.r \in A$ pour un certain $r \in R \setminus \{0\}$. Alors il existe $q \in R$ de degré minimal tel que $x.q \in A$. Pour tout tel q et tout r tel que $x.r \in A$, q divise r . Si de plus q est unitaire alors on l'appelle le polynôme minimal de x sur A . En particulier, pour tout $x \in M_{\text{tor}} \setminus \{0\}$, il existe un unique polynôme unitaire de degré minimal tel que $x.q = 0$. On l'appelle le polynôme minimal de x .*

PREUVE. Soit $I = \{r \in R \mid x.r \in A\}$; I est un idéal à droite, et donc principal. D'où il existe un générateur de I , qu'on peut prendre comme q . ■

Remarque 2.2.6. Le polynôme minimal d'un élément n'est pas nécessairement premier.

Jusqu'à la fin de cette section, le symbole « \simeq » exprimera l'isomorphisme entre deux K_0 -espaces vectoriels. Les lemmes qui suivent établissent une généralisation des lemmes 2.9 et 2.10 de [HrPo] qui supposent que φ est un automorphisme de K .

Lemme 2.2.7. *Soit $M \models T'$ et $q, r \in R \setminus \{0\}$ vérifiant $\text{ann}_M(q) \subseteq \text{ann}_M(r)$. Si q est séparable alors q divise r . Dans ce cas, pour $q' \in R$ tel que $r = qq'$, on a $\text{ann}_M(r)/\text{ann}_M(q) \simeq \text{ann}_M(q')$. Si $q = t^n s$ avec s séparable alors s divise r^{φ^n} et $\text{ann}_M(r)/\text{ann}_M(q) \simeq \text{ann}_M(r^{\varphi^n})/\text{ann}_M(s)$.*

PREUVE. Supposons q séparable. Remarquons que si q est premier alors (quitte à multiplier par un élément de K^\times) q est le polynôme minimal de tout élément non nul de $\text{ann}_M(q)$. Donc q divise r , par le lemme 2.2.5. Dans le cas général, comme q est séparable, on peut écrire $q = q_1 \dots q_n$, où pour tout i , q_i est premier (où on autorise $q_i = q_j$ avec $i \neq j$). On procède par induction. Supposons que $q' = q_1 \dots q_{n-1}$ divise r , donc $r = q'r'$. Soit $x \in M$ une racine non nulle de q_n et $x' \in M$ tel que $x'.q' = x$, alors $x'.q = 0$. Puisque $\text{ann}_M(q) \subseteq \text{ann}_M(r)$, $x'.r = 0$, ce qui implique $x.r' = 0$. Par conséquent q_n divise r' et ainsi q divise r . Maintenant, puisque M est divisible, l'application K_0 -linéaire $x \mapsto x.q$ induit une surjection $\text{ann}_M(r) \rightarrow \text{ann}_M(q')$ ayant comme noyau $\text{ann}_M(q)$. Donc on a $\text{ann}_M(r)/\text{ann}_M(q) \simeq \text{ann}_M(q')$.

Supposons $q = t^n s$ avec n non nul et s séparable. Alors, puisqu'il n'y a pas de t -torsion, $\text{ann}_M(s) = (\text{ann}_M(q)).t^n \subseteq (\text{ann}_M(r)).t^n$. Voyons que $(\text{ann}_M(r)).t^n = \text{ann}_M(r^{\varphi^n})$. Soit $x \in (\text{ann}_M(r)).t^n$. Écrivons $x = x'.t^n$, avec $x'.r = 0$. Alors, $x.r^{\varphi^n} = x'.rt^n = 0$. Réciproquement, si $x.r^{\varphi^n} = 0$ alors pour x' tel que $x'.t^n = x$, on a $x'.rt^n = x.r^{\varphi^n} = 0$. Donc $x'.r = 0$ et par le paragraphe ci-dessus, s divise r^{φ^n} . Enfin, comme la multiplication par t^n induit un automorphisme de K_0 -espace vectoriel de M , on a $\text{ann}_M(r)/\text{ann}_M(q) \simeq \text{ann}_M(r^{\varphi^n})/\text{ann}_M(s)$. ■

Corollaire 2.2.8. *Si $M \models T'$, pour tout $0 \neq q = t^n q_1 \dots q_k \in R$, on a*

$$|\text{ann}_M(q)| = \prod_{i=1}^k |\text{ann}_M(q_i)|,$$

où $|\text{ann}_M(q_i)|$ est à valeurs cardinales.

Corollaire 2.2.9. *Les complétions de la théorie T' sont obtenues en spécifiant pour chaque q premier, le nombre ($\in \mathbb{N} \cup \{\infty\}$) d'éléments de $\text{ann}_M(q)$ et elles admettent l'élimination des quantificateurs. En particulier, si K_0 est infini, alors T' est complète.*

PREUVE. Par la proposition 2.2.1 toute p.p. formule sans paramètre définit $\text{ann}_M(q)$ pour un certain $q \in R$. Donc les indices p.p sont de la forme $|\text{ann}_M(q)/\text{ann}_M(r)|$, où $r, q \in R$. Par le lemme 2.2.7 ceci est un $|\text{ann}_M(s)|$ avec $s \in R$.

Dans le cas où K_0 est infini, $\text{ann}_M(r)$ est infini pour tout r premier. ■

On veut maintenant considérer les modèles de $T_{R,d}$, c'est-à-dire considérer éventuellement le cas où $\text{ann}_M(q)$ puisse être égal à $\{0\}$ pour certains $q \in R$, et prouver un analogue du lemme 2.2.7.

Lemme 2.2.10. *Soit N un modèle de $T_{R,d}$. Pour tous $s, q \in R \setminus \{0\}$ tels que $\text{ann}_N(q) \supseteq \text{ann}_N(s) \neq 0$, il existe $r \in R$ tel que*

$$\text{ann}_N(q)/\text{ann}_N(s) \simeq \text{ann}_N(r).$$

PREUVE. Soit N , s et q comme dans l'énoncé. Si s est premier, alors s divise q car s est le polynôme minimal d'un même élément non nul annulé par q et s . Dans ce cas, $q = sr$ pour un certain $r \in R$ et on conclut en considérant l'application $\text{ann}_M(s) \rightarrow \text{ann}_M(q)$, $x \mapsto x.r$, comme dans la preuve du lemme 2.2.7. Écrivons $s = s_1 \dots s_n$, avec s_i premier sauf éventuellement s_1 qui est peut être une puissance de t . Supposons l'énoncé du lemme vrai pour tout couple (r_1, r_2) tel que r_1 s'écrit avec au plus $n - 1$ facteurs premiers. Posons $s' = s_2 \dots s_n$. Puisque $\text{ann}_N(s) \neq 0$, s_1 ou s' a des racines non-nulles dans N .

cas 1 : $\text{ann}_N(s_1) \neq 0$. Alors s_1 divise q . Il vient $q = s_1 r$ et, par le fait que N est divisible, $\text{ann}_N(s') \subseteq \text{ann}_N(r)$. Si $\text{ann}_N(s') = 0$ alors : $\text{ann}_N(q)/\text{ann}_N(s) \simeq \text{ann}_N(q)/\text{ann}_N(s_1) \simeq \text{ann}_N(r)$. Sinon, par hypothèse d'induction il existe s'_t et r' tel que s'_t divise r' et

$$\text{ann}_N(r')/\text{ann}_N(s'_t) \simeq \text{ann}_N(r)/\text{ann}_N(s').$$

Alors l'application « $x \mapsto x.s_1 \text{ mod } \text{ann}_N(s')$ » établit un morphisme de K_0 -espaces vectoriels surjectif de $\text{ann}_N(q)$ vers $\text{ann}_N(r)/\text{ann}_N(s')$ ayant comme noyau $\text{ann}_N(s)$.

cas 2 : $\text{ann}_N(s_1) = 0$. Alors, $\text{ann}_N(s') \neq 0$ et $\text{ann}_N(s).s_1 = \text{ann}_N(s') \subseteq \text{ann}_N(q).s_1$ et l'action de s_1 induit un isomorphisme de K_0 -espace vectoriel $\text{ann}_N(q) \rightarrow \text{ann}_N(q).s_1$. Par conséquent $\text{ann}_N(q)/\text{ann}_N(s) \simeq \text{ann}_N(q).s_1/\text{ann}_N(s')$. Puisque N est divisible t -injectif, par le lemme 2.2.1 la p.p. formule $\exists y \ y.s_1 = x \wedge y.q = 0$ définissant $\text{ann}_N(q).s_1$ est équivalente à une formule de la forme : $x.q_1 = 0$ par le lemme 2.2.1, pour un certain $q_1 \in R$. En appliquant l'hypothèse d'induction à (s', q_1) on obtient r' et s'_t comme ci-dessus. ■

Du résultat ci-dessus on aboutit à la même conclusion du corollaire 2.2.8 aussi pour les modèles de $T_{R,d}$.

Corollaire 2.2.11. *Si $M \models T_{R,d}$, pour tout $0 \neq q = t^n q_1 \dots q_k \in R$, on a*

$$|\text{ann}_M(q)| = \prod_{i=1}^k |\text{ann}_M(q_i)|,$$

où $|\text{ann}_M(q_i)|$ est à valeurs cardinales.

Définition 2.2.12. Un module M est dit indécomposable s'il n'admet aucun facteur direct non-trivial. C'est-à-dire s'il n'existe pas de sous-modules non nuls N_1, N_2 tels que $M = N_1 \oplus N_2$.

Lemme 2.2.13. *Soit N_1 et N_2 deux R -modules indécomposables modèles de $T_{R,d}$ et $q \in R$ un polynôme premier, tels que $\text{ann}_{N_i}(q)$ est non-trivial pour $i = 1, 2$. Alors N_1 et N_2 sont isomorphes.*

PREUVE. Soit $a \in \text{ann}_{N_1}(q)$ et $b \in \text{ann}_{N_2}(q)$. Alors N_1 est une clôture divisible de $a.R$, et N_2 est une clôture divisible de $b.R$. Donc il suffit de montrer que $a.R$ est isomorphe à $b.R$. Or, l'application $a.r \mapsto b.r$ est un isomorphisme de R -module. En effet, pour tout $r \in R \setminus \{0\}$, $a.r = 0$ si, et seulement si, q divise r , si et seulement si $b.r = 0$. ■

Lemme 2.2.14. *Soit N un modèle de $T_{R,d}$ indécomposable et $r \in R$ un polynôme premier tel que $\text{ann}_N(r) \neq 0$. Alors, pour tout $q \in R$ premier, $\text{ann}_N(q) \neq 0$ si, et seulement si, il existe $\lambda, \mu \in K \setminus \{0\}$ tels que $q = \lambda r \mu$; dans ce cas $\text{ann}_N(r) \simeq \text{ann}_N(q)$.*

PREUVE. Soit $0 \neq a \in \text{ann}_N(r)$ et $0 \neq b \in \text{ann}_N(q)$. Alors N est une clôture divisible à la fois de $a.R$ et de $b.R$. Soit r_0 de degré minimal tel que $0 \neq a.r_0 \in b.R$. Donc r_0 divise r . Or r étant premier et $a.r_0 \neq 0$, cela implique $r_0 \in K$. Donc $a \in b.R$, i.e. $a = b.s$ pour un certain $s \in R \setminus \{0\}$. Par conséquent s divise q . Comme q est premier, $s \in K$. De plus, comme $b.sr = 0$, q divise sr . Or sr est premier car $s \in K$. Par conséquent $\deg(q) = \deg(r)$ et $sr = q\nu$ avec $s, \nu \in K$.

Réciproquement, soit r, q, λ, μ donnés comme dans l'énoncé. Il est clair que $a \neq 0$ est une racine de q si et seulement si $a.\lambda$ est une racine de r . En particulier, l'application $x \mapsto x.\lambda$ établit un isomorphisme de K_0 -espace vectoriel entre $\text{ann}_N(q)$ et $\text{ann}_N(r)$. ■

Définition 2.2.15. Soit $r, q \in R$ premiers. On dit que r et q sont K -conjugués s'il existe $\lambda, \mu \in K \setminus \{0\}$ tels que $q = \lambda r \mu$.

Remarque 2.2.16. La K -conjugaison entre éléments premiers de R est clairement une relation d'équivalence.

On fixe pour la suite un système \mathcal{P} de représentants des classes de K -conjugaison de R .

Corollaire 2.2.17. *Soit $r \in \mathcal{P}$ et $N \models T_{R,d}$ indécomposable contenant une racine non nulle de r . Alors pour tous $q, s \in R \setminus \{0\}$ tels que $\text{ann}_N(q) \supset \text{ann}_N(s) \neq 0$, si $|\text{ann}_N(q)/\text{ann}_N(s)|$ est fini, alors il est égal à $k|\text{ann}_N(r)|$, pour un certain $0 \neq k \in \mathbb{N}$.*

PREUVE. Puisque $N \models T_{R,d}$, par le lemme 2.2.10 il existe $r' \in R$ tel que

$$\text{ann}_N(q)/\text{ann}_N(s) \simeq \text{ann}(r').$$

Or, en notant r_0, \dots, r_k les facteurs premiers de r' , on a d'une part, par le corollaire 2.2.11,

$$|\text{ann}_N(r')| = \prod_{i < k} |\text{ann}_N(r_i)|$$

et d'autre part chaque $|\text{ann}_N(r_i)| \in \{|\text{ann}_N(r)|, 1\}$ par le lemme ci-dessus. \blacksquare

Proposition 2.2.18. *Tout R -module divisible est somme directe de ses facteurs indécomposables. Ceux-ci sont nécessairement divisibles.*

PREUVE. En effet tout module injectif sur un anneau Noetherien est la somme directe de ses facteurs indécomposables (cf. [Zi] corollary 7.3). Puisque chaque facteur direct d'un module divisible est divisible, ses facteurs indécomposables sont divisibles. \blacksquare

Définition 2.2.19. Soit $M \models T_{R,d}$ et $q \in R$ premier. On appelle M_q la somme directe des sous-modules indécomposables de M_{tor} contenant au moins une racine non nulle de q .

Proposition 2.2.20. *Soit M comme ci-dessus. On a $M_{\text{tor}} = \bigoplus_{q \in \mathcal{P}} M_q$.*

PREUVE. Il suffit de voir que si $N \subseteq M_{\text{tor}}$ un sous-module indécomposable alors N est une clôture divisible d'un élément a annihilant un polynôme premier q . D'abord en effet, N étant indécomposable, il est une clôture divisible de tous ses éléments. Puis, si q_x est le polynôme minimal de $x \in N$, alors q_x s'écrit comme $t^n q_1 \dots q_k$, où les q_i sont les facteurs premiers, et donc $x \cdot (t^n q_1 \dots q_{k-1})$ est annihilé par q_k . \blacksquare

On déduit en particulier de ces trois derniers résultats et du corollaire 2.2.2 que :

Corollaire 2.2.21. *Les complétions de $T_{R,d} \cup \{\exists x \ x \neq 0\}$ sont obtenues en spécifiant pour chaque $q \in \mathcal{P} \cup \{0\}$, $|\text{ann}(q)| \in (\bigcup_{n \in \mathbb{N}} |K_0|^n) \cup \{\infty\}$, et elles admettent l'élimination des quantificateurs.*

Corollaire 2.2.22. *Soit $M, N \models T_{R,d}$ élémentairement équivalents, f un isomorphisme partiel entre les sous-modules $A \subset M$ et $B \subset N$. Supposons de plus N , $|M|^+$ -saturé. Alors la restriction de f à $A \cap M_{\text{tor}}$ admet un prolongement en un plongement de M_{tor} dans N_{tor} .*

Quand tous les annulateurs sont finis, le type d'isomorphisme du sous-module de torsion est déterminé par la théorie complète. Plus précisément :

Proposition 2.2.23. *Pour un R -module M , soit η_M la fonction à valeurs cardinales définie sur \mathcal{P} par $\eta_M(q) = |\text{ann}_M(q)|$. Si M et N sont deux modèles de $T_{R,d}$, vérifiant $\eta_M \leq \eta_N$, alors M_{tor} se plonge dans N_{tor} . En particulier si $\eta_M = \eta_N$ et à valeurs finies, M_{tor} et N_{tor} sont isomorphes.*

PREUVE. On considère deux tels modèles M, N . Soit $q \in \mathcal{P}$. Alors M_q est somme directe de sous-modules indécomposables $(M^i)_{i \in I}$, tous isomorphes entre eux par le lemme 2.2.13. De la même façon N_q est somme de modules $(N^j)_j$ indécomposables et isomorphes. De plus, toujours par le lemme 2.2.13, les M_i et les N_j sont isomorphes. Par l'hypothèse sur les fonctions η_M et η_N , M_q se plonge dans N_q , donc aussi M_{tor} dans N_{tor} . \blacksquare

2.3 Cas des corps

Soit K un corps de caractéristique $p > 0$. On dit qu'il est p -clos si tout polynôme de la forme $X^{p^n}a_n + \cdots + X^pa_1 + Xa_1 + a_0 \in K[X]$ a une racine dans K . Cela équivaut à dire que K est divisible comme $K[t; x \mapsto x^p]$ -module. On a aussi le résultat suivant qui a été d'abord montré par Whaples (cf. [Wh]) et puis une démonstration plus élémentaire a été fournie par F. Delon dans sa thèse d'état en 1982.

Proposition 2.3.1. *Un corps de caractéristique $p > 0$ est p -clos si et seulement si il n'a aucune extension de degré divisible par p .*

Corollaire 2.3.2. *Si L est un corps de caractéristique $p > 0$, p -clos, alors toute extension algébrique de L est p -close.*

Théorème 2.3.3. *Soit $K \subset F$ une extension des corps (de caractéristique $p > 0$), alors le sous-module de torsion F_{tor} de F comme $K[t; x \mapsto x^p]$ -module est égale à la clôture algébrique de K dans F . De plus, deux extensions algébriques et p -closes F_1 et F_2 de K sont élémentairement équivalentes comme $K[t; x \mapsto x^p]$ -modules, si et seulement si F_1 et F_2 sont isomorphes comme $K[t; x \mapsto x^p]$ -modules.*

PREUVE. Tout élément de F qui est annulé par polynôme additif à coefficients dans K est algébrique et réciproquement tout élément algébrique de F sur K est annulé par un polynôme additif par le fait que tout polynôme divise un polynôme additif. Cela montre la première assertion.

Puisque F_1 et F_2 sont p -clos, par le corollaire 2.1.7, leurs théories comme $K[t; x \mapsto x^p]$ -modules sont données par les théories de leurs sous-modules de torsion. Comme F_1 et F_2 sont algébriques sur K , $F_1 = F_{1_{tor}}$ et $F_2 = F_{2_{tor}}$. Avec la proposition 2.2.23, si les modules F_1 et F_2 sont élémentairement équivalents alors ils sont isomorphes. ■

Corollaire 2.3.4. *Soit la tour d'extension de corps de caractéristique $p > 0$,*

$$K \subset L \subsetneq M \subset K^{alg},$$

où K est p -clos. Alors $L \not\cong M$ comme $K[t; x \mapsto x^p]$ -modules. ■

Chapitre 3

$K[t; \varphi]$ -modules K -trivialement valués : K agit en préservant la valuation

Ce chapitre peut être vu comme un cas simple du chapitre suivant. Un des objets que l'on considère est par exemple un corps (U, v) valué de caractéristique $p > 0$, vu comme $K[t; x \mapsto x^p]$ -module pour K un sous-corps trivialement valué de U . On introduit une première notion de module valué (voir définition 3.1.2); c'est une structure à deux sortes (M, Δ) où Δ est un ensemble totalement ordonné muni d'un plus grand élément ∞ et où on a une valuation $v : M \rightarrow \Delta$. Ces modules valués (M, v) satisferont ici, pour tout $\mu \in K^\times$, l'égalité $v(x.\mu) = v(x)$, d'où le nom de ce chapitre. De plus on décrètera pour tout $x \in M$, que l'on a $v(x.t) = \tau(v(x))$, où τ est une fonction strictement croissante sur l'ensemble Δ , possédant au plus un seul point fixe dans $\Delta \setminus \{\infty\}$; on notera ce point fixe par θ . Ces propriétés avec les propriétés ultramétrique générales impliqueront qu'étant donné $r = \sum_i t^i a_i \in R \setminus \{0\}$, on a $v(x.r) = \min_i \{v(x.t^i a_i)\}$ quand $v(x) \neq \theta$ (voir 3.1.4).

Pour gérer les particularités provenant des éléments de valuation θ , on introduira la notion de module valué henselien (voir définition 3.2.1). Pour cela on s'est inspiré de l'exemple suivant : Si K est un sous-corps trivialement valué d'un corps valué henselien (L, v) de caractéristique $p > 0$, alors pour tout polynôme P séparable et additif à coefficients dans K , pour tout $z \in \mathcal{M}_L \setminus \{0\}$, il existe $y \in \mathcal{M}_L$, tel que $P(y) = z$ (voir 3.2.2). Remarquons que dans ce cas \mathcal{M}_L est muni d'une structure de $K[t; x \mapsto x^p]$ -module, et ce que l'on vient de dire revient à dire que \mathcal{M}_L est divisible par les éléments séparables de $K[t; x \mapsto x^p]$. En particulier si L est de plus parfait alors \mathcal{M}_L est divisible comme module.

Après avoir remarqué qu'en général l'hypothèse de divisibilité seule n'implique pas l'henselianité (voir 3.2.9), on considérera les modules valués divisibles et henséliens. Ces modules valués se présentent tous comme une somme valuation-indépendante de quatre sous-modules valués dont le sous-module de torsion et trois sous D -espaces vectoriels. Cette décomposition (voir 3.2.7) permettra de contrôler suffisamment les modèles pour établir des principes d'Ax, Kochen et Ershov.

Noter qu'on trouve la notion de module valué depuis les années cinquante, et la première référence que l'on a remarquée est celle de I.Fleischer en 1958 (cf. [Fl]).

3.1 Modules K -trivialement valués

Comme dans les chapitres précédents, durant tout ce chapitre aussi, tout R -module mentionné sera t -injectif, i.e. l'application $x \mapsto x.t$ sera injective.

Soit $L_{V_0} = \{<, \tau, \infty\}$ le langage des ensembles ordonnés enrichi d'un symbole de fonction unaire τ et d'un symbole de constante ∞ . Nous considérerons toujours des L_{V_0} -structures où $<$ est un ordre total, avec ∞ son élément maximal et τ un morphisme de la structure ($<, \infty$) (i.e. τ est strictement croissante et $\tau(\infty) = \infty$). De plus, dans ce chapitre, l'axiome :

$$\forall \gamma, \delta \neq \infty \quad (\tau(\gamma) \leq \gamma \wedge \delta < \gamma) \rightarrow \tau(\delta) < \delta \quad (3.1)$$

sera toujours satisfait. Remarquons que cet axiome implique son dual :

$$\forall \gamma, \delta \neq \infty \quad (\tau(\gamma) \geq \gamma \wedge \gamma < \delta) \rightarrow \tau(\delta) > \delta. \quad (3.2)$$

Ainsi, si Δ est une telle L_{V_0} -structure, l'ensemble $\Delta_+ := \{\gamma \in \Delta \mid \tau(\gamma) > \gamma\} \cup \{\infty\}$ est un segment final de Δ et $\Delta_- := \{\gamma \in \Delta \mid \tau(\gamma) < \gamma\}$ en est un segment initial. En particulier, il existe dans Δ au plus un point fixe de τ autre que ∞ . Dans le reste de ce chapitre, si un tel point existe, on va le désigner par θ . Si θ existe, c'est l'unique point de Δ vérifiant $\Delta_- < \theta < \Delta_+$. Cela nous autorise, même en l'absence de θ , à écrire $\gamma < \theta$ pour $\gamma \in \Delta_-$, et $\gamma > \theta$ pour $\gamma \in \Delta_+$. De même l'écriture $\gamma \leq \theta$, ou $\gamma \geq \theta$, ne supposera pas l'existence de θ . Il est immédiat de vérifier que, avec cette convention, l'axiome 3.1 implique :

$$\forall \gamma \neq \infty \quad (\gamma > \theta \rightarrow \tau(\gamma) > \gamma) \wedge (\gamma < \theta \rightarrow \tau(\gamma) < \gamma). \quad (3.3)$$

Exemple 3.1.1. Pour tout entier $n > 1$, la structure $(\mathbb{Z} \cup \{\infty\}, <, x \mapsto nx)$ satisfait les axiomes ci-dessus, avec $\theta_{\mathbb{Z}} = 0$.

Si L_R est le langage des R -modules, notons L le langage à deux sortes $L_R \cup L_{V_0} \cup \{v\}$. On va considérer les L -structures (M, Δ, v) qui sont des groupes abéliens valués tels que M est un R -module t -injectif, Δ une L_{V_0} -structure comme ci-dessus, v une application surjective $M \rightarrow \Delta$. Notons T la théorie (clairement du 1er ordre) dont on vient de décrire les modèles.

Définition 3.1.2. On appelle module K -trivialement valué une L -structure modèle de T et des (schémas d') axiomes suivants :

- i. $\forall x \quad v(x.\lambda) = v(x)$, pour tout $\lambda \in K \setminus \{0\}$,
- ii. $\forall x \quad v(x.t) = \tau(v(x))$.

On désignera la L -théorie des modules K -trivialement valués par T_{mv} .

Durant cette section, l'expression module valué, désignera toujours un module K trivialement valué.

Remarque 3.1.3. Soit (M, v) un module K -trivialement valué et $x \in M$. Alors $v(x) > \theta$ si et seulement si $v(x.t) > v(x)$, et $v(x) < \theta$ si et seulement si $v(x.t) < v(x)$.

Lemme 3.1.4. Soit (M, v) un module K -trivialement valué et $r = \sum_{i \in I} t^i a_i \in R \setminus \{0\}$. Alors, pour tout $x \in M$, on a $v(x.r) \geq \min_{i \in I} \{v(x.t^i a_i)\} = \min_{i \in I} \{\tau^i(v(x))\}$. De plus

1. pour tout $x \in M$, si $v(x) > \theta$ alors $v(x.r) = \tau^{\deg_{is}(r)}(v(x)) = \min_{i \in I} \{\tau^i(v(x))\}$,
2. pour tout $x \in M$, si $v(x) < \theta$ alors $v(x.r) = \tau^{\deg(r)}(v(x)) = \min_{i \in I} \{\tau^i(v(x))\}$,
3. si $x.r = 0$ et $x \neq 0$ alors θ existe et $v(x) = \theta$.

PREUVE. Soit $x \in M \setminus \{0\}$. On écrit $r = \sum t^i a_i$ avec $a_i \in K \setminus \{0\}$. La première assertion est évidente car $v(\sum x.t^i a_i) \geq v(x.t^i a_i)$ pour tout $i \in I$, par les axiomes des groupes valués et on a $v(x.t^i a_i) = v(x.t^i) = \tau^i(v(x))$ par les axiomes i et ii de la définition 3.1.2.

1. Puisque $v(x.t) > v(x)$, par les axiomes de la définition 3.1.2 et par l'axiome 3.1, $v(x.t^i a_i) = v(x.t^i) > v(x.t^j) = v(x.t^j a_j)$ quand $i > j$. Alors, $v(x.r) = v(\sum x.t^i a_i) = \min_i \{v(x.t^i)\} = \tau^k(v(x))$, où $k = \deg_{i_s}(r)$.
2. Puisque $v(x.t) < v(x)$, par l'axiome 3.1, $v(x.t^i a_i) < v(x.t^j a_j)$ quand $i > j$. Ainsi $v(x.r) = v(\sum x.t^i a_i) = \min_i \{v(x.t^i)\} = \tau^n(v(x))$ où $n = \deg(r)$.
3. Si $x.r = 0$ alors $v(x.r) = \infty$; puisque $x \neq 0$, par ce qui précède x ne peut être que de valuation θ . ■

Remarque 3.1.5. Rappelons que, dans un groupe abélien valué (M, v) , pour tout $\gamma \in v(M)$ on note $M_{\geq \gamma}$ (respectivement $M_{> \gamma}$) la boule fermée (respectivement la boule ouverte) centrée en 0 et de rayon valuatif γ . Selon notre convention sur la notation θ , les notations $M_{> \theta}$ ou $M_{\geq \theta}$ ne présupposent pas l'existence de θ dans $v(M)$. On a toujours : $M_{> \theta} = \{x \in M \mid v(x.t) > v(x)\}$ et $M_{\geq \theta} = \{x \in M \mid v(x.t) \geq v(x)\}$. Par le lemme ci-dessus, $M_{> \theta}$ et $M_{\geq \theta}$ sont des R -sous-modules de M .

Définition 3.1.6. Soit (G, v) un groupe abélien valué. Un sous-groupe de G est dit convexe s'il est l'image réciproque par v d'un segment final (non vide) de $v(G)$.

Lemme 3.1.7. Une boule (ouverte ou fermée) contenant 0 d'un groupe valué est un sous-groupe convexe. Si (M, v) est un module K -trivialement valué, alors $M_{\geq \theta}$ et $M_{> \theta}$ sont des sous-groupes convexes de M .

PREUVE. Une boule centrée en 0 est de la forme $\{x \in M \mid v(x) > \gamma\}$ et est donc l'image réciproque par v du segment final $]\gamma, \infty]$. Il est clair que de même une boule fermée centrée en 0 est un sous-groupe convexe. Si $\theta \in v(M)$, alors $M_{\geq \theta}$ et $M_{> \theta}$ sont des boules centrées en 0, donc ce sont des sous-groupes convexes. Si θ n'est pas présent, alors $M_{> \theta} = M_{\geq \theta}$ est l'image réciproque par v de Δ_+ , donc est convexe (cf. la discussion entre les équations 3.2 et 3.3). ■

Lemme 3.1.8. Si H est un sous-groupe convexe d'un groupe abélien valué (G, v) alors le groupe G/H est valué par v_H , définie par :

$$v_H(g + H) := \begin{cases} v(g) & \text{si } g \notin H \\ \infty & \text{sinon} \end{cases} .$$

PREUVE. Il suffit de vérifier que v_H définit une fonction. Soit I_H le segment final de $v(G)$ tel que $H = v^{-1}(I_H)$. D'abord, si $g \notin H$ et $g' \notin H$ sont deux représentants de la classe de g modulo H , alors $v(g) \notin I_H$ et $v(g') \notin I_H$ et $g - g' \in H$. Donc $v(g - g') \in I_H$ et nécessairement $v(g - g') > v(g)$. Cela implique que $v(g) = v(g')$ et donc $v_H(g + H) = v_H(g' + H)$. ■

Corollaire 3.1.9. Soit (M, v) un module K -trivialement valué. Alors $M/M_{\geq \theta}$ est muni d'une structure canonique de module K -trivialement valué.

Définition 3.1.10. On appellera régulier un module K -trivialement valué (M, v) tel que, pour tout $x \in M \setminus \{0\}$ et tout $r = \sum_{i=0}^n t^i a_i \in R$, non nul, on a $v(x.r) = \min_i \{v(x.t^i)\}$ ($= \min_i \{\tau^i(v(x))\}$). Noter que M est nécessairement sans-torsion.

Corollaire 3.1.11. Soit (M, v) un module K trivialement valué. Alors le sous-module $(M_{>\theta}, v)$ et le module quotient $(M/M_{\geq\theta}, v_{M_{\geq\theta}})$ sont des modules K -trivialement valués réguliers.

PREUVE. Le fait que $(M/M_{\geq\theta}, v_{M_{\geq\theta}})$ induise une structure de module valué découle du lemme 3.1.8 et que si $x \notin M_{\geq\theta}$ alors $v(x.t) < v(x)$. Alors ces deux modules valués sont réguliers par le lemme 3.1.4. ■

3.2 Modules K -trivialement valués divisibles et henséliens

On aborde maintenant la notion de module K -trivialement valué hensélien. Noter que les modules valués henséliens ont été aussi considérés par Bélaïr et Point dans [BéPo] (cf. définition 2.5).

Définition 3.2.1. Un module K -trivialement valué est dit hensélien s'il satisfait le schéma d'axiomes suivant :

$$\text{H} : \forall x \ v(x) > \theta \rightarrow \exists y \ x = y.r \wedge v(y) > \theta$$

pour tout $r \in R_{\text{sep}}$.

On notera T_h la théorie des modules K -trivialement valués henséliens.

Les modèles de T_h que l'on veut étudier incluent par exemple le corps valué $(\mathbb{F}_p(X))^{alg}$, où la valuation est triviale sur \mathbb{F}_p^{alg} , et qu'on voit comme module sur $\mathbb{F}_p^{alg}[t; x \mapsto x^p]$. Le schéma d'axiomes H ci-dessus peut se voir comme une sorte de propriété de Hensel. En effet, si φ est le morphisme de Frobenius, alors, pour chaque $r = \sum_{i=0}^n t^i a_i \in R$, l'application $x \mapsto x.r$ est la fonction polynomiale induite par le polynôme additif $X^{p^n} a_n + \dots + X a_1$. Dans ce cas, dans un modèle comme $\mathbb{F}_p(X)^{alg}$, il est facile de vérifier que le lemme de Hensel classique implique le schéma H. Plus précisément on a :

Lemme 3.2.2. Si K est un sous-corps trivialement valué d'un corps valué (U, v) , de caractéristique $p > 0$, alors U porte une structure canonique de $K[t; x \mapsto x^p]$ -module K -trivialement valué. De plus, si v est hensélienne sur le corps U , alors (U, v) est un module K -trivialement valué hensélien. De plus, si U est parfait, alors l'idéal maximal \mathcal{M}_U associé à v est un $K[t; x \mapsto x^p]$ -module divisible.

PREUVE. On interprète $x.t$ par x^p , τ comme la fonction $v(U) \rightarrow v(U)$, $\gamma \mapsto p\gamma$, et θ comme $0 \in v(U)$. Il est clair que (U, v) est un module K -trivialement valué. Supposons maintenant que v est une valuation hensélienne au sens des valuations sur les corps. Soit $r = t^n a_n + \dots + a_0 \in R_{\text{sep}}$, et $y \in U$ tel que $v(y) > 0$. Soit R le polynôme associé à r , i.e. $R(X) = a_n X^{p^n} + \dots + a_0 X$. Puisque r est séparable, $a_0 \neq 0$, et puisque $a_0 \in K$, $v(a_0) = 0$. Alors, avec $F(X) := R(X) - y$, on a $F'(0) = a_0$ et $F(0) = -y$. Puisque v est hensélienne, il existe $z \in U$ de valuation > 0 , tel que $F(z) = 0$. Donc $R(z) = y$. C'est-à-dire $z.r = y$ et $v(z) > 0$.

Enfin, $U_{\geq\theta} = \mathcal{M}_U$ et si U est parfait, alors en particulier $U_{\geq\theta}$ est divisible par t . Puisqu'il est divisible par les polynômes séparables et par t , il est divisible. ■

Les résultats qui suivent contiennent toute l'information qu'on va utiliser pour montrer un résultat de type Ax-Kochen et Ershov dans la section suivante.

Lemme 3.2.3. *Si (M, v) est un module K -trivialement valué divisible et hensélien, alors $M_{\geq \theta}$ est divisible et $M_{> \theta}$ est divisible et sans torsion ; par conséquent $M_{\geq \theta}$ est facteur direct dans M , et $M_{> \theta}$ facteur direct dans $M_{\geq \theta}$.*

PREUVE. Soit $r \in R \setminus \{0\}$, $x \in M_{\geq \theta}$ et $y \in M$ tel que $y.r = x$. Alors nécessairement $y \in M_{\geq \theta}$, et donc celui-ci est divisible. Montrons que $M_{> \theta}$ est divisible. Si $r \in R_{sep}$ alors l'assertion est triviale par les axiomes H. Sinon, en écrivant $r = t^n.r'$ avec r' séparable, il existe, par les axiomes H, $y \in M_{> \theta}$ tel que $x = y.r'$. Or $y = y'.t^n$ pour un certain $y' \in M$, donc $y'.r = x$ et nécessairement $y' \in M_{> \theta}$ par l'axiome ii de la définition 3.1.2. Le fait que $M_{> \theta}$ est sans torsion découle du fait qu'il est régulier par le corollaire 3.1.11. Donc ces deux modules sont facteurs directs par le lemme 2.1.3. ■

Corollaire 3.2.4. *Soit (M, v) un module K -trivialement valué divisible et hensélien. Si $x \in M$ est de valuation θ et tel que $v(x.r) > \theta$ pour un certain $r \in R \setminus \{0\}$, alors $x = x_{tor} + x_{> \theta}$ avec $x_{tor} \in \text{ann}_M(r) \setminus \{0\}$ et $x_{> \theta} \in M_{> \theta}$. En conséquence, pour tout $x \in M \setminus \{0\}$ et $q = \sum_{i \in I} t^i a_i \in R \setminus \{0\}$, il existe $y \in M$ tel que $x = y.q$ et $v(x) = \tau^k(v(y))$, avec $k = \deg_{is}(q)$ si $v(x) > \theta$, $k = \deg(q)$ si $v(x) < \theta$, et $k = 0$ si $v(x) = \theta$; autrement dit $v(x) = \min_{i \in I} \{v(y.t^i a_i)\} = \min_{i \in I} \{\tau^i(v(y))\}$.*

PREUVE. Soit $x \in M$ de valuation θ et $r \in R \setminus \{0\}$ tel que $v(x.r) > \theta$. Si $x.r = 0$ alors $x \in M_{tor}$ et on a fini. Sinon, par 3.2.3, $M_{> \theta}$ étant divisible sans torsion, il existe un unique $z \in M_{> \theta}$ tel que $z.r = x.r$. D'où $z - x \in \text{ann}_M(r)$ et $x = x - z + z$ s'écrit comme voulu. ■

Définition 3.2.5. On dit qu'une suite de sous-groupes $(A_i)_{i \in I}$ de M est (en somme) valuation-indépendante si, pour tout $(x_i)_{i \in I}$, avec $x_i \in A_i$, pour tout J fini, $J \subset I$,

$$v\left(\sum_{i \in J} x_i\right) = \min\{v(x_i) \mid i \in J\}.$$

Remarque 3.2.6. Si $(A_i)_{i \in I}$ est une suite de sous-modules sans torsion qui est en somme valuation-indépendante, alors toute famille $(x_i)_{i \in I}$ avec $x_i \in A_i \setminus \{0\}$, est une famille R -linéairement indépendante.

La proposition suivante est un résultat de structure qui récapitule les lemmes ci-dessus.

Proposition 3.2.7. *Soit (M, v) un module K -trivialement valué divisible et hensélien.*

1. *Le plongement de M_{tor} dans $M_{\geq \theta}/M_{> \theta}$ est scindé.*
2. *Les R -modules $M_{\geq \theta}/(M_{tor} + M_{> \theta})$, $M_{> \theta}$ et $M/M_{\geq \theta}$ sont divisibles sans torsion.*
3. *M s'écrit comme $M_{tor} \oplus M_{\theta} \oplus M_{> \theta} \oplus M_-$, où M_{θ} est isomorphe à $M_{\geq \theta}/(M_{tor} + M_{> \theta})$ et (M_-, v) isomorphe en tant que module valué à $(M/M_{\geq \theta}, v_{/M_{\geq \theta}})$. Une telle décomposition est valuation-indépendante et chaque membre de cette décomposition est un D -espace vectoriel régulier.*

PREUVE. 1. Les éléments de M_{tor} sont tous de valuation θ par le lemme 3.1.4, donc M_{tor} se plonge dans $M_{\geq \theta}/M_{> \theta}$. De plus M_{tor} est divisible. Donc son image dans $M_{\geq \theta}/M_{> \theta}$ y est facteur direct.

2. Le fait que $M_{>\theta}$ est divisible sans torsion a été déjà établi dans le lemme 3.2.3. La divisibilité de $M/M_{\geq\theta}$ est induite par la divisibilité de M . Il est sans torsion car il est régulier par 3.1.11. $M_{\geq\theta}/(M_{tor} + M_{>\theta})$ est divisible trivialement, par le fait que M est divisible. Maintenant, soit $x \in M \setminus (M_{tor} + M_{>\theta})$. Alors $v(x) = \theta$. Supposons $x.r \in M_{tor} + M_{>\theta}$ pour un certain $r \neq 0$. Par le fait que M_{tor} est divisible, on a $x.r - z'.r = (x - z').r \in M_{>\theta}$ pour un certain $z' \in M_{tor}$. Si $x - z' \in M_{>\theta}$ alors $x \in M_{tor} + M_{>\theta}$ et on a fini. Sinon, par le corollaire 3.2.4 $x - z' \in M_{tor} + M_{>\theta}$ d'où $x \in M_{tor} + M_{>\theta}$: contradiction. Cela montre que $M_{\geq\theta}/(M_{tor} + M_{>\theta})$ est sans torsion.

3. Par le fait que $M_{\geq\theta}$ est divisible, $M \simeq M_{\geq\theta} \oplus M/M_{\geq\theta}$. Or $M_{>\theta}$, étant divisible, est facteur direct dans $M_{\geq\theta}$. C'est à dire $M_{\geq\theta} \simeq M_{>\theta} \oplus M_{\geq\theta}/M_{>\theta}$. Enfin par la première assertion $M_{\geq\theta}/M_{>\theta} \simeq M_{tor} \oplus (M_{\geq\theta}/(M_{tor} + M_{>\theta}))$.

Maintenant si $x \in M_- \setminus \{0\}$ alors $v(x) < \theta$ et par la définition de la valuation quotient $v_{M_{\geq\theta}}$, (M_-, v) sont isomorphes. Montrons que la décomposition établie est valuation-indépendante. Pour cela il suffit de voir que M_{tor} et M_θ sont en somme valuation-indépendante; i.e. si $x \in M_{tor}$, $y \in M_{\geq\theta} \setminus (M_{tor} + M_{>\theta})$ de valuation θ alors $v(x - y) = \theta$. Supposons pour une contradiction qu'il existe $x \in M_{tor}$, $y \in M_{\geq\theta} \setminus (M_{tor} + M_{>\theta})$ avec $v(x - y) > \theta$. Alors, pour un $r \in R \setminus \{0\}$ annulant x , on a $v((x - y).r) = v(y.r) > \theta$: contradiction car $M_{\geq\theta}/(M_{tor} + M_{>\theta})$ est sans torsion. ■

Corollaire 3.2.8. *Soit (M, v) un module K -trivialement valué divisible et henselien. Alors, pour toute décomposition de M en $M_- \oplus M_{tor} \oplus M_\theta \oplus M_{>\theta}$ comme dans la proposition 3.2.7, pour $i \in \{\theta, > \theta, -\}$, pour tous $x, y \in M_i \setminus \{0\}$ et pour tout $q \in R \setminus \{0\}$, on a $v(x.q) = v(y.q)$ et $v(x - y) > v(x) = v(y)$ si et seulement s'il existe $r \in R \setminus \{0\}$ tel que $v(x.r - y.r) > v(x.r) = v(y.r)$.*

PREUVE. Découle du fait que chaque M_i est régulier. ■

On a vu que la propriété de Hensel, à savoir les axiomes H, impliquait la divisibilité du sous-module $M_{>\theta}$ quand M est lui-même divisible. Pourtant, l'hypothèse de divisibilité, seule, n'implique pas les axiomes H, comme le montre la proposition suivante.

Proposition 3.2.9. *Il existe des modules K -trivialement valués, divisibles mais qui ne sont pas henseliens.*

PREUVE. Soit U un corps algébriquement clos de caractéristique $p > 0$, v une valuation non triviale sur U et K un sous-corps trivialement valué de U . Par exemple on peut penser que K est \mathbb{F}_p ou la clôture algébrique de \mathbb{F}_p . On munit U d'une structure de $K[t; x \mapsto x^p]$ -module K -trivialement valué comme dans le lemme 3.2.2.

Soit $y \in U$, de valuation > 0 . Alors, par le lemme 3.1.4, y n'est pas un élément de torsion. Puisque 1 est annulé par $(t - 1)$, c'est un élément de torsion. Par conséquent le sous-module $A := (1 + y).R$ est sans torsion. Désignons par x l'élément $(y + 1).(t - 1) \in A$. Puisque $1.(t - 1) = 0$ ($1.t$ étant l'élément $1^p = 1$), on a également $x = y.(t - 1)$. Par ailleurs, puisque U est algébriquement clos, comme R -module il est a fortiori divisible. Donc U contient une

clôture divisible du sous-module A . Soit B une telle clôture; B est clairement un module K -trivialement valué par la restriction de v . Remarquons que B est sans torsion parce que clôture divisible de A , qui est sans torsion, et que $y \notin B$, car sinon B contiendrait 1. Mais y est l'unique élément de U de valuation > 0 tel que $y.(t-1) = x$. C'est-à-dire que v n'induit pas une valuation henselienne sur B . ■

Remarque 3.2.10. La preuve ci-dessus montre que $y.R$ et $(y+1).R$ ont des clôtures divisibles non-élémentairement équivalentes en tant que modules K -trivialement valués, a fortiori non-isomorphes. De plus, chaque clôture divisible de $y.R$ ou de $(y+1).R$ étant aussi une clôture divisible de $x.R$, $x.R$ a des clôtures divisibles qui ne sont pas isomorphes en tant que modules K -trivialement valués.

3.3 Un principe d'Ax-Kochen et Ershov

On continue à désigner par (M, v) un module K -trivialement valué divisible et henselien. Si A est un sous-module de M , la remarque 3.2.10 dit que les différentes clôtures divisibles de A dans M , tout en étant isomorphes en tant que R -modules, peuvent se distinguer élémentairement en tant que modules valués. C'est le seul phénomène auquel il faille faire attention pour établir un résultat de type Ax-Kochen et Ershov.

Définition 3.3.1. Soit (M, v) un module K -trivialement valué, divisible et henselien, et $A \subset M$ un sous-module de M . Alors on définit

$$\hat{A} := \{y \in M \mid y.r \in A \text{ pour un certain } r \in R \setminus \{0\}\}.$$

Lemme 3.3.2. \hat{A} est la clôture divisible de $A + M_{tor}$. En particulier, pour tout $r \in R \setminus \{0\}$ et tout $x \in M$, si $x.r \in \hat{A}$ alors $x \in \hat{A}$. De plus, si (M, v) est henselien, \hat{A} est henselien.

PREUVE. Par construction \hat{A} est divisible et clairement tout sous-module divisible de M contenant A et M_{tor} contient \hat{A} . De plus par définition de \hat{A} , si $x \in \hat{A}$, et $r \in R \setminus \{0\}$, puisque \hat{A} contient M_{tor} , \hat{A} contient tout y tel que $y.r = x$. En particulier si (M, v) est henselien et $x \in \hat{A}$ de valuation $> \theta$, \hat{A} contient l'unique élément de $y_{>\theta} \in M_{>\theta}$ tel que $y_{>\theta}.r = x$. Ce qui montre que \hat{A} est henselien dans ce cas. Enfin, $v(\hat{A})$ est bien une sous-structure de $v(M)$, c'est la clôture de $v(A)$ par la fonction τ^{-1} . ■

Pour tout module K -trivialement valué divisible et henselien (M, v) , on définit une fonction $\eta_M : R \setminus \{0\} \rightarrow \mathbb{N} \cup \{\infty\}$ par l'égalité $\eta_M(r) = |\text{ann}_M(r)|$.

Ajoutons, pour chaque $n \in \mathbb{N}$, un prédicat unaire R_n à notre langage L_{V_0} et notons L'_{V_0} cet enrichissement. Posons $L' := L_R \cup L'_{V_0} \cup \{v\} \cup \{\theta\}$. Dans un module valué (M, v) , pour tout $\gamma \in v(M) \setminus \{\infty\}$, on interprète $R_n(\gamma)$ comme $|M_{\geq \gamma} / M_{> \gamma}| \geq n$. Donc ces prédicats sont L -définissables.

Remarque 3.3.3. Soit (M, v) et (N, w) deux modules K -trivialement valués. Alors un L -plongement de (M, v) dans (N, w) est donné par un couple (f, f_v) où $f : M \rightarrow N$ est un L_R -plongement, et $f_v : v(M) \rightarrow w(N)$ un L'_{V_0} -plongement, et sont tels que, pour tout $x \in M$, on ait $f_v(v(x)) = w(f(x))$.

Par la suite, on désignera par $T_{h,d}$ la théorie des R -modules t -injectifs, divisibles, K -trivialement valués et henséliens. Dans ce qui suit, sans mention du contraire (M, v) et (N, w) seront des modèles de $T_{h,d}$.

Proposition 3.3.4. *Soit (M, v) et (N, w) deux modules K -trivialement valués divisibles, henséliens et tels que $\eta_M = \eta_N$, $A \subset M$ et $B \subset N$ des L' -sous-structures de M et N respectivement, qui sont L' -isomorphes via $\mathbf{f} = (f, f_v)$. Supposons que (N, w) est $|M|^+$ -saturé. Alors \mathbf{f} induit un L' -prolongement de \hat{A} dans \hat{B} qui le prolonge.*

PREUVE. Remarquons que $f|_{A \cap M_{tor}}$ est un isomorphisme (de module) de $A \cap M_{tor}$ vers $B \cap N_{tor}$ et qu'il se prolonge par la proposition 2.2.22 en un plongement de M_{tor} dans N_{tor} . Notons ce prolongement par h . De plus, par le lemme 3.1.4, tout élément non nul de torsion doit être de valuation θ . Donc ce plongement induit un plongement de modules valués de (M_{tor}, v) dans (N_{tor}, w) .

Par la proposition 3.2.7 on peut écrire \hat{A} comme $M_{tor} \oplus \hat{A}_\theta \oplus \hat{A}_- \oplus \hat{A}_{>\theta}$, où on rappelle que \hat{A}_θ est isomorphe à $\hat{A}_{\geq\theta}/(\hat{A}_{>\theta} + M_{tor})$ et \hat{A}_- isomorphe à $\hat{A}/\hat{A}_{\geq\theta}$. Soit $I = \{\theta, > \theta, -\}$; pour $i \in I$ désignons par f_i la restriction de f à $A \cap \hat{A}_i$. Par la définition de \hat{A} et par le fait que chaque \hat{A}_i est sans torsion, si $0 \neq x \in \hat{A}_i$ alors il existe $r \in R \setminus \{0\}$ tel que $x.r \in A$; puisque \hat{A}_i est sans torsion, $x.r \neq 0$. Par conséquent, chaque tel \hat{A}_i non nul admet en tant que D -espace vectoriel une base constituée d'éléments de A et si $j \in I$ est tel que $A_j \neq 0$, alors, pour toute décomposition de \hat{B} comme $N_{tor} \oplus \bigoplus_{i \in I} \hat{B}_i$, on a $\hat{B}_j \neq 0$. Donc, chaque f_i se prolonge en un isomorphisme de D -espace vectoriel, $\hat{f}_i : \hat{A}_i \rightarrow \hat{B}_i$. On définit alors un plongement de R -module \hat{f} de $\hat{A} = M_{tor} \oplus \hat{A}_{>\theta} \oplus \hat{A}_\theta \oplus \hat{A}_-$ vers N , en posant pour $a = a_{tor} + a_\theta + a_- + a_{>\theta} \in \hat{A}$, $\hat{f}(a) := h(a_{tor}) + \hat{f}_\theta(a_\theta) + \hat{f}_-(a_-) + \hat{f}_{>\theta}(a_{>\theta})$.

Voyons maintenant que l'on peut prolonger d'une seule façon f_v à $v(\hat{A})$, qui est une L_{V_0} -sous-structure de $v(M)$. Remarquons d'abord que, puisque la décomposition de \hat{A} en les facteurs directs M_{tor} , A_θ , $A_{>\theta}$ et A_- est valuation-indépendante, $v(\hat{A}) = v(\hat{A}_-) \cup v(A_{>\theta}) \cup \varepsilon$, où l'union est disjointe et $\varepsilon = \{\theta\}$ ou est vide. On pose $f_v(\theta) = \theta$ si $\varepsilon \neq \emptyset$. Soit $\gamma \in v(\hat{A})$, $i \in \{> \theta, -\}$ et $x \in \hat{A}_i$ tels que $v(x) = \gamma$, alors on pose $\hat{f}_v(\gamma) := w(\hat{f}_i(x))$. Remarquons que si $y \in \hat{A}_i$ est de valuation γ , et si r_1 et r_2 sont les polynômes minimaux respectifs de x et y sur A , alors avec $s = \text{ppcm}(r_1, r_2)$, on a $x.s \in A \cap \hat{A}_i$ et $y.s \in A \cap \hat{A}_i$. De plus $v(x.s) = v(y.s)$ et donc $w(\hat{f}_i(x).s) = w(\hat{f}_i(y).s)$. Or $\hat{f}_i(x).s \in B \cap \hat{B}_i$ et $\hat{f}_i(y).s \in B \cap \hat{B}_i$, $\hat{f}_i(x) = \hat{f}_i(x)$ et $\hat{f}_i(y) = \hat{f}_i(y)$; il suit par le corollaire 3.2.8 qu'ils ont la même valuation. Donc \hat{f}_v est bien défini. Montrons que (\hat{f}, \hat{f}_v) est un L -plongement de (\hat{A}, v) dans (N, w) . Soit $y \in \hat{A} \setminus \{0\}$, on écrit $y = \sum_{i \in \{tor, > \theta, \theta, -\}} y_i$. On a $v(y) = \min_i \{v(y_i)\}$. Soit $j \in \{tor, > \theta, \theta, -\}$ tel que $v(y_j) = v(y)$. Par définition de \hat{f}_v , $\hat{f}_v(v(y)) = w(\hat{f}_j(y_j))$. Or $\hat{f}(y) = \sum_{i \in \{tor, > \theta, \theta, -\}} \hat{f}_i(y_i)$ donc $w(\hat{f}(y)) = w(\hat{f}_j(y_j))$.

Il reste à voir que \hat{f}_v préserve les prédicats R_n . Par ce qu'on vient de faire, \hat{f}_v commute en particulier avec τ . Maintenant, si $M_{tor} \neq 0$ alors, du fait que M_{tor} est divisible, M_{tor} est infini. De même \hat{A}_θ est infini s'il est non nul. Cela implique que : (pour tout entier $n > 0$, $R_n(\theta)$ est vrai) si et seulement si M_{tor} , ou \hat{A}_θ , est non nul. Soit maintenant $\gamma \neq \theta$ et

$x_1, \dots, x_n \in \hat{A}$ de valuation γ tels que leurs classes dans $\hat{A}_{\geq \gamma} / \hat{A}_{> \gamma}$ soient toutes distinctes, et soit x_i^j la composante de x_i dans \hat{A}_j , où $j \in \{-, \theta, > \theta\}$ est tel que $v(x_i^j) = \gamma$. Soit $r \in R \setminus \{0\}$ tel que $x_i^j.r \in A$ pour tout $i \in \{1, \dots, n\}$. Alors tous les x_i^j sont dans \hat{A}_j , donc $v(x_i^j.r) = \tau^k(\gamma) = v((\sum_i x_i^j).r)$ pour un entier k dépendant uniquement de r et de j . Ainsi les classes de $x_1^j.r, \dots, x_n^j.r$ sont toutes différentes dans $A_{\geq \tau^k(\gamma)} / A_{> \tau^k(\gamma)}$. Donc les quotients de \hat{A} sont déterminés uniquement par ceux de A , et, par le fait qu'il commute avec τ , \hat{f}_v préserve les prédicats R_n .

On conclut de ce qui précède que (\hat{f}, \hat{f}_v) est un L' -plongement comme voulu. ■

Proposition 3.3.5. *Soit M et N comme précédemment, A un sous-module de M tel que $M_{\text{tor}} \subset A \subset M$ et $\mathbf{f} = (f, f_v) : A \rightarrow (N, w, \dots)$ un L' -plongement de A dans N . Supposons que N est $|M|^+$ saturé et $v(A) = v(M)$. Alors on peut prolonger \mathbf{f} en un plongement de M dans N .*

PREUVE. Soit $x \in M \setminus A$. Il suffit de prolonger \mathbf{f} sur $A \oplus x.R$. En effet, si on sait le faire, par la proposition qui précède, on peut prolonger \mathbf{f} sur la clôture divisible (unique par le fait que $A \supset M_{\text{tor}}$) de $A \oplus x.R$. Ainsi, par induction transfinitive, on peut prolonger \mathbf{f} sur M .

On va montrer que l'ensemble $p(Y)$ de formules ci-dessous est réalisable dans N et que, si $y \in N$ est un élément qui les réalise, alors on peut prolonger \mathbf{f} en un L' -plongement de $A \oplus x.R \rightarrow N$ en envoyant x sur y . Soit $p(Y)$ l'ensemble

$$\{\gamma_a = w(Y - b) \mid \gamma_a = f_v(v(x - a)) \text{ et } b = f(a)\}_{a \in A}.$$

Supposons dans un premier temps que $p(Y)$ est réalisé dans N . Soit $y \in N$ réalisant $p(Y)$, notons B l'image $f(A)$. Alors $y \notin B$ et, pour $r \in R \setminus \{0\}$, $y.r \notin R$. On pose $\tilde{f}(a + x.r) = f(a) + y.r$. Puisque $v(A) = v(M)$ il suffit de voir que \tilde{f} est compatible avec f_v , i.e. vérifier que l'on a $f_v(v(a - x.r)) = w(f(a) - y.r)$, pour tout $a \in A$ et $r \in R \setminus \{0\}$. Soit alors $a \in A$ et $r \in R \setminus \{0\}$. Alors chaque z_i vérifiant $z_i.r = x.r - a$, pour $1 \leq i \leq \deg(r) - \deg_s r$, est de la forme $z_i = a_i - x$ avec $a_i.r = a$; de tels a_i sont tous dans A car A contient M_{tor} et est divisible. Par l'observation 3.2.4, pour un certain i , $v(z_i.r) = v(x.r - a) = \tau^k(v(z_i)) = \tau^k(v(a_i - x))$, où k est uniquement déterminé par r et par $v(x - a_i)$. Puisque y réalise $p(Y)$, $f_v(v(a_i - x)) = w(f(a_i) - y)$. Donc $f_v(\tau^k(v(a_i - x))) = \tau^k(f_v(v(a_i - x))) = \tau^k(w(f(a_i) - y))$. Il reste à vérifier que $\tau^k(w(f(a_i) - y)) = w(y.r - f(a))$. Puisque f est un L' -isomorphisme partiel, on a $f(a_i).r = f(a)$ et donc $y.r - f(a) = (y - f(a_i)).r$. Si $\tau^k(w(f(a_i) - y)) \neq w(y.r - f(a))$ alors nécessairement $\tau^k(w(f(a_i) - y)) = w(f(a_i) - y) = \theta$ et $w(y.r - f(a)) > \theta$. Alors, par le fait que $\tau^k(w(f(a_i) - y)) = w(f(a_i) - y)$, $v(x - a_i) = \tau^k(v(x - a_i)) = \theta$; d'où $v(x.r - a) = \theta$. Par ailleurs, par le fait que $(y.r - f(a)) > \theta$, il existe $b \in N$ tel que $b.r = f(a)$, $w(y - b) > \theta$ et $\tau^k(w(y - b)) = w(y.r - f(a))$. Dans ce cas $a' := f^{-1}(b)$ vérifie $a'.r = a$ et $v(x - a') > \theta$; donc $v(x.r - a) > \theta$. Contradiction.

Il reste à établir que $P(Y)$ est réalisable dans N . On va montrer qu'il est finiment consistant. Soit $\alpha = \{a_1, \dots, a_m\} \subset A$. On va trouver $y \in N$ tel que, pour tout $1 \leq i \leq m$, $\gamma_i := f_v(v(x -$

a_i) soit égal à $w(y - f(a_i))$. Soit \sim la relation d'équivalence sur α définie par $a_i \sim a_j$ si et seulement si $\gamma_i = \gamma_j$, et $\beta \subset \alpha$ la classe d'équivalence qui correspond à $\gamma := \max\{\gamma_i\}_{i \in \{1, \dots, m\}}$. Soit $a \in \beta$ et $a' \notin \beta$. Alors $f_v(v(x - a')) = f_v(v(x - a + a - a')) = f_v(v(a - a')) = w(f(a) - f(a')) = w(f(a) - y + y - f(a')) = w(f(a') - y)$. Cette observation montre que sans perdre de généralité on peut supposer $\alpha = \beta$. Soit $\delta = f_v^{-1}(\gamma)$, i.e. la valeur commune des $v(x - a)$, pour $a \in \alpha$. Alors pour tout $a \in \alpha$, la classe de x dans $M_\delta(a)$ est différent de la classe de chaque $a \in \alpha$. Pour conclure, il suffit de choisir un élément $y \in N$ dont la classe dans $N_\gamma(f(a))$ de la classe y soit différente de la classe de $f(a)$ pour tout $a \in \alpha$, ce qui est possible puisque $|M_\gamma(a)| = |N_\gamma(f(a))|$ du fait que f_v préserve les prédicats R_n . On conclut par le fait que N est $|M|^+$ -saturé. \blacksquare

Avant d'établir la conclusion de ce procédé de va-et-vient, on donne un résultat général d'élimination de quantificateur sur lequel on va s'appuyer.

Proposition 3.3.6. *Soient \mathcal{L} un langage contenant un symbole de constante, \mathcal{T} une \mathcal{L} -théorie, et Θ un ensemble de formules de \mathcal{L} clos par combinaisons booléennes. Supposons que :*

Pour tous $M, N \models \mathcal{T}$ et $M \supseteq A \xrightarrow{f} N$ où N est $|M|^+$ -saturé et f est un \mathcal{L} -plongement préservant les formules de Θ , il existe un \mathcal{L} -plongement g qui préserve Θ et prolonge f à M .

Alors toute formule de \mathcal{L} est équivalente à une formule de Θ .

PREUVE. Le cas où Θ est l'ensemble des formules sans quantificateur est bien connu (cf. [Ma] proposition 4.3.28). Le cas général s'y ramène en ajoutant au langage des prédicats $\{P_\phi \mid \phi \in \Theta\}$ et à la théorie les énoncés $\{\forall x P_\phi(x) \leftrightarrow \phi(x) \mid \phi \in \Theta\}$. \blacksquare

Soit $(F, v(F)) \models T_{h,d}$. Soit T_v la L'_{V_0} -théorie complète de $v(F)$ et Tor_F la L_R -théorie constituée d'énoncés de la forme $|\eta_F(r)| = n$ ou des ensembles d'énoncés exprimant $|\eta_F(r)| = \{\infty\}$. On considère $\mathbf{T} = T_{h,d} \cup T_v \cup \text{Tor}_F$, et l'ensemble Θ_v des L' -formules de la forme :

$$\varphi(\bar{x}) \bigwedge Q \bar{y}_1 \psi(\bar{y}_1, \bar{y}_2, v(t_1(\bar{x})), \dots, v(t_k(\bar{x}))), \text{ où :}$$

- φ est sans quantificateur dans L_R , ψ est sans quantificateur dans L_{V_0} , et Q est un ensemble des quantificateur,
- \bar{x} est un uplet de variables de la sorte de module, \bar{y}_1, \bar{y}_2 des uplets de variables de la sorte de l'ensemble des valeurs, et les t_i sont des L_R -termes en \bar{x} .

Théorème 3.3.7. *La théorie \mathbf{T} élimine les quantificateurs portant sur les variables de la sorte module : toute formule de L' est équivalente modulo \mathbf{T} à une formule de Θ_v .*

PREUVE. Soit $(A \subset M, v), (N, w)$ et $\mathbf{f} = (f, f_v) : A \rightarrow B \subset N$ vérifiant pour \mathbf{T} et Θ_v les hypothèses du critère de la proposition 3.3.6. Alors, par la proposition 3.3.4, il existe un L' -plongement $\hat{\mathbf{f}} = (\hat{f}, \hat{f}_v)$, étendant \mathbf{f} à (\hat{A}, v) . Puisque θ est l'unique point fixe de τ autre que ∞ et que tout élément $\gamma \in v(\hat{A}) \setminus \{0\}$ vérifie $\tau^k(\gamma) = \gamma_a$ pour un entier k et un $\gamma_a \in v(A)$; en particulier tout élément de $v(\hat{A})$ est $v(A)$ -définissable. Cela implique que $\hat{\mathbf{f}}$ préserve les formules de Θ_v . Donc on peut supposer que $A = \hat{A}$ et $B = \hat{B}$. Notons que puisque f_v préserve toutes les L'_{V_0} -formules, f_v est un plongement élémentaire (au sens de la théorie de $v(F)$)

de $v(A)$ dans $v(N)$. Soit $\gamma \in v(M) \setminus v(A)$. Puisque $v(N)$ est $|v(M)|^+$ -saturé, il est $|v(M)|^+$ -homogène. Comme f_v est partiel élémentaire il existe g_v partiel élémentaire prolongeant f_v sur $\Delta = v(A) \cup \{\tau^k(\gamma) \mid k \in \mathbb{Z}, \gamma \in A\}$. Soit $x \in M$ tel que $v(x) = \gamma$ et $y \in N$ tel que $w(y) = g_v(\gamma)$. Alors en posant $g(a + x.r) = f(a) + y.r$ pour tout $r \in R$ et $a \in A$, on obtient que $\mathbf{g} = (g, g_v)$ est un isomorphisme partiel entre $A \oplus x.R$ et $B \oplus y.R$. De plus, \mathbf{g} préserve les formules de Θ_v par le fait que g_v est partiel élémentaire. En effet, puisque $v(A)$ est clos par τ et τ^{-1} , pour tout $r \in R$, $v(x.r) \notin v(A)$. Donc, pour tout $r \in R$ et pour tout $a \in A$, $v(a + x.r) = \min\{v(a), v(x.r)\}$. En utilisant le fait que g_v est un L'_{V_0} -isomorphisme, on montre immédiatement que $g_v(v(a + x.r)) = w(f(a) + y.r)$.

Maintenant par la proposition 3.3.4 on peut étendre \mathbf{g} sur $\widehat{A + x.R}$, qui n'est autre que la clôture divisible de $A + x.R$. C'est-à-dire qu'on peut étendre \mathbf{g} à un modèle U tel que $v(U) = v(M)$. Alors, il suffit de prolonger g pour avoir un plongement prolongeant \mathbf{g} à M . Cela est possible par la proposition 3.3.5. ■

On en déduit les trois théorèmes ci-dessous.

Théorème 3.3.8 (A-K-E \equiv). *Soit (F, v) et (G, w) deux modèles de \mathbf{T} , tels que $v(F)$ et $v(G)$ sont élémentairement équivalents dans le langage L'_{V_0} . Alors (F, v) et (G, v) sont élémentairement équivalents dans le langage L' .*

PREUVE. Soit T_V la théorie complète de $v(F)$ dans le langage L'_{V_0} . Alors, modulo $\mathbf{T} = T_V \cup T$, tout L' -énoncé est équivalent à un énoncé de Θ_v . Or tout énoncé de Θ_v est équivalent à un énoncé de L'_{V_0} . ■

Les preuves des résultats qui suivent sont similaires à celle du théorème ci-dessus.

Théorème 3.3.9 (A-K-E \preceq). *Soit (F, v) et (G, w) deux modèles de \mathbf{T} tels que $v(F)$ se plonge élémentairement dans $v(G)$ par un L'_{V_0} -plongement. Alors (F, v) se plonge élémentairement dans une extension élémentaire de (G, w) .*

Théorème 3.3.10 (A-K-E \leq_{\exists}). *Soit $(F \subset G, v)$ deux modèles de \mathbf{T} tels que $v(F)$ est existentiellement clos dans $v(G)$ en tant que L'_{V_0} -structure. Alors (F, v) est existentiellement clos dans (G, v) en tant que L' -structure.*

Chapitre 4

$K[t; \varphi]$ -modules valués : K agit par translations sur la valuation

Comme précédemment, durant ce chapitre aussi, K désignera un corps avec un endomorphisme φ de $(K, +, \times, 1, 0)$ et R l'anneau $K[t; \varphi]$.

On va d'abord considérer des ensembles totalement ordonnés sur lesquels l'anneau R agit. Les chaînes $(\Delta, <, \tau, \infty)$ du chapitre précédent en étaient le cas simple où K agit trivialement sur Δ . C'est-à-dire qu'on avait, pour tout $\lambda \in K \setminus \{0\}$, $v(x.\lambda) = v(x)$. La croissance comparée de l'action de t , à savoir la fonction τ , et de l'action des constantes provenant de K impliquait alors que la partie de torsion était trivialement valuée. La différence est qu'on ne veut maintenant plus supposer cette hypothèse. On va faire agir K sur Δ par des "translations", puis on va étendre cette action à tout R . Les modèles envisagés seront en particulier les groupes de valuation des corps valués.

Puis on définira les modules dits non K -trivialement valués. On verra qu'il est possible d'avoir une théorie des extensions analogue à celle de Kaplansky dans son fameux article [Ka]. On introduira la notion de module valué henselien. La propriété de Hensel est vue ici comme un théorème d'inversion locale (cf. théorème 4.4.7). La notion clé de ce chapitre est la notion d'élément irrégulier. C'est un élément x tel que pour un certain $r \in R$, $v(x.r)$ n'est pas le résultat de l'action de r sur $v(x)$. La propriété de Hensel "régularise" une grande partie des éléments irréguliers mais pas tous. Nous aurons alors recours à la notion de «maximalité affine» (analogue à la maximalité algébrique pour les corps valués). Enfin ces résultats seront utilisés pour donner des résultats du type Ax-Kochen et Ershov, et un théorème de structure.

Je tiens à remercier Franz-Viktor Kuhlmann qui m'avait parlé de ses travaux sur les modules valués qu'il appelle "*valued modules with only finitely many exceptional values*". Il a également considéré dans son livre [Ku3] les extensions immédiates de modules valués, et fait une étude analogue à celle de Kaplansky sur les extensions immédiates de corps valués.

4.1 R -chaînes

On commence par décrire l'action des éléments de K , puis de R , sur un ensemble totalement ordonné. Le langage qu'on va utiliser est $L_V = \{<, (\cdot r)_{r \in R}, \infty\}$ où chaque $\cdot r$ est un symbole de

fonction unaire, $<$ un symbole de relation binaire et ∞ un symbole de constante. On appellera R -chaîne un modèle de la théorie que l'on axiomatise dans les lignes qui suivent.

Définition 4.1.1. Soit $(\Delta, <, \infty)$ un ensemble totalement ordonné avec un plus grand élément ∞ . On dit que la structure $(\Delta, <, \infty, (\cdot a)_{a \in K})$, où chaque $\cdot a$ est un symbole de fonction unaire, est une K -chaîne si, pour tous $a, b \in K \setminus \{0\}$ et pour tous $\gamma, \delta \in \Delta \setminus \{\infty\}$, on a :

1. $\gamma > \delta \rightarrow \gamma \cdot a > \delta \cdot a$
2. $(\gamma \cdot ab = (\gamma \cdot a) \cdot b) \wedge (\gamma \cdot 1 = \gamma) \wedge (\gamma \cdot 0 = \infty)$
3. $\gamma \cdot a \geq \gamma \rightarrow \delta \cdot a \geq \delta$
4. $(\gamma \cdot (a + b) \geq \min\{\gamma \cdot a, \gamma \cdot b\}) \wedge (\gamma \cdot a = \gamma \cdot -a)$
5. $\gamma \cdot a \neq \infty \wedge \infty \cdot b = \infty$

Proposition 4.1.2. L'ensemble $\mathcal{O} = \{a \in K \mid \forall \gamma \in \Delta \setminus \{\infty\}, \gamma \cdot a \geq \gamma\}$ est un anneau de valuation de K , d'idéal maximal $\{a \in K \mid \forall \gamma \in \Delta \setminus \{\infty\}, \gamma \cdot a > \gamma\}$.

PREUVE. La vérification est immédiate. On peut également consulter [Maa] page 8. ■

Notation 4.1.3. On désignera par v_K la valuation définie sur K par le sous-anneau \mathcal{O} ci-dessus, par K_0 le sous-corps de K fixé par φ , et par R_0 l'anneau $K_0[t; \varphi] \simeq K_0[t]$ qui est en particulier commutatif. Ensuite on notera $R_{\mathcal{O}}$ le sous-anneau de R constitué des polynômes à coefficient dans \mathcal{O} . Enfin, pour désigner l'ensemble des éléments séparables d'un sous-anneau R_m de R (par exemple $m = \mathcal{O}, 0 \dots$ etc.), on utilisera la notation $R_{m, sep}$.

On étend à R l'action de K sur Δ en définissant, pour $\gamma \in \Delta$ et $r \in R \setminus \{0\}$, la valeur $\gamma \cdot r$ en fonction des monômes de r . Soit Δ une K -chaîne. On choisit d'abord une action de t sur Δ , vérifiant :

6.a $\cdot t : \Delta \setminus \{\infty\} \rightarrow \Delta \setminus \{\infty\}$, est strictement croissante.

Puis on étend ces axiomes à tout R en décrétant, pour tout $\infty \neq \gamma \in \Delta$ et tout $0 \neq r = \sum_{i \in I} t^i a_i \in R$:

6.b $\gamma \cdot t^n a = (\dots((\gamma \cdot t) \cdot t) \dots) \cdot a$, ($0 \neq a \in K$ et $n \in \mathbb{N}$)

6.c $\gamma \cdot r = \min_{i \in I} \{\gamma \cdot t^i a_i\}$.

Cette action munit Δ d'une L_V -structure.

Notation 4.1.4. Conservant en cela l'habitude du chapitre précédent, on introduit la fonction τ et on notera indifféremment $\tau(\gamma)$ ou $\gamma \cdot t$.

Exemple 4.1.5. Soit (L, v) un corps valué de caractéristique $p > 0$, R l'anneau des polynômes additifs sur L , et $P(X) = \sum_{i \in I} a_i X^{p^i} \in R$. Interprétons $\gamma \cdot P(X)$, où $\gamma = v(x) \in v(L)$, comme

$$\min_{i \in I} \{v(x^{p^i} a_i)\} = \min_{i \in I} \{p^i \gamma + v(a_i)\}.$$

Alors $v(L)$ satisfait les axiomes 1 – 6.

Il est immédiat de vérifier les assertions du lemme suivant :

Lemme 4.1.6. Soit $r, q \in R$. On a $\gamma \cdot (r + q) \geq \min\{\gamma \cdot r, \gamma \cdot q\}$ et si $\gamma \cdot q \neq \gamma \cdot r$ alors $\gamma \cdot (r + q) = \min\{\gamma \cdot r, \gamma \cdot q\}$. ■

Définition 4.1.7. Soit Δ une L_V -structure. On dit que Δ est une R -chaîne si elle satisfait les (schémas d') axiomes 1 – 6 ci-dessus et vérifie :

7. Pour tout entier $k > 0$ et $0 \neq a \in K$,

$$\forall \gamma \in \Delta \setminus \{\infty\} \quad \tau^k(\gamma) \leq \gamma \cdot a \implies \forall \delta \quad (\delta < \gamma \rightarrow \tau^k(\delta) < \delta \cdot a).$$

Remarque 4.1.8. Si (M, v) est un module K -trivialement valué infini, non-trivialement valué comme dans le chapitre précédent, alors $v(M)$ est un R -chaîne.

Lemme 4.1.9. Soit Δ une R -chaîne, $j > i \in \mathbb{N}$, $0 \neq a, b \in K$ et $\gamma \in \Delta$. Soit $A = \{\gamma \in \Delta \mid \tau^j(\gamma) \cdot a < \tau^i(\gamma) \cdot b\}$. Alors A est un segment initial (éventuellement vide) de Δ et il existe au plus un $\gamma \in \Delta$ tel que

$$\tau^j(\gamma) \cdot a = \tau^i(\gamma) \cdot b.$$

Si A est une partie propre de Δ , si de plus τ est surjective sur Δ , et s'il n'existe aucun tel γ , alors A définit une coupure au sens de Dedekind; s'il existe un tel δ , alors il est limite inférieure et supérieure dans Δ .

PREUVE. Soit $\delta \in \Delta$ tel que $\tau^j(\delta) \leq \tau^i(\delta)$ et $\rho < \delta$. On va montrer que $\rho \in A$. Si $i = 0$, alors c'est l'axiome 7 qui l'affirme. Sinon, on pose $\alpha = \tau^i(\delta)$, $m = j - i$ et $c = b/a$. Par les axiomes 1 et 2, on a $\tau^m(\alpha) \leq \alpha \cdot c$. Comme $\tau^i(\rho) < \alpha$ (par l'axiome 6.a), par les axiomes 7 on a $\tau^m(\tau^i(\rho)) < \tau^i(\rho) \cdot c$. Cela montre à la fois que $\rho \in A$ et qu'il existe au plus un seul δ tel que l'égalité énoncée ait lieu.

Considérons le cas où τ est surjectif et $A \neq \emptyset, \Delta$. Il suffit de voir que A n'a pas de maximum et que l'ensemble $B = \{\gamma \in \Delta \mid \tau^j(\gamma) \cdot a > \tau^i(\gamma) \cdot b\}$ n'a pas de minimum. Posons de nouveau $c = b/a$. Soit $\delta \in \Delta \setminus \{\infty\}$. Alors

$$\begin{aligned} \delta \in A &\Leftrightarrow \tau^j(\delta) < \tau^i(\delta) \cdot c \Leftrightarrow \delta < \tau^{-j}(\tau^i(\delta) \cdot c) \Leftrightarrow \tau^i(\delta) \cdot c < \tau^i(\tau^{-j}[\tau^i(\delta) \cdot c]) \cdot c \\ &\Leftrightarrow \tau^{-j}[\tau^i(\delta) \cdot c] \in A \end{aligned}$$

En particulier, quand $\delta \in A$, on a $\delta < \tau^{-j}(\tau^i(\delta) \cdot c)$ et $\tau^{-j}(\tau^i(\delta) \cdot c) \in A$.

Pour montrer que B n'a pas de minimum, le raisonnement est le même en inversant les inégalités. ■

Notation 4.1.10. Notons en particulier qu'il existe au plus une seule valuation $\gamma \in \Delta$, $\gamma \neq \infty$, telle que $\tau(\gamma) = \gamma$. On va noter cette valeur θ quand elle existe. Dans ce cas, pour tout $\gamma < \theta$, on a $\tau(\gamma) < \gamma$, et pour tout $\delta > \theta$, $\tau(\delta) > \delta$.

Définition 4.1.11. Soit $r \in R \setminus \{0\}$. On écrit $r = \sum_{i \in I} t^i a_i$. Pour tout $i \in I$, on pose

$$U_i(r) = \{\gamma \in \Delta \mid \gamma \cdot r = \tau^i(\gamma) \cdot a_i\}$$

et

$$J(r) = \{j \in I \mid U_j(r) \neq \emptyset\}.$$

Remarquons que $J(r)$ n'est jamais vide et que $\Delta = \bigcup_{j \in J(r)} U_j(r)$. Le lemme suivant montrera que les $U_j(r)$ sont des intervalles.

Lemme 4.1.12. Soit $0 \neq r = \sum_{i \in I} t^i a_i \in R$, $m = \min J(r)$ et $M = \max J(r)$. Écrivons $J(r)$ comme $\{j_0, \dots, j_k\}$ avec $m = j_0 < j_1 < \dots < j_k = M$. Alors,

1. $U_M(r)$ est un segment initial de Δ et $U_m(r)$ un segment final. Si $i \in J(r)$ et $m < i < M$ alors $U_i(r)$ est un intervalle borné ou un singleton. De plus on a

$$U_M(r) < \dots U_{j_{i+1}} \leq U_{j_i} \dots < U_m(r)$$

où $U_l(r) \leq U_{l'}(r)$ signifie : $\forall \gamma \in U_l(r) \setminus U_{l'}(r) \quad \forall \delta \in U_{l'}(r), \quad \gamma < \delta$.

2. Soit $s < l \in \{0, \dots, k\}$ tels que $U_{j_s}(r) \cap U_{j_l}(r) \neq \emptyset$. Alors $U_{j_s}(r) \cap U_{j_l}(r)$ est un singleton et pour tout $i, s < i < l$, on a $U_{j_s}(r) \cap U_{j_i}(r) = U_{j_i}$.

PREUVE. Les preuves des différentes assertions de l'énoncé sont imbriquées les unes dans les autres.

Par le lemme 4.1.9, pour tous $l, l' \in J(r)$, avec $l \neq l'$, l'ensemble $\{\gamma \in \Delta \mid \tau^l(\gamma) \cdot a_l = \tau^{l'}(\gamma) \cdot a_{l'}\}$ est ou bien vide ou bien un singleton; en particulier $U_{j_l} \cap U_{j_{l'}}$ est un singleton ou vide. Ce lemme implique également que l'ensemble $\{\gamma \in \Delta \mid \tau^l(\gamma) \cdot a_l > \tau^{l'}(\gamma) \cdot a_{l'}\}$ est un segment final si et seulement si $l' < l$, et dans ce cas ce segment n'est pas vide car $l, l' \in J(r)$. Donc, pour tout l vérifiant $m < l \in J(r)$, $C_l := \{\gamma \in \Delta \mid \tau^l(\gamma) \cdot a_l > \tau^m(\gamma) \cdot a_m\}$ est différent de Δ et en est un segment final. D'où $C := \bigcap_{l > m} C_l$ est aussi un segment final de Δ . Clairement $C \subset U_m$. De plus, on a : $U_m \neq C$ si et seulement s'il existe $\gamma \in U_m$ et $l \in J(r)$ tels que $\tau^l(\gamma) \cdot a_l = \tau^m(\gamma) \cdot a_m$. Soit l_1, \dots, l_s tous les éléments de $J(r)$ qui sont supérieurs à m et vérifient

$$\tau^{l_1}(\gamma) \cdot a_{l_1} = \dots = \tau^{l_s}(\gamma) \cdot a_{l_s} = \tau^m(\gamma) \cdot a_m.$$

Or il existe au plus un tel γ . En conséquence, U_m est de la forme $C \cup \varepsilon$ où ε est ou vide ou un singleton, en particulier U_m est un segment final. De même, pour tout $l \in J(r), l < M$, l'ensemble $A_l = \{\gamma \in \Delta \mid \tau^l(\gamma) \cdot a_l \geq \tau^M(\gamma) \cdot a_M\} \neq \Delta$ et est un segment initial. On a de même, avec $A := \bigcap_{l < M} A_l$, $U_M(r) = A \cup \varepsilon$ où ε est ou vide ou un singleton.

Voyons que pour tout $1 \leq i \leq k-1$, U_{j_i} est un intervalle ou un singleton. Soit $\gamma, \delta \in U_{j_i}(r)$, $\gamma < \delta$. Soit $\rho \in \Delta$ tel que $\gamma < \rho < \delta$. Supposons par l'absurde que $\rho \cdot r = \tau^j(\rho) \cdot a_j$ pour un $j \in J(r) \setminus \{j_i\}$. Donc $\tau^j(\rho) \cdot a_j < \tau^{j_i}(\rho) \cdot a_{j_i}$. Si $j < j_i$, par le lemme 4.1.9, on devrait avoir $\tau^j(\delta) \cdot a_j < \tau^{j_i}(\delta) \cdot a_{j_i}$. Si $j > j_i$, de même on devrait avoir $\tau^j(\gamma) \cdot a_j < \tau^{j_i}(\gamma) \cdot a_{j_i}$.

Enfin montrons que $U_{j_{i+1}} \leq U_{j_i}$. On a par les paragraphes précédents $U_m = U_{j_0} \geq U_{j_i} \geq U_{j_k} = U_M$ pour tout i . Soit $\gamma \in U_{j_i} \setminus U_{j_{i+1}}$. On a $\tau^{j_i}(\gamma) \cdot a_{j_i} < \tau^{j_{i+1}}(\gamma) \cdot a_{j_{i+1}}$. Par conséquent, pour tout $\delta > \gamma$, $\tau^{j_i}(\delta) \cdot a_{j_i} < \tau^{j_{i+1}}(\delta) \cdot a_{j_{i+1}}$. Donc $\delta \notin U_{j_{i+1}}$. Cela montre que $\gamma > U_{j_{i+1}}$. ■

Remarque 4.1.13. Avec les notations du lemme ci-dessus, posons $B_0 = \emptyset$ et, pour tout entier $i, 1 \leq i \leq k$, $B_i = \{\gamma \in \Delta \mid \tau^{j_i}(\gamma) \cdot a_{j_i} > \tau^{j_{i-1}}(\gamma) \cdot a_{j_{i-1}}\}$. Alors les B_i contiennent tous C et sont des segments finaux de Δ . De plus, $B_i \cap U_{j_i} = \emptyset$. Donc on a $B_i \subset B_{i+1}$ et U_{j_i} est de la forme $(B_{i+1} \setminus B_i) \cup \varepsilon$, avec ε vide ou un singleton.

Corollaire 4.1.14. *Pour tout $r \in R \setminus \{0\}$, la fonction $\cdot r : \Delta \rightarrow \Delta, \gamma \mapsto \gamma \cdot r$, est strictement croissante. De plus pour tous $p, q \in R$, on a $(\gamma \cdot p) \cdot q = \gamma \cdot pq$.*

PREUVE. Soit $\gamma < \delta \in \Delta$. Puisque la fonction $\cdot r$ est strictement croissante sur chaque intervalle U_j ($j \in J(r)$), il suffit de traiter le cas où il existe des entiers $j, k \in J(r)$, $j \neq k$,

pour lesquels $\gamma \in U_j \setminus U_k$ et $\delta \in U_k \setminus U_j$. On écrit $r = \sum_{i \in I} t^i a_i$. Par le lemme 4.1.11, on a nécessairement $k < j$ et, par le lemme 4.1.9, $\gamma \cdot r = \gamma \cdot t^j a_j < \gamma \cdot t^k a_k$; d'où $\gamma \cdot r < \delta \cdot t^k a_k = \delta \cdot r$.

Soit $0 \neq p = \sum_{i \in I} t^i a_i, q = \sum_{j \in J} t^j b_j \in R$ et $\gamma \in \Delta$. Montrons l'égalité $(\gamma) \cdot p \cdot q = \gamma \cdot pq$. On a $pq = \sum_k t^k c_k$ avec $c_k = \sum_{i+j=k} a_i^{\varphi_j} b_j$. Soit $\gamma \in \Delta$ et $i_0 \in J(p)$ tels que $\gamma \cdot p = \tau^{i_0}(\gamma) \cdot a_{i_0}$. Posons $\delta = \tau^{i_0}(\gamma) \cdot a_{i_0}$ et soit $j_0 \in J(q)$ tel que $\tau^{j_0}(\delta) \cdot b_{j_0} = \delta \cdot q$. Soit $(i, j) \in I \times J$. Alors $\tau^j(\delta) \cdot b_j \geq \tau^{j_0}(\delta) \cdot b_{j_0}$ et par le fait que $\tau^i(\gamma) \cdot a_i \geq \delta$, on a $\tau^{j_0}(\delta) \cdot b_{j_0} \leq \tau^j(\tau^i(\gamma) \cdot a_i) \cdot b_j$. Or, par le schéma 6.b, ce dernier terme est égal à $\tau^{i+j}(\gamma) \cdot a_i^{\varphi_j} b_j$. Par l'axiome 4, $\tau^{j_0}(\delta) \cdot b_{j_0} \leq \tau^{i+j}(\gamma) \cdot c_{i+j}$. D'où $(\gamma \cdot p) \cdot q \leq \gamma \cdot pq$.

Montrons l'inégalité inverse. Soit i_0, j_0 comme ci-dessus. On peut supposer que $i_0 = \min\{i \in I \mid \gamma \cdot p = \gamma \cdot t^i a_i\}$ et $j_0 = \min\{j \in J \mid (\gamma \cdot p) \cdot t^j b_j = (\gamma \cdot p) \cdot q\}$. Posons $k_0 = i_0 + j_0$. Si $k_0 = \min I + \min J$ alors $i_0 = \min I$ et $j_0 = \min J$, et $t^{k_0} a_{i_0}^{\varphi_{j_0}} b_{j_0} = t^{k_0} c_{k_0}$ est le monôme de plus petit de degré de pq . Par le paragraphe ci-dessus, $\gamma \cdot t^{k_0} c_{k_0} \leq \gamma \cdot t^k c_k$ pour tout k , donc $t^{k_0} c_{k_0} = \gamma \cdot pq$, par conséquent $\gamma \cdot pq = (\gamma \cdot p) \cdot q$. Si $k_0 = \deg(p) + \deg(q)$, on montre de même l'égalité voulue. Considérons le cas où $\deg(p) + \deg(q) > k_0 > \min I + \min J$. Écrivons le monôme $t^{k_0} c_{k_0}$ comme $t^{k_0} a_{i_0}^{\varphi_{j_0}} b_{j_0} + t^{k_0} a_{i_1}^{\varphi_{j_1}} b_{j_1} + \dots + t^{k_0} a_{i_l}^{\varphi_{j_l}} b_{j_l}$. Supposons $\gamma \cdot t^{k_0} c_{k_0} > \gamma \cdot t^{k_0} a_{i_0}^{\varphi_{j_0}} b_{j_0}$. Puisque $\gamma \cdot t^{k_0} a_{i_0}^{\varphi_{j_0}} b_{j_0} \leq \gamma \cdot t^{k_0} a_i^{\varphi_j} b_j$ pour tout $(i, j) \in I \times J$ par ce qui précède, l'ensemble $S := \{s \in \{1, \dots, l\} \mid \gamma \cdot t^{k_0} a_{i_s}^{\varphi_{j_s}} b_{j_s} = \gamma \cdot t^{k_0} a_{i_0}^{\varphi_{j_0}} b_{j_0}\}$ est nécessairement non-vide. Soit $s \in S$. En écrivant $t^{k_0} a_{i_s}^{\varphi_{j_s}} b_{j_s} = t^{i_s} a_{i_s} t^{j_s} b_{j_s}$, on voit que nécessairement $\gamma \cdot t^{i_s} a_{i_s} = \gamma \cdot t^{i_0} a_{i_0} = \gamma \cdot p$ car sinon, comme $(\gamma \cdot t^{i_0} a_{i_0}) \cdot t^{j_s} b_{j_s} \geq (\gamma \cdot t^{i_0} a_{i_0}) \cdot t^{j_0} b_{j_0}$, $\gamma \cdot t^{i_s} a_{i_s} > \gamma \cdot t^{i_0} a_{i_0}$ impliquerait $\gamma \cdot t^{k_0} a_{i_s}^{\varphi_{j_s}} b_{j_s} > \gamma \cdot t^{k_0} a_{i_0}^{\varphi_{j_0}} b_{j_0}$. Donc on a également $\gamma \cdot t^{i_s} a_{i_s} \cdot t^{j_s} b_{j_s} = (\gamma \cdot p) \cdot q$. En conséquence, $i_s > i_0$ et $j_s > j_0$. Mais $i_s + j_s = k_0$: contradiction. \blacksquare

Définition 4.1.15. Soit Δ une R -chaîne. On appellera saut potentiel, tout élément de l'ensemble

$$\{\delta \in \Delta \setminus \{\infty\} \mid \tau^i(\delta) \cdot a = \tau^j(\delta) \cdot b \text{ pour } i > j, i, j \in \mathbb{N} \setminus \{0\}, \text{ et pour } a, b \in K^\times\}.$$

Définition 4.1.16. On dira qu'une R -chaîne Δ est pleine si

1. τ est surjective sur Δ ,
2. tout segment initial de la forme $\{\gamma \in \Delta \setminus \{\infty\} \mid \tau^i(\gamma) \leq \gamma \cdot a\}$, où $i \in \mathbb{N} \setminus \{0\}$ et $a \in K^\times$, est propre
3. pour tous $i \in \mathbb{N} \setminus \{0\}$ et $a \in K^\times$, il existe $\gamma \in \Delta \setminus \{\infty\}$ tel que $\tau^i(\gamma) \cdot a = \gamma$.

Remarque 4.1.17. Par surjectivité de τ , dans une R -chaîne pleine toute équation en γ de la forme $\tau^i(\gamma) \cdot a = \tau^j(\gamma) \cdot b$, avec des entiers naturels $i > j$ et $a, b \in K \setminus \{0\}$, a une solution qui est unique par le lemme 4.1.9; en particulier si γ est une solution de cette équation, alors pour tout $\delta \in \Delta \setminus \{\infty\}$,

$$\begin{aligned} \delta > \gamma &\Rightarrow \tau^i(\delta) \cdot a > \tau^j(\delta) \cdot b \\ \delta < \gamma &\Rightarrow \tau^i(\delta) \cdot a < \tau^j(\delta) \cdot b. \end{aligned}$$

Proposition 4.1.18. Toute R -chaîne satisfaisant les conditions 1 et 2 de la définition ci-dessus se plonge dans une R -chaîne pleine, dans laquelle elle est dense.

PREUVE. Soit CS l'ensemble des coupures données comme dans le lemme 4.1.9; ce sont des segments initiaux propres par hypothèse, que l'on ordonne par l'inclusion. Notons $\Delta^p := \Delta \cup CS$

et désignons un élément de Δ^p par la notation $[\gamma]$. Définissons $[\gamma] \cdot t := \{\delta \cdot t \mid \delta \in [\gamma]\}$ et, pour $a \in K \setminus \{0\}$, $[\gamma] \cdot a := \{\delta \cdot a \mid \delta \in [\gamma]\}$. Il est clair que CS est stable par τ , τ^{-1} et par l'action de K^\times . Ceci permet d'étendre l'action de R sur Δ^p . Pour voir qu'il s'agit d'une K -chaîne, il est facile de vérifier les axiomes 1, 2, 4 et 5 de la définition 4.1.1 ; pour vérifier les axiomes 3, il suffit de voir que, pour tout $a \in \mathcal{O}_K$, l'on a $[\gamma] \cdot a := \{\gamma' \cdot a \mid \gamma' \in [\gamma]\} \supseteq [\gamma]$, pour tout $[\gamma] \in \Delta^p$. Ceci est clair car pour tout $[\gamma] \in \Delta^p$ et pour tout $\gamma' \in [\gamma]$ on a $\gamma' \cdot a \geq \gamma'$, d'où $\gamma' \in [\gamma] \cdot a$.

Les axiomes 6 et 7 des R -chaînes et l'unicité suivent de la construction. ■

Remarque 4.1.19. Clairement Δ^p est minimale parmi les extensions pleines de Δ dans lesquelles Δ est dense.

Remarque 4.1.20. Si Δ est un groupe abélien ordonné plein comme $K[t; x \mapsto x^p]$ -chaîne, alors il est divisible.

PREUVE. Dans Δ on a une solution à toute équation de la forme : $p^n \gamma + \delta = \gamma$. Il suffit alors de montrer que si Δ est divisible par $p^n - 1$ pour tout entier $n > 1$, alors Δ est divisible. Soit $q \neq p$, un nombre premier. Alors, par le petit théorème de Fermat, $p^{q-1} - 1$ est divisible par q . Comme Δ est divisible par $p^{q-1} - 1$, il est q -divisible. Donc Δ , étant divisible par tout nombre premier $q \neq p$, et par p d'après l'hypothèse, est divisible. ■

4.2 Modules valués dans une R -chaîne

Définition 4.2.1. Soit (M, v) un groupe abélien valué. On dit que c'est un K -espace vectoriel valué si M est un K -espace vectoriel et $v(M)$ une K -chaîne tels que, pour tout $x \in M$ et pour tout $\mu \in K$, $v(x \cdot \mu) = v(x) \cdot \mu$.

Définition 4.2.2. Soit (M, v) un groupe valué. On dira que (M, v) est un module valué si M est un R -module et $\Delta := v(M)$ une R -chaîne, tels que (M, v) est un K -espace vectoriel valué satisfaisant $v(x \cdot t) = \tau(v(x))$ pour tout $x \in M$. On dira que (M, v) est non K -trivialement valué si la valuation v_K est non triviale sur K .

Remarque 4.2.3. Par la remarque 4.1.8 la classe des modules K -trivialement valués est exactement la classe des modules valués au sens de la définition ci-dessus et tels que la valuation induite v_K sur K est triviale.

Sauf mention contraire, dans ce qui suit, (M, v) désignera un module valué, et $\Delta = v(M)$.

Remarque 4.2.4. Soit $x \in M \setminus \{0\}$ et $r = \sum_{i \in I} t^i a_i \in R \setminus \{0\}$. Alors on a

$$v(x \cdot r) = v\left(\sum_{i \in I} x \cdot t^i a_i\right) \geq \min_{i \in I} (v(x \cdot t^i a_i)) = \min_{i \in I} (v(x) \cdot t^i a_i) = v(x) \cdot r.$$

Définition 4.2.5. On dira que $x \in M \setminus \{0\}$ est régulier pour r si $v(x \cdot r) = v(x) \cdot r$, et régulier tout court si x est régulier pour tout r non nul. On dira qu'une partie $A \subset M$ est régulière si tous ses éléments sont réguliers.

Remarque 4.2.6. Tout élément non nul annulé par un polynôme $r \neq 0$ est irrégulier. Si $x \in \text{ann}_M(r)$ et si $y \in M$ est tel que $v(y) > v(x)$, alors $v((x+y).r) = v(y.r) \geq v(y) \cdot r > v(x) \cdot r$. Donc $x+y$ est irrégulier.

Définition 4.2.7. Soit $r = t^n a_n + \dots + ta_1 + a_0 \in R \setminus \{0\}$. On définit $Saut_M(r)$ comme étant l'ensemble $\{\gamma \in \Delta \mid \exists x \in M \ v(x) = \gamma \wedge v(x.r) > \gamma \cdot r\}$.

Notation 4.2.8. On notera $Saut_M(R)$, l'union des $Saut_M(r)$, pour $r \in R \setminus \{0\}$.

Proposition 4.2.9. Pour un polynôme $r \in R$, si $\gamma \in Saut_M(r)$ alors γ vérifie nécessairement une équation de la forme $\tau^i(\gamma) \cdot a_i = \tau^j(\gamma) \cdot a_j$. Par le lemme 4.1.9 $Saut_M(r)$ est fini.

Notation 4.2.10. Si $Saut_M(r) \neq \emptyset$, γ_r désignera son maximum.

Lemme 4.2.11. 1. Soit $x \in M$ et $r, q \in R \setminus \{0\}$. Alors on a l'équivalence : x est régulier pour r et $x.r$ régulier pour q , si et seulement si, x est régulier pour rq .

2. Si (M, v) est un module non K -trivialement valué et $|R|^+$ -saturé alors il possède un élément régulier.

3. L'ensemble des éléments réguliers est stable sous l'action de R , mais n'est pas en général un sous-module.

PREUVE.

1. Si x est régulier pour r et $x.r$ régulier pour q alors $v(x.rq) = v(x.r) \cdot q = (v(x) \cdot r) \cdot q = v(x) \cdot rq$ par le corollaire 4.1.14. Réciproquement, si x est régulier pour rq , alors $v((x.r).q) = v(x.rq) = v(x) \cdot rq = (v(x) \cdot r) \cdot q$ et, par croissance stricte des fonctions $\cdot q$ et $\cdot r$, x est régulier pour r et $x.r$ est régulier pour q .

2. C'est juste parce que l'ensemble des sauts d'un polynôme donné est fini et que $v(M)$ est infini puisque la valuation v_K sur K est non-triviale.

3. La première assertion suit du point 1. Montrons la seconde. Si (M, v) est non K -trivialement valué $|R|^+$ -saturé, et $|M_{\text{tor}}| \geq 2$, alors il existe $\delta \in v(M)$ tel que $\delta < v(Saut_M(r))$ pour tout $r \in R \setminus \{0\}$. Soit $x, y \in M_{\text{tor}} \setminus \{0\}$, $x \neq y$ et $z \in M$ de valuation δ . Alors $u := z + x$ et $v := z + y$ sont réguliers, ce qui n'est pas le cas pour $u - v$ qui appartient à M_{tor} . \blacksquare

4.3 Extensions de modules valués

Définition 4.3.1. Si $i : M \rightarrow N$ est un plongement de R -modules, on dit que N est une extension transcendante de M s'il existe $x \in N$ tel que, pour tout $0 \neq r \in R$, alors $x.r \notin i(M)$. Sinon on dit que N est une extension affine de M .

Lemme 4.3.2. Soit A un sous-module d'un module valué t -divisible (M, v) . Alors l'ensemble $A^t := \{x \in M \mid \exists n \in \mathbb{N} \ x.t^n \in A\}$ est un R -sous-module de M qui est une extension affine de A . De plus, pour tout $x \in M$ et $r \in R \setminus \{0\}$, si $x.r \in A$, alors $v(x) \in v(A^t) \cup Saut_M(r)$.

PREUVE. Clairement A^t est un sous-groupe de M et une extension affine de A . Soit $r \in R$ et $x \in A^t$, alors $(x.r).t^n = x.(t^n r^{\varphi^n}) = (x.t^n).r^{\varphi^n}$, qui appartient à A quand $x.t^n \in A$. Donc A^t est un sous-module de M .

Soit $x \in M \setminus \{0\}$ tel que $x.r \in A$. Disons $x.r = a \in A$. Si $v(x) \notin \text{Saut}_M(r)$, alors $v(x.r) = v(x) \cdot r$ est de la forme $\tau(v(x))^k \cdot a_k$, donc $v(x) = \tau^{-k}(v(a.a_k^{-1})) = v((a.a_k^{-1}).t^{-k})$. ■

Dans ce qui suit (M, v) désignera un module valué.

Définition 4.3.3. Soit Ω un ordinal limite et $(a_\gamma)_{\gamma \in \Omega}$ une suite d'éléments de M indexés par Ω . On dit que $(a_\gamma)_{\gamma \in \Omega}$ est pseudo-Cauchy si, pour tous $\gamma > \delta > \rho$ suffisamment grands,

$$v(a_\gamma - a_\delta) > v(a_\delta - a_\rho). \quad (4.1)$$

Si $(a_\gamma)_{\gamma \in \Omega}$ est une suite pseudo-Cauchy, on déduit des axiomes des groupes valués que, pour $\rho > \gamma$, la valeur $v(a_\gamma - a_\rho)$ ne dépend que de γ . On la notera par la suite δ_γ . On dit que $(a_\gamma)_{\gamma \in \Omega}$ converge dans M s'il existe $z \in M$ tel que $v(z - a_\gamma) = \delta_\gamma$ pour tout $\gamma \in \Omega$; z est alors dit limite de la suite $(a_\gamma)_{\gamma \in \Omega}$.

Remarque 4.3.4. Il n'y a pas unicité de la limite. En effet, soit $\mathcal{U} = \{y \in M \mid v(y) > \delta_\gamma \text{ pour tout } \gamma\}$. Alors, l'ensemble des limites est $z + \mathcal{U}$. Toujours par les axiomes des groupes valués on déduit que la suite des valuations $(v(a_\gamma))_{\gamma \in \Omega}$ est ou bien strictement croissante -ce cas se produit si et seulement si $(a_\gamma)_\gamma$ a 0 parmi ses limites- ou bien constante à partir d'un certain rang. Pour les démonstrations on renvoie à [Ka].

Le fait qu'étant donné $r \in R \setminus \{0\}$ l'ensemble $\text{Saut}_M(r)$ est fini implique :

Lemme 4.3.5. Soit $(a_\gamma)_\gamma$ une suite pseudo-Cauchy de M et $r \in R \setminus \{0\}$. Alors, pour tous δ et γ assez grands vérifiant $\delta > \gamma$, $a_\delta - a_\gamma$ est régulier pour r .

PREUVE. Par définition d'une suite pseudo-Cauchy, la suite $v(a_{\gamma+1} - a_\gamma)_\gamma$ est strictement croissante. Or, l'ensemble $\text{Saut}_M(r)$ est fini. D'où le résultat. ■

Corollaire 4.3.6. Soit $(a_\gamma)_{\gamma \in \Omega}$ une suite pseudo-Cauchy de M . Soit $r \in R \setminus \{0\}$ et $a \in M$. Alors la suite définie par $z_\gamma = a_\gamma.r - a$ est pseudo-Cauchy.

PREUVE. On a $z_\gamma - z_\rho = (a_\gamma - a_\rho).r$. Par le lemme ci-dessus, pour tous γ et ρ suffisamment grands, l'élément $a_\gamma - a_\rho$ est régulier. La fonction $\cdot r$ étant strictement croissante sur Δ , le fait que $v(a_\gamma.r - a_\rho.r) = v(a_\gamma - a_\rho) \cdot r$ implique l'assertion. ■

Soit $(z_\gamma = a_\gamma.r - a)_{\gamma < \Omega}$ définie comme dans le lemme ci-dessus. Par la remarque 4.3.4 la suite des valuations $v(z_\gamma)_{\gamma \in \Omega}$ est soit strictement croissante à partir d'un certain rang soit constante à partir d'un certain rang. C'est-à-dire qu'on a ou bien :

$$v(a_\gamma.r - a) > v(a_\delta.r - a) \quad \text{pour tous } \gamma > \delta \text{ suffisamment grands,} \quad (4.2)$$

ou bien :

$$v(a_\gamma.r - a) = v(a_\delta.r - a) \quad \text{pour tous } \gamma > \delta \text{ suffisamment grands.} \quad (4.3)$$

Notons que dans le premier cas la suite $(a_\gamma.r - a)_{\gamma < \Omega}$ converge vers 0; autrement dit, la suite $(a_\gamma.r)_\gamma$ converge vers a .

Définition 4.3.7. Soit $(a_\gamma)_{\gamma \in \Omega}$ une suite pseudo-Cauchy de M . On dit qu'elle est de type affine s'il existe $r \in R$ et $a \in M$ tel que la suite $(a_\gamma.r - a)_\gamma$ satisfait la condition (4.2) ci-dessus. Si ce n'est pas le cas, on dit que la suite $(a_\gamma)_\gamma$ est de type transcendant.

Remarque 4.3.8. Dire qu'une suite pseudo-Cauchy $(a_\gamma)_\gamma$ de M est de type affine est équivalent à dire que, pour un certain $r \in R \setminus \{0\}$, la suite $(a_\gamma.r)_\gamma$ a une limite dans M .

Lemme 4.3.9. Soit $(a_\gamma)_\gamma$ une suite pseudo-Cauchy de M de type affine et $r \in R$ tels que $(a_\gamma.r)_\gamma$ converge vers $a \in M$. Alors,

1. pour tout $q \in R \setminus \{0\}$, $(a_\gamma.rq)_\gamma$ converge vers $a.q$ et $(a_\gamma.q)_\gamma$ est de type affine.
2. Supposons $r \in R$ de degré minimal tel que $(a_\gamma.r)_\gamma$ a une limite dans M . Soit $q \in R$ de degré $\geq \deg(r)$ et supposons que $m \in M$ est une limite de la suite $(a_\gamma.q)_\gamma$. Alors, après avoir effectué la division euclidienne $q = rr' + r_0$ de q par r , il existe λ tel que, pour tout $\delta \geq \lambda$, $m - a_\delta.r_0$ est une limite de la suite $(a_\gamma.r.r')_\gamma$.

PREUVE. 1. Soit $q \in R \setminus \{0\}$. Pour tout $\gamma \in v(M) \setminus \{0\}$, assez grand, $a_\gamma.r - a$ est régulier pour q , i.e. $v((a_\gamma.r - a).q) = v(a_\gamma.r - a) \cdot q$. D'où il existe λ tel que la suite $(v((a_\gamma.r - a).q))_{\gamma \geq \lambda}$ est strictement croissante. Si $r', q' \in R \setminus \{0\}$ sont tels que $rr' = qq'$, alors $(a_\gamma.r.r')_\gamma$ converge vers $a.r'$. Cela montre que $(a_\gamma.q)_\gamma$ est de type affine.

2. Puisque $\deg(r_0) < \deg(r)$, la suite $v(a_\gamma.r_0 + (a.r' - m))_\gamma$ est constante à partir d'un certain rang λ_1 . D'autre part, par le point 1, $a.r'$ est une limite de la suite $(a_\gamma.r.r')_\gamma$, i.e. la suite $(v(a_\gamma.r.r' - a.r'))_\gamma$ est strictement croissante à partir d'un certain rang λ_2 . Or $(v(a_\gamma.q - m))_\gamma = (v(a_\gamma.r.r' - a.r' + a_\gamma.r_0 + (a.r' - m)))_\gamma$ est strictement croissante à partir d'un certain rang λ_3 . Soit $\lambda > \max\{\lambda_i \mid i = 1, 2, 3\}$. Alors pour tous $\gamma, \delta > \lambda$, on a nécessairement

$$v(a_\delta.r_0 + (a.r' - m)) = v(a_\gamma.r_0 + (a.r' - m)) > v(a_\gamma.r.r' - a.r').$$

Notons $b_\gamma = a_\gamma.r.r'$ et comme d'habitude $\delta_\gamma = v(b_{\gamma+1} - b_\gamma)$. Alors, par le fait que $a.r'$ est une limite de $(b_\gamma)_\gamma$, on a pour tout γ assez grand, $v(b_{\gamma+1} - b_\gamma) = v(a_\gamma.r.r' - a.r')$. Puis en posant $\mathcal{U} = \{z \in M \mid \forall \gamma \ v(z) > \delta_\gamma\}$ on sait que les limites de $(b_\gamma)_\gamma$ sont de la forme $\mathcal{U} + a.r'$. Donc on a montré que $m - a_\delta.r_0 - a.r' \in \mathcal{U}$, i.e. $m - a_\delta.r_0$ est également limite de la suite $(a_\gamma.r.r')_\gamma$. ■

Remarque 4.3.10. Dans le lemme ci-dessus, en prenant $r = 1$, on montre en particulier que pour tout $q \in R \setminus \{0\}$, pour toute suite pseudo-Cauchy $(a_\gamma)_\gamma$ et pour tout $a \in M$, si $(a_\gamma)_\gamma$ converge vers a , alors $a_\gamma.q$ converge vers $a.q$.

Définition 4.3.11. On notera $\mathbf{i} : (M, v) \rightarrow (N, w)$ et on appellera plongement de modules valués, tout couple d'applications (i, i_v) tel que $i : M \rightarrow N$ est un plongement de R -module et $i_v : v(M) \rightarrow w(N)$ est un plongement de R -chaînes, tels que pour tout $x \in M$, $i_v(v(x)) = w(i(x))$. On dira que N est une extension immédiate de M si, pour tout $z \in N \setminus \{0\}$, il existe $x \in M$ tel que $v(z - i(x)) > v(z)$.

Remarque 4.3.12. Soit N une extension immédiate de M comme ci-dessus. Alors $w(i(M)) = w(N)$ et pour tout $\gamma \in w(N)$, $N_{\geq \gamma} / N_{> \gamma} = i(M)_{\geq \gamma} / i(M)_{> \gamma}$.

Proposition 4.3.13. Si $(M \subset N, v)$ est une extension immédiate propre alors tout élément de $N \setminus M$ est limite d'une suite pseudo-Cauchy de M sans limite dans M .

PREUVE. Soit $(M \subset N, v)$ une extension immédiate de modules valués comme énoncé. Alors $v(M) = v(N)$ et, si $b \in N \setminus M$, alors l'ensemble $S = \{v(a - b) \mid a \in M\}$ n'a pas d'élément

maximal. Soit $(\delta_\rho)_\rho$ une suite cofinale croissante dans S et, pour tout ρ , un élément $a_\rho \in M$ tel que $v(a_\rho - b) = \delta_\rho$. Par l'inégalité ultramétrique, si $\sigma < \rho$, alors $v(a_\rho - a_\sigma) = \delta_\sigma$; et donc $(a_\rho)_\rho$ est pseudo-Cauchy convergeant vers b . De plus cette suite n'a pas de limite dans M . En effet si $a \in M$ en est une limite, alors $v(a - b) > v(a_\rho - a_\sigma) = v(b - a_\sigma) = \delta_\sigma$ pour tout $\rho > \sigma$. Ceci contredit le fait que la suite δ_ρ est cofinale dans S . \blacksquare

Définition 4.3.14. On dit qu'un module valué est maximal s'il n'admet aucune extension immédiate propre. Il est dit affinement maximal s'il n'admet aucune extension immédiate affine propre.

Corollaire 4.3.15. Si dans (M, v) toute suite pseudo-Cauchy a une limite alors (M, v) est maximal.

PREUVE. Le résultat suit de la proposition 4.3.13 \blacksquare

Les propositions qui suivent établiront la réciproque du corollaire 4.3.15.

Proposition 4.3.16. Soit (M, v) un R -module valué et $(a_\gamma)_{\gamma \in \Omega}$ une suite pseudo-Cauchy de M , de type transcendant et sans limite dans M . Soit $x.R$ le R -module libre à un seul générateur x . Alors $M \oplus x.R$ admet une structure de module valué qui en fait une extension immédiate de M telle que x soit une limite de $(a_\gamma)_{\gamma \in \Omega}$. De plus, si (N, v) est une extension immédiate de M et $y \in N$ une limite de $(a_\gamma)_\gamma$, alors y n'est pas un élément de torsion, $y.R \cap M = 0$, et $M \oplus y.R$ est isomorphe en tant que module valué à $M \oplus x.R$, par un isomorphisme fixant M et envoyant x sur y .

PREUVE. Pour définir la valuation sur $M \oplus x.R$, considérons $m \in M$ et $r \in R \setminus \{0\}$. Puisque la suite $(a_\gamma)_{\gamma \in \Omega}$ est de type transcendant, la suite des valuations $(v(m + a_\gamma.r))_{\gamma \in \Omega}$ est constante à partir d'un certain rang λ . Alors on pose $v(m + x.r) = v(m + a_\gamma.r)$ avec $\gamma \geq \lambda$.

Il est clair que $M \oplus x.R$ est un groupe valué. Pour voir que $M \oplus x.R$ est un module valué, il suffit alors de vérifier que pour tout $(m, r, \mu) \in M \times R \times K$, on a $v((m + x.r)t\mu) = \tau(v(m + x.r)) \cdot \mu$. Soit λ tel que la suite des valuations $(v(m + a_\gamma.r))_\gamma$ est constante à partir de λ . Alors la suite des valuations $v((m + a_\gamma.r).t\mu)_\gamma = (\tau(v(m + a_\gamma.r)) \cdot \mu)_\gamma$ est aussi constante à partir du rang λ . Par conséquent, si $\rho > \lambda$, on a $v((m + x.r).t\mu) = v((m + a_\rho.r).t\mu) = \tau(v(m + a_\rho.r)) \cdot \mu = \tau(v(m + x.r)) \cdot \mu$.

Montrons que $M' := M \oplus x.R$ est une extension immédiate de M . Pour tous $r \in R \setminus \{0\}$ et $m \in M$, il suffit de montrer qu'il existe ρ tel que $\delta_\rho \cdot r := v(a_{\rho+1} - a_\rho) \cdot r > v(x.r + m)$. En effet, dans ce cas, pour un tel ρ fixé, la suite $v(a_\gamma.r - a_\rho.r)_{\gamma < \Omega}$ est stationnaire à partir d'un certain rang, prenant la valeur $v(x.r - a_\rho.r)$, et on a donc pour tous $\gamma > \rho$ assez grands,

$$v(m + x.r - m - a_\rho.r) = v(x.r - a_\rho.r) = v(a_\gamma.r - a_\rho.r) \geq \delta_\rho \cdot r > v(m + x.r).$$

Soit $r \in R$ et $m \in M$ comme ci-dessus, et γ tel que, pour tout $\gamma' \geq \gamma$, $v(x.r + m) = v(a_{\gamma'}.r + m)$. De plus, quitte à prendre un γ plus grand, on peut supposer $\delta_\gamma \notin \text{Saut}_M(r)$. On

a $v(a_\gamma.r + m) \leq v(a_\gamma.r - x.r)$ et, de nouveau, puisque la suite des valuations $(v(a_\gamma.r - a_\eta.r))_\eta$ est stationnaire, il existe β qu'on peut choisir $> \gamma$ tel que, pour tout $\beta' \geq \beta$, $v(a_\gamma.r - x.r) = v((a_\gamma - a_{\beta'}).r)$. Or, puisque $\beta > \gamma$, $v(a_\gamma - a_\beta) = \delta_\gamma \notin \text{Saut}_M(r)$. En particulier $a_\gamma - a_\beta$ est régulier pour r , donc $v(a_\gamma.r - x.r) = v((a_\gamma - a_\beta).r) = v(a_\gamma - a_\beta).r = \delta_\gamma.r$. D'où, par le fait que la fonction $\cdot r$ est strictement croissante sur Δ , $\delta_{\gamma+1}.r > v(a_\gamma.r - x.r) \geq v(a_\gamma.r + m) = v(x.r + m)$.

Enfin, soit N et $y \in N$ comme énoncés. Si $y.r \in M$ pour un certain $r \neq 0$ alors $(a_\gamma.r)_\gamma$ converge vers $y.r$ par la remarque 4.3.10. Or ceci n'est pas possible car $(a_\gamma)_\gamma$ est supposée de type transcendant. De même, pour tout $m \in M$, $(m + a_\gamma.r)_\gamma$ converge vers $m + y.r$. Par conséquent $v(m + y.r)$ est égal à $v(m + a_\gamma.r)$ pour γ suffisamment grand. Donc $M \oplus x.R$ et $M \oplus y.R$ sont valués de la même façon. Ainsi la preuve est achevée. \blacksquare

Corollaire 4.3.17. *Soit $(M \subset N, v)$ une extension immédiate de modules valués et $y \in N \setminus M$ tel que $y.r \in M$ pour un certain $r \neq 0$. Alors y est limite d'une suite pseudo-Cauchy de M , sans limite dans M et de type affine.*

PREUVE. Par 4.3.13, y est limite d'une suite sans limite dans M . Par la proposition ci-dessus, cette suite ne peut pas être de type transcendant. \blacksquare

Proposition 4.3.18. *Soit (M, v) un module valué et $(x_\gamma)_{\gamma \in \Omega}$ une suite pseudo-Cauchy de M , de type affine et sans limite dans M . Soit $q \in R$ et $a \in M$ tels que $(v(x_\gamma.q - a))_\gamma$ est croissante à partir d'un certain rang, et q de degré minimal parmi les $r \in R$ tels que $(v(x_\gamma.r - m))_\gamma$ soit strictement croissante à partir d'un certain rang pour un certain $m \in M$. Alors q est de degré nécessairement ≥ 1 . De plus :*

1. on peut valuer le module $M(x) := (M \oplus x.R)/(x.q - a).R$ de telle façon qu'il soit une extension immédiate affine de M ;
2. soit $(M \subset N, v)$ une extension de M , et $y \in N$ une limite de la suite $(x_\gamma)_\gamma$ telle que $y.q = a$; alors $M + y.R$ est isomorphe en tant que module valué à $M(x)$, par un isomorphisme fixant M et envoyant x sur y .

PREUVE. Soit $n = \deg(q)$. Alors $n \neq 0$. Sinon en effet $q \in K \setminus \{0\}$ et $v((x_\gamma.q - a).q^{-1}) = v(x_\gamma - a.q^{-1})$, et donc $(x_\gamma)_\gamma$ converge vers $a.q^{-1}$. Contradiction.

Notons Z le sous-module $(x.q - a).R$ de $M + x.R$. Remarquons que chaque classe d'équivalence modulo Z du module $M(x)$ a un représentant canonique de la forme $x.s - m$, où s est de degré $< \deg(q)$ et $m \in M$. On définit sur $M \oplus x.R/Z$ une valuation, qu'on notera toujours v , en posant $v(x.s - m + Z) := v(x_\gamma.s - m)$ pour γ suffisamment grand. Il est facile de vérifier que $M(x)$ est un K -espace vectoriel valué.

Montrons que, si s est de degré $< \deg(q)$, alors $v((x.s - m + Z).t) = v(x.s - m + Z) \cdot t$. Si $\deg(st) < \deg(q)$, on a fini. Sinon $\deg(st) = \deg(q)$. Puisque $v(x_\gamma.st - m.t) = v(x_\gamma.s - m) \cdot t$ pour tout γ , la suite $(v(x_\gamma.st - m.t))_\gamma$ est constante à partir d'un certain rang. Écrivons st comme $q\mu + q_0$ avec $\deg(q_0) < \deg(q)$ et $\mu \in K$. Alors le représentant canonique de $x.st - m.t + Z$ est l'élément $x.q_0 - m.t + a.\mu$ et, pour γ suffisamment grand, $v(x.st - m.t) = v(x_\gamma.q_0 - m.t + a.\mu)$. On écrit $v(x_\gamma.st - m.t) = v(x_\gamma.q\mu - a.\mu + a.\mu + x_\gamma.q_0 - m.t)$. Puisque les suites $(v(x_\gamma.st - m.t))_\gamma$

et $(v(a.\mu + x_\gamma.q_0 - m.t))_\gamma$ sont constantes à partir d'un certain rang mais que $(x_\gamma.q\mu)_\gamma$ converge vers $a.\mu$, on a $v(x_\gamma.st - m.t) = v(a.\mu + x_\gamma.q_0 - m.t)$ pour γ suffisamment grand.

Enfin on montre de même manière que dans le lemme 4.3.16 que $M(x)$ est une extension immédiate de M et que, si N et y sont comme dans l'énoncé, alors $M(x)$ et $M + y.R$ sont isomorphes par un isomorphisme de modules valués fixant M envoyant la classe de x sur y . ■

On résume les résultats précédents dans le théorème suivant.

Théorème 4.3.19. *Un R -module valué (M, v) est affinement maximal (respectivement maximal) si et seulement si toute suite pseudo-Cauchy de type affine (respectivement toute suite pseudo-Cauchy) admet une limite dans M .*

On en déduit :

Corollaire 4.3.20. *Soit (F, v) un corps valué de caractéristique $p > 0$. Alors, (F, v) est un $F[t; x \mapsto x^p]$ -module valué affinement maximal (respectivement maximal) si, et seulement si, le corps valué (F, v) est algébriquement maximal (respectivement maximal). En particulier toute extension algébrique, immédiate, et algébriquement maximale du corps (F, v) est une extension affine, immédiate et affinement maximale du module valué (F, v) .*

PREUVE. Si (F, v) n'est pas algébriquement maximal (respectivement n'est pas maximal) alors il existe un corps (L, v) , qui est une extension algébrique immédiate propre de (F, v) (respectivement une extension immédiate propre de (F, v)). Or (F, v) et (L, v) sont munis canoniquement d'une structure de $F[t; x \mapsto x^p]$ -module valué, et (L, v) est une extension immédiate propre de (F, v) comme module valué. De plus, si L est algébrique sur F , alors l'extension de module $F \subset L$ est affine par le fait tout polynôme de $F[X]$ divise (dans l'anneau $F[X]$) un polynôme additif.

Réciproquement, si (F, v) est algébriquement maximal, alors, toute suite pseudo-Cauchy de type algébrique admet une limite dans F . Puisque toute suite de type affine est en particulier de type algébrique, (F, v) est affinement maximal. ■

Proposition 4.3.21. *Tout module valué a une extension immédiate maximale et une extension immédiate affine, affinement maximale.*

PREUVE. Par les propositions 4.3.16 et 4.3.18 tout module valué non maximal admet des extensions immédiates propres. On utilisera le lemme de Zorn. Pour cela on doit montrer que la cardinalité d'une extension immédiate est bornée par la cardinalité du module valué considéré.

Soit (M, v) un module valué, κ un cardinal majorant strictement les cardinaux de $M_{\geq \gamma}/M_{> \gamma}$ pour tout $\gamma \in v(M)$ et (M', v) une extension immédiate de (M, v) . Soit $k \in \kappa$ et N l'ensemble des fonctions $f : v(M) \setminus \{\infty\} \rightarrow \kappa$ tel que $\{\gamma \mid f(\gamma) \neq k\}$ est bien ordonné. On munit N de la distance ultramétrique d définie par $d(f, g) := \min\{\gamma \mid f(\gamma) \neq g(\gamma)\}$, où on convient que

$\min \emptyset = \infty$. Il est bien connu (et facile de vérifier) qu'un tel espace ultramétrique est maximal. On va montrer que (M', v) se plonge dans (N, d) .

Soit λ le cardinal de M' . Énumérons les éléments de M' comme $\{m_\alpha \mid \alpha < \lambda\}$. Si $\rho < \lambda$, posons $M_\rho = \{m_\alpha \mid \alpha < \rho\}$. Il suffit de montrer que si l'espace ultramétrique M_ρ muni de la distance induite par v se plonge dans (N, d) alors on peut étendre ce plongement en un plongement de $M_{\rho+1}$ dans N . Soit $\rho < \lambda$. Supposons qu'on a un tel plongement, disons $f : M_\rho \rightarrow N$. On considère deux cas : ou bien l'ensemble $\{v(m_\alpha - m_{\rho+1}) \mid \alpha < \rho + 1\}$ a un plus grand élément et dans ce cas c'est un élément de $v(M)$ différent de ∞ , ou bien il n'en a pas. Si on est dans le premier cas, prenons $\alpha_0 < \rho + 1$ tel que $\max\{v(m_\alpha - m_{\rho+1}) \mid \alpha < \rho + 1\} = v(m_{\alpha_0} - m_{\rho+1})$ et désignons cette valeur par γ . Puisque $|M_{\geq \gamma}/M_{> \gamma}| < |N_{\geq \gamma}/N_{> \gamma}|$ il existe $h \in N \setminus f(M_\rho)$ tel que $d(h, f(m_{\alpha_0})) = \gamma$. Alors on envoie $m_{\rho+1}$ sur h . Si on est dans le second cas, par le fait que (N, d) est maximal, il existe $g \in N \setminus f(M_\rho)$ tel que pour tout $\alpha < \rho + 1$, $d(f(m_\alpha), g) = v(m_\alpha - m_{\rho+1})$. Alors on envoie $m_{\rho+1}$ sur g . Dans le deux cas il est immédiat de vérifier que la correspondance suggérée prolonge f sur $M_{\rho+1}$.

On a montré que les cardinaux des extensions immédiates de (M, v) sont tous bornés par celui de N . Alors on applique le lemme de Zorn : puisqu'une union croissante d'extensions immédiates (respectivement immédiates affines) de (M, v) est une extension immédiate (respectivement immédiate affine) de (M, v) , par le lemme de Zorn, il existe une extension immédiate de (M, v) (respectivement une extension immédiate affine de (M, v)) qui est maximale parmi les extensions immédiates (respectivement parmi les extensions immédiates affines) pour l'ordre d'inclusion ; notons-la (\overline{M}, v) . Alors (\overline{M}, v) est maximal (respectivement affinement maximal) car il a sinon une extension immédiate (respectivement une extension affine et immédiate) et celle-ci est une extension immédiate (respectivement affine et immédiate) de (M, v) par le fait que la relation « être une extension immédiate » est transitive (respectivement les relations « être une extension immédiate » et « être une extension affine » sont transitives). \blacksquare

L'extension immédiate affine affinement maximale d'un module valué n'est en général pas unique, comme le montre l'exemple ci-dessous.

Exemple 4.3.22. Soit K le corps des séries de Puiseux sur le corps \mathbb{F}_p , en la variable ξ . On le considère comme module valué sur son anneau de polynômes additifs. Le polynôme $Q(X) = X^p - X - \xi^{-1}$ n'a pas de solution dans K et il est bien connu qu'il existe des extensions L_1, L_2 de K , algébriques, immédiates, et algébriquement maximales, telles que L_1 contient une racine de Q et L_2 n'en contient pas. En particulier L_1 et L_2 ne peuvent être isomorphes au dessus de K comme corps. En fait, dans ce langage de modules on peut dire plus :

Théorème 4.3.23. Soit K, L_1 et L_2 comme dans l'exemple ci-dessus. Alors L_1 et L_2 ne sont pas élémentairement équivalents en tant que $K[t; x \mapsto x^p]$ -modules.

PREUVE. Soit L une extension (de corps) de K . On va montrer que Q a une racine dans L si et seulement si il existe $x \in L$ tel que $x.(t-1)\xi(t-1) = 0$ et $x.(t-1) \neq 0$; ceci s'exprime dans le langage des modules et donc l'assertion en découle.

Supposons $\zeta \in L$ tel que $Q(\zeta) = 0$. Alors, $\zeta^p - \zeta = \xi^{-1}$ et $(\zeta^p - \zeta)\xi = 1 \in \mathbb{F}_p$; donc $(\zeta^p - \zeta)\xi$ est une racine de $X^p - X$. Réciproquement, si pour un $x \in L$, $x \cdot (t-1) \neq 0$ (i.e. $x \notin \mathbb{F}_p$) et $x \cdot (t-1)\xi(t-1) = 0$, alors $x \cdot (t-1)\xi \in \mathbb{F}_p \setminus \{0\}$. Posons $a = x \cdot (t-1)\xi = (x^p - x)\xi$. Donc $x^p/a - x/a - \xi^{-1} = 0$ et puisque $a \in \mathbb{F}_p \setminus \{0\}$, $Q(x/a) = 0$. \blacksquare

4.4 Modules valués henséliens

Définition 4.4.1. Soit Δ une R -chaîne et $r = \sum_{i \in I} t^i a_i \in R \setminus \{0\}$ avec $a_i \neq 0$ pour chaque $i \in I$. On écrit $J(r) = \{j_0, \dots, j_k\}$, avec $j_0 < j_1 < \dots < j_k$ (cf. 4.1.11 pour les définitions de $J(r)$ et des $U_j(r)$). Si $j_0 = \min I$, on note $H_v(r)$ l'ensemble L_V -définissable

$$(U_{j_0}(r) \setminus U_{j_1}(r)) \setminus \{\infty\},$$

i.e. $H_v(r) = U_{j_0}(r) \setminus \{\infty\}$ s'il n'existe pas de γ vérifiant $\tau^{j_0}(\gamma) \cdot a_{j_0} = \tau^{j_1}(\gamma) \cdot a_{j_1}$, et sinon, si γ est l'unique élément de $U_{j_0}(r) \cap U_{j_1}(r)$, alors $H_v(r) = U_{j_0}(r) \setminus \{\gamma, \infty\}$; par le lemme 4.1.11 $H_v(r)$ est un segment final; on appelle marge hensélienne de r l'ensemble $\tau^{j_0}(H_v(r)) \cdot a_{j_0}$ et on le note $Hens_v(r)$. Enfin, si $j_0 > \min I$, on pose $H_v(r) = Hens_v(r) = \emptyset$.

Remarque 4.4.2. Soit Δ une R -chaîne, $\gamma \in \Delta \setminus \{\infty\}$ et $r = t^n a_n + \dots + t^k a_k \in R \setminus \{0\}$ avec k le minimum des exposants en t et $a_k \neq 0$. Alors, $\gamma \in H_v(r)$ si et seulement si $\gamma \cdot t^k a_k < \gamma \cdot (r - t^k a_k)$.

Exemple 4.4.3. Soit $r = \sum_{i=0}^n t^i a_i$, séparable. Écrivons $J(r) = \{j_0, \dots, j_k\}$, avec $j_0 < \dots < j_k$. Si $j_0 = 0$ alors

$$Hens_v(r) = H_v(r) \cdot a_0 = \{\gamma \in \Delta \mid \tau^{j_1}(\gamma) \cdot a_{j_1} > \gamma \cdot a_0\} \cdot a_0,$$

donc, $Hens_v(r)$ est aussi un segment final de Δ .

Définition 4.4.4. Soit (M, v) un module valué et $\Delta := v(M)$. On pose :

$Hens_M(r) := \{x \in M \setminus \{0\} \mid v(x) \in Hens_v(r)\}$ et

$H_M(r) := \{x \in M \setminus \{0\} \mid v(x) \in H_v(r)\}$.

Noter que si $U_{j_0}(r) \cap U_{j_1}(r)$ est un singleton $\{\gamma\}$ alors $H_M(r)$ est la boule ouverte $M_{>\gamma}$.

Remarque 4.4.5. Si $x \in H_M(r)$ alors $v(x)$ est strictement plus grande que tous les sauts de r dans M , en particulier x est régulier pour r .

Lemme 4.4.6. Soit (M, v) un module valué et $r \in R$ séparable tel que $H_v(r) \neq \emptyset$. Alors, pour tous $a, b \in K \setminus \{0\}$, on a :

1. $H_v(ra) = H_v(r)$ et $Hens_v(ra) = Hens_v(r) \cdot a$,
2. $Hens_v(br) = Hens_v(r)$ et $H_v(br) = H_v(r) \cdot b^{-1}$,
3. $Hens_v(tr) = Hens_v(r)$ et $H_v(tr) = H_v(r) \cdot t$.

On a aussi les égalités analogues avec H_M (respectivement $Hens_M$) au lieu de H_v (respectivement $Hens_v$).

PREUVE. Écrivons $r = t^n c_n + \dots + c_0$, avec $c_0 \neq 0$. Soit $\gamma \in v(M) \setminus \{\infty\}$. Alors :

1. $\gamma \in H_v(ra) \Leftrightarrow \gamma \cdot c_0 a < \gamma \cdot (ra - c_0 a) \Leftrightarrow \gamma \cdot c_0 < \gamma \cdot (r - c_0) \Leftrightarrow \gamma \in H_v(r)$, i.e. $H_v(r) = H_v(ra)$.

Or $Hens_v(r) = H_v(r) \cdot c_0$ et $Hens_v(ra) = H_v(ra) \cdot c_0 a$. Il vient $Hens_v(ra) = Hens_v(r) \cdot a$.

2. $\gamma \in H_v(br) \Leftrightarrow \gamma \cdot bc_0 < \gamma \cdot (br - bc_0) \Leftrightarrow (\gamma \cdot b) \cdot c_0 < (\gamma \cdot b)(r - c_0) \Leftrightarrow \gamma \cdot b \in H_v(r) \Leftrightarrow \gamma \in H_v(r) \cdot b^{-1}$. Alors $Hens_v(br) = H_v(br) \cdot bc_0 = H_v(r) \cdot c_0 = Hens_v(r)$.

3. $\gamma \in H_v(tr) \Leftrightarrow \gamma \cdot tc_0 < \gamma \cdot (tr - tc_0) \Leftrightarrow (\gamma \cdot t) \cdot c_0 < (\gamma \cdot t)(r - c_0) \Leftrightarrow \gamma \cdot t \in H_v(r)$. Alors $Hens_v(tr) = H_v(tr) \cdot tc_0 = H_v(r) \cdot c_0 = Hens_v(r)$. \blacksquare

On va considérer un schéma d'axiome de Hensel analogue au cas de l'action triviale de K sur Δ . On l'énonce comme ci-dessous, pour tout polynôme unitaire séparable $r = t^n + \dots + ta_1 + a_0$ à coefficients dans \mathcal{O}_K ,

$$7. \forall z \ z \in Hens(r) \longrightarrow \exists y \ y.r = z \wedge v(z) = v(y) \cdot r = v(y) \cdot a_0,$$

Théorème 4.4.7 (Inversion locale). *Un module valué (M, v) vérifie les axiomes 7 si et seulement si pour tout $r \in R$, séparable unitaire à coefficients dans \mathcal{O}_K la fonction $x \mapsto x.r$ induit une bijection de $H_M(r)$ vers $Hens_M(r)$.*

PREUVE. Si la fonction $x \mapsto x.r$ induit une bijection de $H_M(r)$ vers $Hens_M(r)$ alors pour tout $y \in Hens_M(r)$ il existe $x \in H_M(r)$ tel que $x.r = y$, et, puisque $x \in H_M(r)$, x est régulier pour r et $v(x.r) = v(x) \cdot a_0$. Réciproquement, il suffit de voir que la restriction de r à $H_M(r)$ est injective. Par définition de $H_M(r)$, $H_v(r) \cap Saut_M(r) = \emptyset$. Ceci implique en particulier que $ann_M(r) \cap H_M(r) = 0$. D'où le résultat. \blacksquare

Remarque 4.4.8. Si (M, v) est hensélien alors il en va de même pour le sous-module (M_{tor}, v) .

Définition 4.4.9. On appellera hensélien un module valué vérifiant le schéma d'axiomes 7.

Remarque 4.4.10. Un module K -trivialement valué hensélien au sens du chapitre 7 vérifie est hensélien.

Lemme 4.4.11. *Soit (L, v) un corps valué hensélien de caractéristique $p > 0$. Alors (L, v) , comme module valué sur $L[t, x \mapsto x^p]$, est hensélien.*

PREUVE. Soit $z \in L \setminus \{0\}$ et $P(X) = \sum_{i=0, \dots, n} a_i X^{p^i}$, avec $a_n = 1$ et $v(a_i) \geq 0$. On considère le polynôme $F(X) = P(X) - z$. Pour $i > 0$ on définit γ_i dans la clôture divisible de $v(L)$ comme $\frac{v(a_0) - v(a_i)}{p^i - 1}$ et on pose $\gamma = \max\{\gamma_i\}$. Puisque P est unitaire, $\gamma \geq 0$. Remarquons que, pour tout $x \in L$ tel que $v(x) > \gamma$, $v(x) + v(a_0) < p^i v(x) + v(a_i)$ et donc $v(P(x)) = v(x) + v(a_0)$. Alors $Hens_v(P) = \{\delta \in L \mid \gamma + v(a_0)\}$ (on fait un abus de langage en désignant encore par P l'élément $\sum_{i=0, \dots, n} t^i a_i \in L[t, x \mapsto x^p]$). Supposons maintenant que $v(z) > \gamma + v(a_0)$ et considérons $G(X) := F(Xz a_0^{-1})/z$. Alors,

$$G(X) = \frac{z^{(p^n - 1)}}{a_0^{p^n}} X^{p^n} + \dots + \frac{z^{(p^i - 1)}}{a_0^{p^i}} a_i X^{p^i} + \dots + X - 1.$$

Or, par la définition de γ_i , pour tout i , $(p^i - 1)(\gamma_i + v(a_0)) + v(a_i) - p^i v(a_0) = 0$. Donc $v(z) > \gamma + v(a_0)$ implique pour tout $i > 1$,

$$v\left(\frac{z^{(p^i - 1)}}{a_0^{p^i}} a_i\right) > 0.$$

Par conséquent $v(G(1)) > v(G'(1)) = v(1) = 0$. En appliquant le lemme de Hensel à G on obtient $y \in L$ tel que $v(y-1) > v(y)$ et $G(y) = 0$. Donc y est de valuation 0 et $P(yza_0^{-1}) = z$. Puisque $v(z) > \gamma + v(a_0)$, $y' := yza_0^{-1}$ est de valuation $> \gamma$, i.e. $y' \in H_L(P)$. Ce qui fallait montrer. \blacksquare

A partir de maintenant, on suppose que si la valuation v_K induite sur K par son action sur la chaîne considérée est non triviale alors on a $x \in \mathcal{O}_K$,

$$v_K(\varphi(x)) \geq 2v_K(x).$$

Lemme 4.4.12. *Soit (M, v) un module valué. Alors les assertions suivantes sont équivalentes :*

1. (M, v) est henselien,
2. pour tout $r \in R_{sep}$, l'application $x \mapsto x.r$ est une bijection de $H_M(r)$ sur $Hens_M(r)$,
3. pour tout $r = \sum_{i=0}^n t^i a_i \in R_{sep}$ tel que $a_0 = 1$ l'application $x \mapsto x.r$ est une bijection de $H_M(r)$ sur $H_M(r)$.

Si de plus M est t -divisible alors, (M, v) est henselien si et seulement si, pour tout $r \in R \setminus \{0\}$, l'application $x \mapsto x.r$ est une bijection de $H_M(r)$ sur $Hens_M(r)$.

PREUVE. [1 \Rightarrow 2]. Soit $s \in R$ un polynôme séparable que l'on écrit comme $s = t^k a_k + \dots + a_0$. On peut supposer que $s \in R_{\mathcal{O}}$. En effet, soit $a \in K$ tel que $sa \in R_{\mathcal{O}}$. Soit $z \in Hens_M(s)$. Alors $za \in Hens_M(sa)$ par le lemme 4.4.6, et si $y \in H_M(sa)$ est tel que $y.ra = za$, alors $y \in H_M(s)$, toujours par le lemme 4.4.6. Donc $y.s = z$. Supposons donc que $s \in R_{\mathcal{O}}$.

Soit $\mu_i := \varphi^k(a_k)/\varphi^{k-i}(a_k)a_k$ si $1 \leq i \leq k-1$, et $\mu_k := \varphi(a_k)/a_k$. Alors $v_K(\mu_i) \geq 0$ car $v_K(\varphi(x)) \geq 2v_K(\varphi(x))$ d'après notre hypothèse sur (K, v_K) . On considère le polynôme $s' := s\mu_k$. On a :

$$s' = a_k t^k + a_k t^{k-1} a_{k-1} \mu_1 + \dots + a_k t a_1 \mu_{k-1} + a_0 \mu_k.$$

Soit $s_u = a_k^{-1} s'$. Donc le polynôme s_u est unitaire à coefficients dans $R_{\mathcal{O}}$ et par le lemme 4.4.6 $Hens_v(s) = Hens_v(s') \cdot \mu_k^{-1} = Hens_v(s_u) \cdot \mu_k^{-1}$. Donc si $z \in Hens_M(s)$ alors $z \cdot \mu_k \in Hens_M(s_u)$. Par suite il existe $y \in H_M(s_u)$ vérifiant $y.s_u = z \cdot \mu_k$. Dans ce cas, $x = y \cdot a_k^{-1} \in H_M(s)$ vérifie $x.s' = z \cdot \mu_k$ et donc $x.s = z$.

[2 \Rightarrow 3]. Évident en constatant que les hypothèses de 3 impliquent $H_M(r) = Hens_M(r)$.

[3 \Rightarrow 1]. Soit $r = t^n a_n + \dots + a_0$ unitaire à coefficients dans \mathcal{O}_K . En considérant $r' = ra_0^{-1}$ et en raisonnant exactement de même manière que dans le premier paragraphe de la partie [1 \Rightarrow 2], on établit le résultat voulu.

Maintenant supposons que (M, v) est t -divisible et henselien. Soit $r \in R_{\mathcal{O}}$ non nécessairement séparable que l'on écrit comme $t^n s$ avec s séparable. Par le lemme 4.4.6 on a $Hens_M(s) = Hens_M(r)$. Maintenant, si $z \in Hens_M(r)$ alors $z \in Hens_M(s)$ et par conséquent il existe un unique $y \in H_M(s)$ tel que $y.s = z$. Alors l'unique $x \in M$ tel que $x.t^n = y$ vérifie l'assertion. \blacksquare

Si (M, v) un module valué, on appellera équation hensélienne sur M , une équation en l'indéterminée x , de la forme $x.r = a$, où $r \in R_{sep}$ et $a \in Hens_M(r)$. Le lemme suivant montre qu'il existe toujours des solutions aux équations henséliennes sur M dans une extension immédiate affine de (M, v) .

Lemme 4.4.13. *Soit (A, v) un module valué, $r \in R_{O,sep}$ unitaire et $y \in Hens_A(r)$. Alors il existe une extension immédiate affine (\tilde{A}, v) de A (éventuellement $\tilde{A} = A$) et $z \in H_{\tilde{A}}(r)$ tel que $z.r = y$.*

PREUVE. Écrivons $r = t^n a_n + \dots + t^k a_k + a_0$ avec $a_0 a_k \dots a_n \neq 0$. Par le lemme 4.4.6, on peut supposer que $a_0 = 1$, donc $Hens_A(r) = H_A(r)$. On définit alors une suite $(c_n)_{n < \omega}$ de A en posant $c_0 = 0$, $c_1 = y$ et $c_{n+1} = c_n - (c_n.r - y)$. Remarquons que comme $y \in H_A(r)$, par induction, $c_n \in H_A(r)$ pour $n \geq 1$. On a $c_2 - c_1 = -(y.r - y) = y.(1 - r)$. Puisque $y \in H_A(r)$, $v(y.(r - 1)) > v(y) = v(c_1 - c_0)$. Soit $n \geq 2$. On a $c_{n+1} - c_n = y - c_{n-1}.r - (c_n - c_{n-1}).r$. Or, $y - c_{n-1}.r = (c_n - c_{n-1})$. Donc $c_{n+1} - c_n = (c_n - c_{n-1}).(1 - r)$; puisque $c_n - c_{n+1} \in H_A(r)$ on a $v((c_n - c_{n-1}).(1 - r)) > v(c_n - c_{n-1})$ par la remarque 4.4.2 (en fait on a montré par induction que $c_{n+1} - c_n = y.(1 - r)^n$). Donc la suite $(c_n)_n$ est pseudo-Cauchy et la suite $(c_n.r)_n$ converge vers y . En particulier la suite $(c_n)_n$ est de type affine.

Il est immédiat de vérifier que, si A contient un élément z tel que $z.r = y$ avec $z \in H_A(r)$, alors nécessairement z est limite de la suite $(c_n)_n$. En effet, on a $v(y - c_n.r) = v((z - c_n).r)$. Puisque pour tout $n < \omega$ on a $z, c_n \in H_A(r)$, $z - c_n$ est régulier pour r . Il vient : $v((z - c_n).r) = v(z - c_n) \cdot r = v(z - c_n)$. Donc $(c_n)_n$ converge vers z .

Soit $\alpha \geq \omega$ un ordinal limite. Supposons qu'on a défini $c_\beta \in A$ pour tout $\beta < \alpha$, de telle façon que la suite $(c_\beta)_{\beta < \alpha}$ soit une suite pseudo-Cauchy et que la suite $(c_\beta.r)_{\beta < \alpha}$ converge vers y . Supposons qu'il existe $z \in A$ limite de la suite $(c_\beta)_{\beta < \alpha}$. Si $z.r = y$ alors on a fini. Sinon, on pose $c_\alpha := z$. Alors $(c_\beta.r)_{\beta < \alpha}$ converge vers $c_\alpha.r$. Par conséquent $v(y - c_\alpha.r) > v(y - c_\beta.r)$ pour tout $\beta < \alpha$. Alors, en définissant par induction $c_{\alpha+n}$, pour $n \in \omega$, par l'équation

$$c_{\alpha+n+1} - c_{\alpha+n} = y - c_{\alpha+n}.r,$$

on obtient une suite pseudo-Cauchy de longueur $\eta = \alpha + \omega$ telle que $(c_\gamma.r)_{\gamma < \eta}$ converge vers y . Ainsi, si on n'a pas trouvé $z \in A$ comme voulu (vérifiant $z.r = y$ et $z \in H_A(r)$), on obtient une suite $(c_\beta)_{\beta < \lambda}$ sans limite dans A et telle que $(c_\beta.r)_{\beta < \lambda}$ converge vers y . Soit $a \in A$ et $q \in R$ tels que la suite $(v(c_\beta.q - a))_{\beta < \lambda}$ est strictement croissante à partir d'un certain rang et q de degré minimal tel que la suite $(c_\beta.q)_\beta$ ait une limite dans A . Par la proposition 4.3.18 il existe une extension immédiate affine A' de A , contenant une limite c_λ de la suite $(c_\beta)_\beta$ vérifiant $c_\lambda.q = a$. Le type d'isomorphisme du module valué $A' = A + c_\lambda.R$ est uniquement déterminé par q et la suite $(c_\beta)_{\beta < \lambda}$. S'il existe $z \in H_{A'}(r)$ tel que $z.r = y$ alors on a fini. Sinon, puisque la suite $(c_\beta.r)_\beta$ converge vers y , on peut définir, par la même formule ci-dessus, une suite pseudo-Cauchy $(c_{\lambda+n})_{n < \omega}$ de A' telle que $(c_{\lambda+n}.r)_{n < \omega}$ converge vers y . En continuant ainsi, puisque la cardinalité de toute extension immédiate est bornée en fonction de la cardinalité de A , on doit finir par trouver z dans une extension immédiate affine \tilde{A} de A , qui vérifie $z.r = y$ et $z \in H_{\tilde{A}}(r)$. ▮

Le lemme ci-dessus nous donne immédiatement le résultat suivant :

Corollaire 4.4.14. *Un module valué affinement maximal est henselien.*

À partir de maintenant on commence à analyser les liens entre points irréguliers et axiomes de Hensel.

Définition 4.4.15. Soit (M, v) un module valué et $r = \sum_{i=0}^n t^i a_i \in R \setminus \{0\}$. Pour $\gamma \in \text{Saut}_M(r)$, on pose

$$I_\gamma = \{i \in \{0, \dots, n\} \mid \tau^i(\gamma) \cdot a_i = \gamma \cdot r\}, \quad k_\gamma = \min I_\gamma \quad \text{et} \quad r_\gamma = \sum_{i \in I_\gamma} t^i a_i.$$

Remarque 4.4.16. Soit $0 \neq r = \sum_{i \in I} t^i a_i \in R$ avec $a_i \neq 0$ et $I = \{i_0, \dots, i_s\}$ ($i_0 < \dots < i_s$). Supposons que $\emptyset \neq \text{Saut}_M(r) = \{\gamma_0, \dots, \gamma_l\}$ avec $\gamma_j < \gamma_{j+1}$. Alors $r_{\gamma_0} = t^{i_s} a_{i_s} + \dots + t^{k_{\gamma_0}} a_{k_{\gamma_0}}$, $r_{\gamma_l} = t^n a_n + \dots + t^{i_0} a_{i_0}$ (i.e. $k_{\gamma_l} = i_0$), et pour tout j vérifiant $0 < j < l$, $r_{\gamma_j} = t^{k'_{j-1}} a_{k'_{j-1}} + \dots + t^{i_{s'}} a_{i_{s'}}$ où $0 < s' < s$ et $k'_{j-1} \leq k_{\gamma_{j-1}}$ avec égalité si et seulement si,

$$\tau^{i_n}(\gamma_j) \cdot a_{i_n} = \tau^{i_n-1}(\gamma_j) \cdot a_{i_n-1},$$

où $i_n = k_{\gamma_{j-1}}$.

Exemple 4.4.17. Soit r de degré 3, que l'on écrit comme $t^3 a_3 + \dots + a_0$. Alors $|\text{Saut}_M(r)| \leq 3$. Si $\text{Saut}_M(r) = \{\gamma_1, \gamma_2\}$ ($\gamma_1 < \gamma_2$) alors les possibilités pour r_{γ_1} et r_{γ_2} sont

$$\begin{cases} r_{\gamma_1} = t^3 a_3 + t^2 a_2, \quad \text{et} \quad r_{\gamma_2} = t^2 a_2 + t a_1 + a_0 \quad \text{ou la somme de deux de ces monômes, ou bien} \\ r_{\gamma_1} = t^3 a_3 + t^2 a_2 + t a_1 \quad \text{ou la somme de deux de ces monômes, et} \quad r_{\gamma_2} = t a_1 + a_0 \quad \text{ou bien} \\ r_{\gamma_1} = t^3 a_3 + t^2 a_2 \quad \text{et} \quad r_{\gamma_2} = t a_1 + a_0. \end{cases} \quad (*)$$

Si $\text{Saut}_M(r) = \{\gamma\}$ alors $r_\gamma = r$ ou n'importe quelle somme d'au moins deux de ses monômes. Enfin si $\text{Saut}_M(r) = \{\gamma_1, \gamma_2, \gamma_3\}$ la seule possibilité est que $r_{\gamma_1} = t^3 a_3 + t^2 a_2$, $r_{\gamma_2} = t^2 a_2 + t a_1$ et $r_{\gamma_3} = t a_1 + a_0$.

Notons qu'il se peut qu'on ait une égalité $\gamma \cdot t^i a_i = \gamma \cdot t^j a_j$ pour des monômes distincts $t^i a_i$ et $t^j a_j$ de r mais sans que cette valeur γ soit un saut.

Lemme 4.4.18. *Soit (M, v) un module valué, $r = \sum_{i=0}^n t^i a_i \in R \setminus \{0\}$ et $\gamma \in \text{Saut}_M(r)$. Alors un $x \in M$ de valuation γ est irrégulier pour r si, et seulement si, il l'est pour r_γ . De plus, si $x \cdot r_\gamma \neq 0$ et si (M, v) est t -divisible et henselien, il existe un unique $x_{>\gamma} \in M$ de valuation $> \gamma$ tel que $x - x_{>\gamma}$ est une racine de r_γ .*

PREUVE. Soit x de valuation γ . Puisque r réalise un saut au point γ , I_γ a nécessairement au moins 2 éléments, et r_γ a au plus un seul point de saut dans $v(M)$, à savoir γ . D'autre part, par définition de r_γ , on a $\gamma \cdot (r - r_\gamma) > \gamma \cdot r_\gamma$ et $\gamma \cdot r_\gamma = \gamma \cdot r$. En conséquence si x est irrégulier pour r_γ alors on a $v(x \cdot r) = v(x \cdot r_\gamma + x \cdot (r - r_\gamma)) > \gamma \cdot r_\gamma$. D'où x est irrégulier pour r . Réciproquement, si x est régulier pour r_γ , on a $v(x \cdot r) = v(x \cdot (r - r_\gamma) + x \cdot r_\gamma) = v(x \cdot r_\gamma) = v(x) \cdot r_\gamma = v(x) \cdot r$, i.e. x est régulier pour r .

Donc γ est un saut de r_γ et par conséquent c'est l'unique saut de r_γ . De plus, la définition de r_γ implique que $H_M(r_\gamma) = M_{>\gamma}$ et $\text{Hens}_M(r_\gamma) = M_{>\gamma \cdot r_\gamma}$. D'où $x \cdot r_\gamma \in \text{Hens}_M(r_\gamma)$ ou bien $x \cdot r_\gamma = 0$.

Supposons maintenant (M, v) t -divisible et hensélien et $x.r_\gamma \in Hens_M(r_\gamma)$. Soit $x_{>\gamma}$ l'unique élément de $H_M(r_\gamma)$ tel que $x_{>\gamma}.r_\gamma = x.r_\gamma$ dont l'existence est justifiée par le lemme 4.4.12. Alors $x - x_{>\gamma} \in \text{ann}_M(r_\gamma)$ comme voulu. \blacksquare

Remarque 4.4.19. Soit $\gamma \in \text{Saut}_M(r)$; si $r_\gamma \neq r$ alors $\text{ann}_M(r_\gamma) \cap \text{ann}_M(r) = 0$.

PREUVE. Si $x.r = 0$ et $x.r_\gamma = 0$, on a nécessairement $x.(r - r_\gamma) = 0$. Or par définition de r_γ , si $r - r_\gamma \neq 0$ alors $\gamma \notin \text{Saut}_M(r - r_\gamma)$; en particulier si $v(x) = \gamma$, x ne peut annuler $r - r_\gamma$. Or $\text{Saut}_M(r_\gamma) \subset \{\gamma\}$, donc un zéro non nul de r_γ est nécessairement de valuation γ . \blacksquare

Corollaire 4.4.20. *Soit (M, v) t -divisible et hensélien. Alors, pour tout $r \in R \setminus \{0\}$, si $x \in \text{ann}_M(r) \setminus \{0\}$, il existe un unique $x' \in \text{ann}_M(r_\gamma)$ tel que $v(x - x') > v(x)$ et $x - x'$ est régulier pour r . En particulier, si N est le sous-module de M engendré par les racines des polynômes n'ayant qu'un seul saut dans M , alors l'extension $(N \subset M_{\text{tor}}, v)$ est immédiate.*

PREUVE. Si $r_\gamma = r$ on prend $x' := x$. Sinon par la remarque précédente $x.r_\gamma \neq 0$ et par le lemme 4.4.18 on obtient l'existence d'un tel x' comme énoncé. Le fait que M_{tor} est une extension immédiate de N suit trivialement.

Il suffit alors de montrer que $x - x'$ est régulier pour r . Soit $\gamma = v(x)$. Le résultat est évident si $\gamma = \max \text{Saut}_M(r)$. Supposons que ce n'est pas le cas. On a $v(x.r_\gamma) = v(r(x - x').r_\gamma) = v(x.(r - r_\gamma))$. Or x est régulier pour $r - r_\gamma$ et $x - x'$ est régulier pour r_γ . Notons $r := r_\gamma + r'$ et γ_s le successeur de γ dans $\text{Saut}_M(r)$. Par l'équation $x.(-r_\gamma) = x.r'$, on a $v(x.r') = v(x) \cdot r' = \gamma \cdot r' = v((x - x').r_\gamma) = v(x - x') \cdot r_\gamma < \gamma_s \cdot r' \leq \gamma_s \cdot r_\gamma$. Par conséquent $v(x - x') \in]\gamma, \gamma_s[$ et $x - x'$ est régulier. \blacksquare

La proposition suivante et son corollaire établissent en effet la conclusion que l'on veut avoir pour les modules affinement maximaux.

Proposition 4.4.21. *Supposons que (M, v) est hensélien et t -divisible. Rappelons que $K_0 = \text{Fix}(\varphi)$. Soit $r \in R \setminus \{0\}$. Alors il existe une K_0 -base $\mathcal{B} = \bigcup_{\gamma \in \text{Saut}_M(r)} b_\gamma$ de $\text{ann}_M(r)$, où chaque b_γ est une famille valuation-indépendante d'éléments de valuation γ , et donc \mathcal{B} est valuation-indépendante. De plus, chaque b_γ s'injecte via une application ξ_γ dans l'ensemble $\text{ann}(r_\gamma) \setminus \{0\}$. En conséquence, l'application*

$$\xi = \sum_{\gamma \in \text{Saut}_M(r)} \xi_\gamma : \text{ann}_M(r) \rightarrow \sum_{\gamma \in \text{Saut}_M(r)} \text{ann}(r_\gamma)$$

est un plongement K_0 -linéaire.

PREUVE. Pour tout $\gamma \in \Delta$, $\text{ann}_M(r)_{\geq \gamma} := \text{ann}_M(r) \cap M_{\geq \gamma} = \{x \in \text{ann}_M(r) \mid v(x) \geq \gamma\}$ (ou de même $\text{ann}_{>\gamma}(r) := \{x \in \text{ann}_M(r) \mid v(x) > \gamma\}$) est un sous-espace vectoriel de $\text{ann}_M(r)$. On va construire par induction une base valuation-indépendante \mathcal{B} de $\text{ann}_M(r)$. On définit b_{γ_r} (rappelons que $\gamma_r = \max \text{Saut}_M(r)$) comme étant une base de $\text{ann}_M(r)_{\geq \gamma_r}$. Cette base est nécessairement valuation-indépendante car, comme dans la preuve de 4.4.18, si $x \neq y \in \text{ann}_M(r)_{\geq \gamma_r}$, alors $v(x - y) = \gamma_r$. Soit $\gamma \in \text{Saut}_M(r)$; supposons que l'on ait défini, pour

chaque $\delta \in \text{Saut}_M(r)$ vérifiant $\gamma < \delta$, un sous-ensemble valuation-indépendant b_δ de M tel que $\bigcup_{\delta > \gamma} b_\delta$ est une base valuation-indépendante de $\text{ann}_M(r)_{>\gamma}$. On définit b_γ en prenant une base d'un supplémentaire de $\text{ann}_M(r)_{>\gamma}$ dans $\text{ann}_M(r)_{\geq \gamma}$.

Soit $y \in b_\gamma$. Par 4.4.20, il existe un et un seul $y_0 \in \text{ann}(r_\gamma)$ tel que $v(y - y_0) > v(y)$. On pose alors $\xi_\gamma(y) = y_0$. Puisque b_γ est une famille valuation-indépendante, pour tous $y' \in b_\gamma \setminus \{0, y\}$, $y - y'$ est de valuation γ , en particulier $\xi_\gamma(y) \neq \xi_\gamma(y')$. Ceci montre l'injectivité de ξ_γ . Enfin, $\sum_\gamma \xi_\gamma$ est bien définie et est un plongement K_0 -linéaire par le procédé même définissant chaque ξ_γ . ■

Corollaire 4.4.22. *Supposons $K_0 = \text{Fix}(\varphi)$ fini de cardinalité q . Soit (M, v) un module valué t -divisible, hensélien et tel que, pour tout $s \in R$ séparable de degré n , $|\text{ann}_M(s)| = q^n$. Alors, pour tout $r \in R \setminus \{0\}$, on peut définir un isomorphisme de K_0 -espaces vectoriels $\xi_r : \text{ann}_M(r) \rightarrow \sum_{\gamma \in \text{Saut}_M(r)} \text{ann}_M(r_\gamma)$, vérifiant, pour tout $y \in \text{ann}_M(r)$, $v(\xi(y) - y) > v(y)$. En conséquence, si $x \in M$ est un élément irrégulier pour r , alors il existe $x_0 \in \text{ann}_M(r)$ tel que $x - x_0$ est régulier pour r .*

PREUVE. Soit $r \in R \setminus \{0\}$ que l'on écrit comme $\sum_{i \in I} t^i a_i$. Si r n'a qu'un seul point de saut γ alors nécessairement $r = r_\gamma$ et on a fini. En effet, pour tous monômes distincts $t^i a_i$ et $t^j a_j$ de r , le polynôme $t^i a_i + t^j a_j$ a des racines non nulles; donc $r \neq r_\gamma$ implique l'existence d'autres points de saut pour r ; de plus, quand r a plusieurs sauts, $\gamma_0 = \min \text{Saut}_M(r) < \dots < \gamma_j < \dots, \gamma_l = \max \text{Saut}_M(r)$, si $t^k a_k$ et $t^m a_m$ sont des termes consécutifs de r , alors $t^k a_k + t^m a_m$ a une racine non-nulle dans M . Ceci implique par la remarque 4.4.16 que pour tout $j \geq 1$, $\deg(r_{\gamma_j}) = k_{\gamma_{j-1}}$ (i.e. on ne peut pas avoir un cas similaire au cas (*) de l'exemple 4.4.17) et $r_{\gamma_0} = t^n a_n + \dots + t^{k_{\gamma_0}} a_{k_{\gamma_0}}$, $r_{\gamma_l} = t^{k_{l-1}} a_{k_{l-1}} + \dots + a_{k_l}$. En particulier $n = \max I$ et $k_l = \min I$.

Supposons donc que r a plusieurs sauts. Montrons d'abord que r a une racine dans M de valuation $\gamma_l = \max \text{Saut}_M(r)$. Par ce qui précède, r_{γ_l} a une racine non nulle, notons-la y_0 . Alors, par le lemme 4.4.18, y_0 est irrégulier pour r . Puisque $\gamma_l = \max \text{Saut}_M(r)$ et par les remarques faites ci-dessus, $Hens_M(r) = Hens_M(r_{\gamma_l})$. Donc $y_0.r \in Hens_M(r)$. Alors par 4.4.12, il existe un unique $y' \in H_M(r)$ tel que $y'.r = y_0.r$, i.e. $y' - y_0$ est une racine non nulle de r de valuation γ_l . Cela montre qu'on peut définir d'une manière et d'une seule une fonction K_0 -linéaire $\xi_{\gamma_l} : \text{ann}_M(r)_{\geq \gamma_l} \rightarrow \text{ann}_M(r_{\gamma_l})$ satisfaisant pour tout y , $v(\xi_{\gamma_l}(y) - y) > v(y)$. Supposons que l'on a défini ξ_{γ_j} pour tout $j, l \geq j \geq 1$, de telle façon que $\sum_{j \geq 1} \xi_{\gamma_j} : \text{ann}_M(r)_{\geq \gamma_1} \rightarrow \sum_{j \geq 1} \text{ann}_M(r_{\gamma_j})$ soit une bijection. Puisque pour chaque $j \geq 1$, $|\text{ann}_M(r_{\gamma_j})| = q^{\deg_s(r_{\gamma_j})} = q^{k_{\gamma_{j-1}} - k_{\gamma_j}}$, on a

$$|\text{ann}_M(r)_{\geq \gamma_1}| = \left| \sum_{j \geq 1} \text{ann}_M(r_{\gamma_j}) \right| = \prod_{j \geq 1} |\text{ann}_M(r_{\gamma_j})| = q^{(\sum_{j \geq 1} k_{\gamma_{j-1}} - k_{\gamma_j})} = q^{k_{\gamma_0} - k_{\gamma_l}}.$$

On a $r_{\gamma_0} = t^n a_n + \dots + t^{k_{\gamma_0}} a_{k_{\gamma_0}}$, donc r_{γ_0} a exactement $q^{n - k_{\gamma_0}}$ racines. Par ailleurs, le fait que r a exactement $q^{n - k_l}$ racines implique $\left| \frac{\text{ann}_M(r)}{\text{ann}_M(r)_{\geq \gamma_1}} \right| = q^{n - k_{\gamma_0}}$. Par conséquent $\frac{\text{ann}_M(r)}{\text{ann}_M(r)_{\geq \gamma_1}}$ et $\text{ann}_M(r_{\gamma_0})$ sont des K_0 -espaces vectoriels isomorphes. Ce qui permet d'établir la bijection voulue.

Enfin, soit x un élément irrégulier pour r . On veut montrer qu'il existe une racine x'_0 de r tel que $x - x'_0$ soit régulier pour r . Si $j = l$ l'assertion suit par henselianité de M . Supposons que, pour tout j' tel que $l \geq j' > j$, si y est de valuation $\gamma_{j'}$ et est irrégulier pour r , alors $v(y - y_0) > \gamma_{j'}$ et $y - y_0$ est régulier pour r . Par le lemme 4.4.18, x s'écrit comme $x'_0 + x_{>\gamma}$ avec $x_{>\gamma}$ de valuation $> \gamma$ et $x'_0 \in \text{ann}_M(r_{\gamma_j})$. Prenons une fonction ξ_r définie comme ci-dessus. Alors, avec $x_0 := \xi^{-1}(x'_0)$, on a $v(x - x_0) > \gamma_j$. Maintenant, ou bien $x - x_0$ est régulier pour r , ou bien il est irrégulier de valuation $\gamma_{j'}$ pour un certain $j' > j$. Dans le second cas, par induction, pour un certain $z_0 \in \text{ann}_M(r)$, $x - x_0 - z_0$ est de valuation $> \gamma_{j'}$ et est régulier pour r . D'où le résultat. \blacksquare

Remarque 4.4.23. Si (L, v) est un corps algébriquement clos non trivialement valué de caractéristique $p > 0$ et φ une puissance de Frobenius alors, pour tout sous-corps F de L , le $F[t; \varphi]$ -module valué (L, v) remplit les hypothèses du corollaire précédent.

On termine cette section par deux résultats concernant en particulier le cas des modules (ou des sous-modules) sans torsion.

Proposition 4.4.24. *Un module valué hensélien sans torsion est régulier.*

PREUVE. Soit (M, v) un module valué sans torsion. Montrons que, pour tout $x \in M$ et tout $r \in R \setminus \{0\}$, on a $v(x.r) = v(x) \cdot v(r)$. Supposons que $x \in M$ est irrégulier pour un certain r . Alors, avec $\gamma = v(x)$, x est irrégulier pour r_γ . Comme dans la preuve du lemme 4.4.18, on montre que $x.r_\gamma \in \text{Hens}_M(r_\gamma)$. Écrivons r_γ comme $t^k s_\gamma$ avec s_γ séparable. Or par le lemme 4.4.6, $\text{Hens}_M(r_\gamma) = \text{Hens}_M(s_\gamma)$. Par conséquent il existe (un unique) $x' \in H_M(s_\gamma)$ tel que $x'.s_\gamma = x.r_\gamma = (x.t^k).s_\gamma$. Donc $x' - x.t^k \in \text{ann}_M(s_\gamma)$. Par le lemme 4.4.6, $H_M(s_\gamma) = H_M(r_\gamma) \cdot t^k$. Or $H_M(r_\gamma) = M_{>\gamma}$. Il vient $v(x') > \gamma \cdot t^k = v(x.t^k)$. En particulier $x' - x.t^k \neq 0$. Contradiction. \blacksquare

Corollaire 4.4.25. *Il existe des D -espaces vectoriels valués tels que toutes ses extensions affines et affinement maximaux contiennent de la torsion. En conséquence, dans la catégorie des D -espaces vectoriels valués on n'a pas l'existence des extensions maximales.*

PREUVE. Le D -espace vectoriel K -trivialement valué, cité dans la proposition 3.2.9, est non hensélien. Donc ses extensions immédiates affines et affinement maximaux comme R -module contiennent de la torsion. \blacksquare

Remarque 4.4.26. Ce résultat va être renforcé par le corollaire 4.5.15.

Proposition 4.4.27. *Soit (M, v) un module valué hensélien et t -divisible. Alors un élément $x \in M$ régulier n'est jamais limite d'une suite pseudo-Cauchy de M_{tor} sans limite dans M_{tor} .*

PREUVE. Supposons que le contraire est témoigné par un $x \in M$. Soit $(x_\delta)_{\delta \in I}$ une suite pseudo-Cauchy de M_{tor} convergeant vers x et n'ayant pas de limite dans M_{tor} , et $(r_\delta)_{\delta \in I}$ une suite d'élément de $R \setminus 0$ tel que $x_\delta.r_\delta = 0$. Puisque x est régulier, pour tout δ , on a $v((x - x_\delta).r_\delta) = v(x.r_\delta) = v(x) \cdot v(r_\delta)$. Donc $v(x) \geq v(x - x_\delta)$ pour tout δ . Mais alors, avec le

fait que la suite $v(x - x_\delta)$ est strictement croissante, on a $v(x) > v(x - x_\delta)$ pour tout δ . Ceci implique que 0 est une limite de la suite $(x_\delta)_\delta$. Contradiction. \blacksquare

4.5 Modules valués résiduellement divisibles

Les résultats qui suivent montreront que l'on peut substituer aux hypothèses du corollaire 4.4.22 précédent, l'hypothèse que le module est affinement maximal (cf. la définition 4.3.14) et *résiduellement divisible*.

Définition 4.5.1. Un module valué (M, v) est dit résiduellement divisible si :

1. pour tout $z \in M$, il existe $y \in M$ tel que $v(z - y.t) > v(z)$
2. pour tout $r = \sum_{i \in I} t^i a_i \in R$, s'il existe (un unique) $\gamma \in \Delta$ tel que, pour tous $i, j \in I$, $\gamma \cdot t^i a_i = \gamma \cdot t^j a_j$, alors, pour tout $z \in M$ de valuation $\gamma \cdot r$, il existe $y \in M$ de valuation γ et tel que $v(z - y.r) > v(z) = \gamma \cdot r$.

Remarque 4.5.2. Les propriétés 1 et 2 sont clairement du premier ordre. La première condition implique en particulier que τ est surjectif sur $v(M)$ et que, pour tout $(m, \lambda) \in \mathbb{N} \times K$ et pour tout $z \in M$, il existe $y \in M$ tel que $v(z - y.t^m \lambda) > v(z)$. En particulier, si (M, v) est résiduellement divisible, alors pour tout $r \in R \setminus \{0\}$ l'application $\gamma \mapsto \gamma \cdot r$ est une bijection. Ce résultat sera renforcé dans le lemme 4.5.9.

Remarquer que y apparaissant dans le deuxième point de la définition ci-dessus est régulier pour r .

Lemme 4.5.3. *Si (M, v) est un module valué résiduellement divisible alors, pour tout $z \in M$ et pour tout $r \in R \setminus \{0\}$, il existe $y \in M$ régulier pour r et tel que $v(y.r - z) > v(z)$.*

PREUVE. Soit $z \in M$. Par la remarque ci-dessus, il existe $\gamma \in v(M)$ tel que $\gamma \cdot r = v(z)$. Soit $r = \sum_{i \in I} t^i a_i \in R$, $J = \{j \in I \mid \gamma \cdot t^j a_j = \gamma \cdot r\}$ et $r_J = \sum_{j \in J} t^j a_j$. On écrit $r = r' + r_J$. Alors, par la définition de r_J , on a $v(z) = \gamma \cdot r_J$. De plus, ou bien r_J est de la forme $t^j a_j$ ou bien, pour tous $j, k \in J$, $\gamma \cdot t^j a_j = \gamma \cdot t^k a_k$. Dans les deux cas, puisque M est résiduellement divisible, il existe $y \in M$ de valuation γ , tel que $v(y.r_J - z) > v(z)$. Encore par la définition de r_J , $v(y.r')r' > v(y) \cdot r_J = v(z)$. Par conséquent $v(y.(r' + r_J) - z) \geq \min\{v(y.r'), v(y.r_J - z)\} > v(z)$. \blacksquare

Remarque 4.5.4. La preuve ci-dessus montre que, si (M, v) satisfait la condition 1. de la définition 4.5.1 et la condition 2 pour les polynômes de degré $\leq n$, alors pour tout $r \in R$, de degré n , et pour tout $z \in M$, il existe $y \in M$ régulier pour r et tel que $v(y.r - z) > v(z)$.

Définition 4.5.5. Soit (K, v) un corps de valué de caractéristique $p > 0$. On dit que (K, v) est un corps de Kaplansky si

- $v(K) = pv(K)$
- le corps résiduel K_{res} de K est p -clos, i.e. K_{res} est divisible comme $K_{res}[t; x \mapsto x^p]$ -module.

Il a été montré dans [Ka] que l'extension immédiate algébrique algébriquement maximale d'un corps de Kaplansky est unique à isomorphisme près.

Proposition 4.5.6. *Soit (K, v) un corps valué de caractéristique $p > 0$, alors les assertions suivantes sont équivalentes :*

1. *Vu comme module valué sur $K[t; x \mapsto x^p]$, K est résiduellement divisible.*
2. *K est un corps de Kaplansky.*

PREUVE. $1 \Rightarrow 2$: Par la remarque 4.5.2, on a $v(K) = pv(K)$. Montrons que le corps résiduel K_{res} de K est un $K_{res}[t; x \mapsto x^p]$ -module divisible. Soit $\bar{z} \in K_{res}$ ($z \in K$) et $\bar{q} = t^n \bar{a}_n + \dots + t^k \bar{a}_k \in K_{res}[t; x \mapsto x^p]$ ($a_i \in K$). On peut clairement supposer que $v(z) = v(a_n) = \dots = v(a_k) = 0$. Alors, avec $q = t^n a_n + \dots + t^k a_k$, 0 est l'unique élément γ de $v(K)$ tel que, pour tout i vérifiant $k \leq i \leq n$, on ait $\gamma \cdot t^i a_i = \gamma \cdot q$. Par conséquent il existe $y \in M$ de valuation 0 et tel que $v(y \cdot q - z) > 0$, i.e $\bar{y} \cdot \bar{q} = \bar{z}$.

$2 \Rightarrow 1$: Soit $z \in K$. Soit Q un polynôme additif de $K[X]$, que l'on identifie avec son image q dans $K[t; x \mapsto x^p]$. Écrivons $q = t^n a_n + \dots + t^k a_k$. Soit $\delta = v(z)$. Puisque $v(K)$ est p -divisible, pour tout i tel que $k \leq i \leq n$, il existe $\gamma_i \in v(K)$ tel que $\gamma_i \cdot t^i a_i = \delta$, en particulier $\cdot q$ est surjectif sur $v(K)$. Soit i_0 tel que $\gamma_{i_0} \cdot q = \delta$. Posons $\gamma := \gamma_{i_0}$ et $J := \{j \in I \mid \gamma \cdot t^j a_j = \delta\}$. Posons $q_J = \sum_{j \in J} t^j a_j$. Puisque $\gamma \cdot (q - q_J) > \delta$, il suffit de trouver un élément y de valuation γ tel que, $v(y \cdot q_J - z) > \delta$. Écrivons $q_J = t^{j_0} s$ avec s séparable. Supposons d'abord $s = 1$. Soit alors $y \in K$ un élément de valuation δ/p^{j_0} . Si $v(y \cdot t^{j_0} - z) > v(z)$, alors on a fini. Sinon, considérons le polynôme $X^{p^{j_0}} y^{p^{j_0}} z^{-1} - 1$. Soit c la classe de $y^{p^{j_0}} z^{-1}$ dans le corps résiduel K_{res} de K . Soit $\bar{d} \in K_{res}$ tel que $\bar{d}^{p^{j_0}} c = \bar{1}$. Alors il est immédiat de vérifier que si $v((dy)^{p^{j_0}} - z) > v(z)$. Supposons maintenant $s \neq 1$. Il suffit de trouver un élément $y \in K$ tel que $v(y \cdot s - z) > v(z)$. Dans ce cas en effet, en procédant comme ci-dessus, on peut trouver $y' \in K$ tel que $v(y' \cdot t^{j_0} - y) > v(y)$; alors, en écrivant $y' \cdot q_J - z$ comme $(y' \cdot t^{j_0} - y) \cdot s + y \cdot s - z$, on voit qu'il est de valuation $> v(z)$. On peut donc supposer que $q_J = s$ est séparable. Soit $u = z/a_0$. Alors, pour tout $j \in J$, $p^j v(u) + v(a_j) = v(z)$. Par conséquent les coefficients du polynôme $F(X) := \sum_{j \in J} (Xu)^{p^j} a_j z^{-1} - 1$ sont tous de valuation 0. Soit f le polynôme à coefficients dans K_{res} obtenu en remplaçant les coefficients de F par leurs résidus dans K_{res} . Puisque K_{res} est p -clos, il existe une racine $\bar{u}_0 \in K_{res}$ de f . Il est facile de vérifier que $(u_0 u) \cdot s - z$ est de valuation $> v(z)$. ■

Les lemmes suivants permettent d'exposer diverses propriétés des modules valués résiduellement divisibles.

Lemme 4.5.7. *Soit (M, v) un module valué résiduellement divisible. Alors toute extension immédiate de (M, v) est résiduellement divisible.*

PREUVE. Soit $(M \subset N, v)$ une extension immédiate. Soit $r \in R$, de la forme $t^m \lambda$ ou comme dans la définition 4.5.1 (2), et $z \in N$ de valuation $\gamma \cdot r$. Puisque N est une extension immédiate de M , il existe $z_M \in M$ tel que $v(z - z_M) > v(z)$. Puisque $v(z_M) = v(z) = \gamma \cdot r$ et que (M, v) est résiduellement divisible, il existe $y_M \in M$ tel que $v(z_M - y_M \cdot r) > v(z_M) = v(z)$. Par conséquent $v(z - z_M + z_M - y_M \cdot r) > v(z)$. ■

Lemme 4.5.8. *Un module valué divisible est résiduellement divisible.*

PREUVE. Soit r et γ comme dans la définition 4.5.1 et $z \in M \setminus \{0\}$. Il suffit de voir qu'il existe $y \in M$ tel que $y.r = z$ et $v(y) = \gamma$. Or, pour tout y tel que $y.r = z$, on a $v(y) = \gamma$. Sinon en effet $v(y) < \gamma$. Alors $v(y) \cdot r < \gamma \cdot r$ mais $v(y.r) = \gamma \cdot r$. Cela implique que $v(y) \in \text{Saut}_M(r)$, ce qui est impossible car r a γ pour seul saut. \blacksquare

Lemme 4.5.9. *Soit (M, v) résiduellement divisible et affinement maximal. Alors (M, v) est divisible. De plus, pour chaque $r \in R \setminus \{0\}$ et pour tout $x \in M \setminus \{0\}$, il existe $y \in M$ régulier pour r tel que $y.r = x$. En conséquence pour tout $x \in M$ et pour tout $r \in R \setminus \{0\}$, tel que $x.r \neq 0$, il existe $a \in \text{ann}_M(r)$ tel que, $x - a$ est régulier pour r .*

PREUVE. On va utiliser le lemme 4.5.3.

Soit $0 \neq z \in M$. Il existe $x_0 \in M$ régulier pour r et tel que $z - x_0.r$ soit de valuation $> v(z)$. Si $z \neq x_0.r$, de même il existe $x_1 \in M$ régulier pour r et tel que $z - x_0.r - x_1.r$ soit de valuation $> v(z - x_0.r)$. Ainsi on peut construire une suite $(x_i)_{i \in \mathbb{N}}$ telle que, pour chaque i , x_i est régulier pour r et que la suite $(v(x_i))_{i \in \mathbb{N}}$ soit strictement croissante. Donc la suite $a_i = \sum_{j \leq i} x_j$ est pseudo-Cauchy et $(a_i.r)_i$ converge vers z .

Soit α un ordinal limite et supposons que l'on a défini une suite pseudo-Cauchy, $(a_i)_{i < \alpha}$, telle que $a_{i+1} - a_i$ est régulier pour r , et que $(a_i.r)_i$ converge vers z . Puisque (M, v) est affinement maximal et que $(a_i)_{i < \omega}$ est de type affine, cette suite a une limite a_α dans M . De plus, $v(a_\alpha) = v(x_0)$, et $v(x_0.r) = v(a_\alpha.r)$ et, puisque x_0 est régulier pour r , a_α est régulier pour r . Alors $z - a_\alpha.r$ est de valuation $> v(z - a_i.r)$ pour tout $i < \alpha$. Cela provient du fait que $v(z - a_\alpha.r - (z - a_i.r)) = v((a_\alpha - a_i).r) = v((a_{i+1} - a_i).r) = v(z - a_i.r)$. Donc $v(z - a_\alpha.r) \geq v(z - a_i.r)$ pour tout $i < \alpha$. Puisque la suite $v(z - a_i.r)$ est strictement croissante, on a en fait $v(z - a_\alpha.r) > v(z - a_i.r)$ pour tout i . Si $z \neq a_\alpha.r$ alors il existe $x_{\alpha+1} \in M$ régulier pour r et tel que $v(z - a_\alpha.r - x_{\alpha+1}.r) > v(z - a_\alpha.r)$. Alors $v(x_{\alpha+1}) > v(a_\alpha - a_i)$ pour tout $i < \alpha$. En effet $v(z - a_\alpha.r) > v(z - a_i.r) = v((a_{i+1} - a_i).r) = v(a_{i+1} - a_i) \cdot r = v(a_\alpha - a_i) \cdot r$, cela montre que $a_\alpha - a_i$ est régulier pour r . Comme $x_{\alpha+1}$ est régulier pour r , $v(x_{\alpha+1}) > v(x_i)$. Alors on pose $a_{\alpha+1} = a_\alpha + x_{\alpha+1}$. Pour des raisons de cardinalité on ne peut prolonger indéfiniment la suite $(a_i)_i$, et donc on trouve $a^* \in M$ régulier pour r et tel que $a^*.r = z$. \blacksquare

Corollaire 4.5.10. *Si (M, v) est affinement maximal et résiduellement divisible alors un élément $x \in M$ est régulier pour r si et seulement si $v(x) = \max\{v(y) \mid y \in M \text{ et } y.r = x.r\}$, si et seulement si $v(x) = \max\{v(x - x') \mid x' \in \text{ann}_M(r)\}$.* \blacksquare

Corollaire 4.5.11. *Soit M un module valué affinement maximal et résiduellement divisible. Soit $r \in R \setminus \{0\}$, $\gamma \in \text{Saut}_M(r)$ et $y_0 \in M$ racine du sous-polynôme r_γ . Alors il existe $y \in \text{ann}_M(r)$ tel que $v(y - y_0) > \gamma$. En particulier chaque fonction ξ_r définie comme dans le lemme 4.4.21 est bijective.*

PREUVE. Par la remarque 4.4.19, y_0 est irrégulier pour r . Par la proposition ci-dessus, il existe $y' \in M$ régulier pour r tel que $y'.r = y_0.r$. Par conséquent y' est de valuation $> v(y_0)$

et il suffit de poser $y := y' - y_0$.

Soit $\xi_r : \text{ann}(r) \rightarrow \sum_{\gamma' \in \text{Saut}_M(r)} \text{ann}(r'_{\gamma'})$, définie comme dans la proposition 4.4.21. Supposons que $\sum_{\gamma' > \gamma} \xi_{\gamma'}$ établit une bijection de $\text{ann}(r)_{>\gamma}$ sur $\sum_{\gamma' > \gamma} \text{ann}(r'_{\gamma'})$. Écrivons $y = y_{\gamma} + y_{>\gamma}$ où $y_{>\gamma}$ appartient à $\text{ann}(r)_{>\gamma}$ et y_{γ} appartient au supplémentaire choisi lors de la définition de ξ . Par l'inégalité ultramétrique on a nécessairement $\xi(y_{\gamma}) = y_0$. D'où le résultat. \blacksquare

Récapitulons les résultats que l'on vient d'exposer dans le théorème suivant. Noter que le point 2. ci-dessous est analogue au résultat 4.4.22, mais qu'on ne suppose plus ici que les annulateurs sont finis.

Théorème 4.5.12. *Soit (M, v) résiduellement divisible. Alors les assertions suivantes sont équivalentes :*

1. (M, v) est affinement maximal.
2. (M, v) est henselien, t -divisible et, pour tout $r \in R \setminus \{0\}$, il existe une bijection K_0 -linéaire ξ entre $\text{ann}_M(r)$ et $\sum_{\gamma \in \text{Saut}_M(r)} \text{ann}_M(r_{\gamma})$ telle que, pour tout $y \in \text{ann}_M(r)$, $(v(\xi(y)) - y) > v(y)$.
3. Pour tout $r \in R \setminus \{0\}$, pour tout $z \in M \setminus \{0\}$, il existe $y \in M$ régulier pour r et tel que $y.r = z$

PREUVE. 1. \Rightarrow 2. : Ce sont les énoncés 4.4.14, 4.5.9 et 4.5.11 qui l'affirment.

2. \Rightarrow 3. : Soit $z \in M \setminus \{0\}$ et $y \in M$ vérifiant $y.r = z$ donné par la divisibilité de M . Supposons que y est irrégulier pour r . Alors y est irrégulier pour un certain sous-polynôme r_{γ} , et puisque (M, v) est t -divisible et henselien, y s'écrit comme $y_0 + y_{>\gamma}$ avec $y_{\gamma}.r_{\gamma} = y.r_{\gamma}$. Soit $a_0 \in \text{ann}_M(r)$ tel que $\xi(a_0) = y_0$, alors $y - a_0$ est valuation $> \gamma$ et $(y - a_0).r = z$. Puisque $\text{Saut}_M(r)$ est fini on doit finir par trouver une suite finie $a_0, a_1, \dots, a_n \in \text{ann}(r)$ avec $y - \sum a_i$ régulier pour r .

3. \Rightarrow 1 : Si une suite pseudo-Cauchy $(x_{\rho}.r)_{\rho < \lambda}$ a une limite $z \in M$, on montre exactement de la même façon que dans la preuve du théorème 4.7.1, que $(x_{\rho})_{\rho}$ converge vers un $x \in M$ tel que $x.r = z$. \blacksquare

On déduit de ce théorème les conséquences suivantes.

Corollaire 4.5.13. *La classe des modules valués résiduellement divisibles et affinement maximaux est une classe élémentaire.*

PREUVE. Découle du point 3. du théorème ci-dessus. \blacksquare

Corollaire 4.5.14. *Si (M, v) est affinement maximal et divisible, alors il en est de même pour M_{tor} . En conséquence, une extension immédiate de M_{tor} est affinement maximale si et seulement elle est divisible.*

PREUVE. La première assertion découle de la 2ème caractérisation du théorème ci-dessus. D'autre part, par le lemme 4.5.7, toute extension immédiate A de M_{tor} est résiduellement divisible, donc si A est de plus affinement maximale alors elle est divisible. \blacksquare

Corollaire 4.5.15. *Un D -espace vectoriel valué est affinement maximal si et si seulement s'il est régulier.*

PREUVE. On avait déjà établi par 4.4.24 que tout module sans torsion henselien doit être régulier. Réciproquement un D -espace vectoriel régulier est affinement maximal par le théorème ci-dessus. ■

On termine cette section avec diverses caractérisations des éléments réguliers d'un module valué résiduellement divisible et affinement maximal (M, v) .

Lemme 4.5.16. *Soit $x \in M \setminus \{0\}$. Les assertions suivantes sont équivalentes :*

1. $x.R$ est un sous-module régulier,
2. il existe $q \in R \setminus \{0\}$ tel que x est régulier pour q et $x.q$ est régulier,
3. x est régulier,
4. $\max\{v(y-x) \mid y \in M_{tor}\}$ existe et est égal à $v(x)$,
5. $x.R$ et M_{tor} sont en somme valuation-indépendante, i.e. pour tout $y \in M_{tor}$ et tout $r \in R$, $v(x.r - y) = \min\{v(x.r), v(y)\}$.

PREUVE. $1 \Rightarrow 2$: Évident en prenant $q = 1$.

$2 \Rightarrow 3$: Soit $q \in R \setminus \{0\}$ tel que x régulier pour q et $x.q$ est régulier. Supposons que x est irrégulier pour un certain $r \in R$. Soit $q', r' \in R \setminus \{0\}$ tels que $qq' = rr'$. Alors x est irrégulier pour rr' et donc pour qq' . Dans ce cas, par le lemme 4.1.14, ou bien x est irrégulier pour q , ou bien $x.q$ est irrégulier pour q' . Contradiction.

$3 \Rightarrow 4$: Par le lemme 4.4.27 x n'est pas une limite d'une suite pseudo-Cauchy sans limite dans M_{tor} . Donc $\max\{v(y-x) \mid y \in M_{tor}\} = v(x-y_0)$ pour un certain $y_0 \in M_{tor}$. Si $v(x-y_0) > v(x)$ alors, x est irrégulier pour un certain $0 \neq r$ annihilant y_0 . D'où le résultat.

$4 \Rightarrow 5$: Supposons $v(x.r - y) > v(x.r) = v(y)$ pour un certain $0 \neq r \in R$ et $y \in M_{tor}$. Soit $z \in M$ régulier pour r , donné par le théorème 4.5.12, tel que $z.r = x.r - y$. Alors $v(z) > v(x)$ et $(x-z).r = y$. Donc $x-z \in M_{tor}$ et $v(x-(x-z)) > v(x)$: contradiction.

$5 \Rightarrow 1$: Soit $r \in R$ tel que $x.r$ est irrégulier pour un certain $s \in R$. Alors, pour un certain $x_0 \in \text{ann}_M(s)$, $v(xr - x_0) > v(x.r)$. Par conséquent les sous-modules $x.R$ et M_{tor} ne peuvent être en somme valuation-indépendante. ■

Remarque 4.5.17. Si $x \in M$ est régulier alors, par le lemme 4.1.14, chaque $x.r$ est régulier. De plus le corollaire 4.4.27, utilisé pour montrer l'implication $2 \Rightarrow 3$ dans la preuve ci-dessus, a comme seule hypothèse que (M, v) est t -divisible et henselien. Cela montre que l'équivalence entre 1, 2 et 3 s'obtient en n'utilisant le fait que (M, v) est henselien et t -divisible.

Corollaire 4.5.18. *Soit $x \in M$ régulier. Alors, pour tout $y \in M$ irrégulier de valuation $\geq v(x)$, on a $v(x+y) = v(x)$ et $x+y$ est régulier.*

PREUVE. Soit $y \in M$ irrégulier. Par l'inégalité ultramétrique, si $v(y) > v(x)$ alors $v(x+y) = v(x)$ et donc pour $r \in R \setminus \{0\}$, on a $v(x.r) = v(x).r < v(y).r \leq v(y.r)$, d'où $v((x+y).r) = v(x).r$, et ainsi $x+y$ est régulier pour r .

Supposons que $v(x) = v(y)$. Soit $q \in R$ pour lequel y est irrégulier. Alors $v(y.q) > v(x.q)$ et par conséquent $v((x+y).q) = v(x.q) = v(x) \cdot q$, donc on ne peut avoir $v(x+y) > v(x) = v(y)$. Soit $r \in R \setminus \{0\}$. Montrons que $x+y$ est régulier pour r . Si y est irrégulier pour r , en répétant l'argument ci-dessus, $v(y.r) > v(x.r) = v(x) \cdot r$ et $v((x+y).r) = v(x) \cdot r = v(x+y) \cdot r$. Si y est régulier pour r alors $v(x.r) = v(y.r)$. De plus $y.r$ est irrégulier car sinon, par le lemme 4.5.16, y serait régulier avec $v(x) = v(y)$. Puisque x est régulier, $x.r$ est régulier et, par le paragraphe ci-dessus, on a $v(x.r+y.r) = \min\{v(x.r), v(y.r)\} = v(x.r)$ qui est égal à $v(x) \cdot r$ car x est régulier. Toujours par le paragraphe ci-dessus $v(x+y) = v(x)$ et donc $v(x+y) \cdot r = v((x+y).r)$; i.e. $x+y$ est régulier pour r . \blacksquare

Corollaire 4.5.19. *Soit $M^* \subset M$ un sous-module valué divisible contenant M_{tor} et $x_1 \in M \setminus M^*$. Supposons que pour un certain $x_0 \in M^*$, on a $v(x_1 - x_0) = \max\{v(x_1 - x') \mid x' \in M^*\}$. Alors $x := x_1 - x_0$ est régulier et les sous-modules M^* et $x.R$ sont en somme valuation-indépendante.*

PREUVE. Même démonstration que pour 4 \Rightarrow 5 dans la preuve du lemme 4.5.16. \blacksquare

4.6 Un principe d'Ax-Kochen et Ershov

Dans cette section on va voir que la théorie d'un module valué affinement maximal et résiduellement divisible est codée dans la théorie de sa chaîne de valuation (cf. le théorème 4.6.3).

Soit Q l'ensemble des éléments premiers $r \in R$, tel qu'il existe $\gamma \in \Delta \setminus \{0\}$ tel que pour tout monôme $t^i a_i$ de r on a :

$$\gamma \cdot t^i a_i = \gamma \cdot r.$$

En particulier, un tel r a exactement un seul saut, à savoir γ . On va montrer que pour tout $r \in R \setminus \{0\}$, $|\text{ann}_M(r)|$ dépend uniquement des $|\text{ann}_M(q)|$ pour un nombre fini de $q \in Q$.

Proposition 4.6.1. *Soit (M, v) résiduellement divisible et affinement maximal. Alors la fonction $\eta_M : R \setminus \{0\} \rightarrow \mathbb{N} \cup \{\infty\}$, $r \mapsto |\text{ann}_M(r)|$, est déterminée par sa restriction à Q .*

PREUVE. Nous raisonnons par induction sur le degré. Soit $d \in \mathbb{N} \setminus \{0\}$. Notons $R_{<d}$ l'ensemble des polynômes non nuls de degré strictement inférieur à d . Soit r un élément de R de degré d , qu'on peut supposer séparable. Si $d = 1$, alors r est premier et a au plus deux monômes. Si de plus $\text{Saut}_M(r)$ est non vide alors $r \in Q$; sinon $\eta_M(r) = 0$, nécessairement. Supposons $d > 1$ et la restriction de η_M à $R_{<d}$ déterminée par la restriction de η_M à Q . On a $r = r_1 \dots r_n$ où les r_i sont premiers. Donc $|\text{ann}_M(r)| = \prod_i |\text{ann}_M(r_i)|$. Si $n > 1$, alors on a fini grâce à l'hypothèse de l'induction. On peut donc supposer que r est premier et $r \notin Q$. Alors, par le théorème 4.5.12, $|\text{ann}_M(r)| = \prod_{\gamma \in \text{Saut}_M(r)} |\text{ann}_M(r_\gamma)|$. Puisque $r \notin Q$, $|\text{Saut}_M(r)| \geq 2$. Soit $\delta = \min \text{Saut}_M(r)$. Alors, r_δ n'est pas séparable et pour tout $\gamma \neq \delta$, r_γ est de degré strictement inférieur à d . Alors on a fini par l'hypothèse d'induction. \blacksquare

Avant d'attaquer le résultat final de cette section, rappelons le contexte dans lequel on travaille. On considère nos modèles dans le langage $L = L_V \cup L_R \cup \{v\}$, où L_R est le langage des R -modules, L_V le langage des R -chaînes et v un symbole de fonction unaire.

Pour établir le résultat d'Ax-Kochen et Ershov on procède comme dans le chapitre précédent et on montre un résultat d'élimination des quantificateurs de la sorte module, relativement à une théorie complète de R -chaînes.

On considère un corps (K, v_K) valué non trivialement, φ un endomorphisme de $(K, +, \times)$ tel que $v_K(\varphi(x)) \geq 2v_K(x)$ pour tout $x \in \mathcal{O}_K$, et $R = K[t; \varphi]$. Soit (F, Δ) un R -module non K -trivialement valué tel que la valuation induite par la K -chaîne $v(F)$ sur K est v_K . Soit T_v la L_V -théorie complète de $v(F)$, Tor_F la L_R -théorie constituée des énoncés vrais dans F , de la forme $|\eta_F(r)| = n$ ou des ensembles d'énoncés exprimant $|\eta_F(r)| = \infty$, pour $r \in Q$, et T_{Mm} la théorie des modules non K -trivialement valués, affinement maximaux et résiduellement divisibles. On pose

$$\mathbf{T} := T_{Mm} \cup T_v \cup \text{Tor}_F.$$

Soit Θ_v l'ensemble des L -formules de la forme :

$$\phi(\bar{x}) \bigwedge \bar{Q} \bar{y}_1 \psi(\bar{y}_1, \bar{y}_2, v(t_1(\bar{x})), \dots, v(t_k(\bar{x}))), \text{ où :}$$

- ϕ est sans quantificateur dans le langage des R -modules L_R , ψ est sans quantificateur dans L_V , et \bar{Q} est un ensemble de quantificateurs,
- \bar{x} est un uplet de variables de la sorte module, \bar{y}_1, \bar{y}_2 sont des uplets de variables de la sorte de l'ensemble des valuations, et les t_i sont des L_R -termes en \bar{x} .

Remarque 4.6.2. Si (M, v) et (N, w) sont deux modules non K -trivialement valués, alors un L -plongement de (M, v) vers (N, w) est donné par un couple (f, f_v) où f est un L_R -plongement et f_v un L_V -plongement, tels que, pour tout $x \in M$, on ait $f_v(v(x)) = w(f(x))$.

Théorème 4.6.3. *La théorie \mathbf{T} élimine les quantificateurs portant sur la sorte module : toute L -formule est équivalente modulo \mathbf{T} à une formule de Θ_v . En conséquence si (M, v) et (N, w) sont des modèles de \mathbf{T} :*

- Si (M, v) se plonge dans (N, w) de telle façon que le plongement induit de $v(M)$ dans $w(N)$ soit L_V -élémentaire, alors $(M, v) \preceq (N, w)$.
- Si (M, v) se plonge dans (N, w) de telle façon que l'image de $v(M)$ dans $w(N)$ par le plongement induit soit existentiellement close dans $w(N)$, alors (M, v) est existentiellement clos dans (N, w) .
- Si les chaînes $v(M)$ et $w(N)$ sont L_V -élémentairement équivalentes, alors (M, v) et (N, w) sont élémentairement équivalents.

Corollaire 4.6.4. *Soit (M, v_1) et (N, v_2) deux corps de Kaplansky algébriquement maximaux, extensions algébriques communes non ramifiées d'un corps valué (K, v) de caractéristique $p > 0$. Alors, avec $R := K[t; x \mapsto x^p]$ et $R' := K_{res}[t; x \mapsto x^p]$, on a $(M, v_1) \equiv (N, v_2)$ comme R -modules valués, si et seulement si $M_{res} \equiv N_{res}$ comme R' -modules.*

PREUVE. Il suffit de vérifier que, pour tout corps (M, w) qui est de Kaplansky, algébriquement maximal, et extension non ramifiée de (K, v) , la théorie du corps résiduel M_{res} , comme R' -module, détermine la fonction η_M .

Soit $q = \sum_{i=0}^n t^i a_i \in Q$ et $\gamma \in w(M) \setminus \{\infty\}$ tel que $\gamma \cdot r = \gamma \cdot t^i a_i$ pour tout monôme $t^i a_i$ de q . On peut clairement supposer que $a_0 = 1$. Soit $z \in K$ de valuation γ . Considérons le

polynôme $r := zqz^{-1}$, qui correspond au polynôme additif :

$$z^{(p^n-1)}a_nX^{p^n} + \dots + z^{(p^i-1)}a_iX^{p^i} + \dots + X.$$

Par le fait que $\{\gamma\} = \text{Saut}_M(q)$, on a pour tout i , $p^i v(z) + v(a_i) = v(z) = \gamma$, d'où r a tous ses coefficients de valuation 0. Par définition de r , en considérant l'application $x \mapsto xz$, on a $|\text{ann}_M(r)| = |\text{ann}_M(q)|$. Ensuite $|\text{ann}_M(r)| = |\text{ann}_{M_{res}}(\bar{r})|$, car r est séparable et M henselien. ■

Le théorème 4.6.3 sera une conséquence du résultat ci-dessous.

Proposition 4.6.5. *Soit (M, v) et (N, w) deux modules valués modèles de \mathbf{T} . Supposons (N, w) $|M|^+$ -saturé. Soit $(A, v) \subset (M, v)$ une sous-structure telle que (A, v) se plonge par un isomorphisme partiel $\mathbf{f} = (f, f_v)$ préservant les formules de Θ_v dans (N, w) . Alors \mathbf{f} s'étend en un plongement préservant les formules de Θ_v , de (M, v) dans (N, w) .*

Afin de montrer la proposition ci-dessus, on commence par établir des lemmes préliminaires.

Dans tout ce qui suit (M, v) et (N, w) seront comme dans l'énoncé ci-dessus.

Lemme 4.6.6. *Soit A un sous-module de M , $x \in M \setminus A$ affine sur A , et r_0 le polynôme minimal de x sur A . Soit $y \in N$ tel que $y.r_0 = f(x.r_0)$. Supposons que, pour tout r de degré $< \deg(r_0)$ et tout $z \in M$, si $z.r \in A$, alors $z \in A$. Supposons de plus que $g_v : v(A + x.R) \rightarrow w(N)$, est un L_V -plongement prolongeant f_v et vérifie pour tout $a \in A$, $g_v(v(x - a)) = w(y - f(a))$. Alors, en notant $g : A + x.R \rightarrow N$, l'homomorphisme de module envoyant x sur y et prolongeant f , $\mathbf{g} := (g, g_v)$ est un plongement de module valué de $(A + x.R, v)$ dans (N, w) .*

PREUVE. Il suffit de montrer que pour tout r de degré $< n$ et pour tout $a \in A$ on a $g_v(v(x.r - a)) = w(y.r - f(a))$. Soit r de degré $< n$. Par hypothèse A contient tous les $a_i \in M$ tels que $a_i.r = a$. Par le lemme 4.5.12 il existe un certain i_0 tel que $(x - a_{i_0})$ est régulier pour r . Or $v(x - a_{i_0}) = \max\{v(z) \mid z \in M, v(z.r) = (x.r - a)\} = \max\{v(x - a_i) \mid a_i.r = a\}$. Par conséquent $w(y - f(a_{i_0})) = g_v(v(x - a_{i_0})) = \max\{v(y - f(a_i)) \mid a_i.r = a\}$. Donc $y - f(a_i)$ est régulier pour r . Il vient : $g_v(v(x.r - a)) = g_v(v(x - a_{i_0}) \cdot r) = w(y - f(a_{i_0})) \cdot r = w(y.r - f(a))$. ■

Lemme 4.6.7. *Soit x, y et r_0 comme ci-dessus. Supposons que $g_v(v(x)) = w(y)$ et $x.r_0 \neq 0$.*

- i. *Si $a \in A$, si $x - a$ est régulier pour r_0 et si $y - f(a)$ est régulier pour r_0 , alors $g_v(v(x - a)) = w(y - f(a))$.*
- ii. *Si de plus A contient toutes les racines de r_0 dans M , alors les assertions suivantes sont équivalentes :*

- (1) *pour tout $a \in A$, $g_v(v(x - a)) = w(y - f(a))$,*
- (2) *pour tout $a \in A$, $x - a$ est régulier pour r_0 si et seulement si $y - f(a)$ est régulier pour r_0 .*

PREUVE. i) Soit $z := x - a$ régulier pour r_0 , et $z' := y - f(a)$ régulier pour r_0 , c'est-à-dire que l'on a $g_v(v(z) \cdot r_0) = w(z') \cdot r_0$ en plus du fait que $g_v(v(z.r_0)) = w(z'.r_0)$. Or $g_v(v(z) \cdot r_0) = g_v(v(z)) \cdot r_0$. D'où $g_v(v(z)) = w(z')$.

ii) (1) \Rightarrow (2) : Soit $a \in A$ tel que $x - a$ est régulier pour r_0 . Supposons que $y - f(a)$ est irrégulier pour r_0 , alors pour un certain $b_0 \in \text{ann}(r_0) \subset B$, $w(y - f(a) - b_0) > w(y - f(a))$.

Par conséquent, avec $a_0 := f^{-1}(b_0)$, on a $v(x - a - a_0) > v(x - a)$. Ceci est impossible.

(2) \Rightarrow (1) : Soit $a \in A$. Si $x - a$ est régulier pour r_0 alors il en va de même pour $y - f(a)$. Par le point i , on a le résultat. Soit maintenant $a \in A$ tel que $x - a$ est irrégulier et donc $y - f(a)$ est irrégulier. Alors pour un certain $a_0 \in \text{ann}(r)$, $x - a - a_0$ est régulier de valuation $> v(x - a)$. Alors $y - f(a) - f(a_0)$ est régulier de valuation $> w(y - f(a))$. En particulier, $v(a - x) = v(a_0)$ et $w(y - f(a)) = w(f(a_0))$. Ceci montre l'assertion. \blacksquare

L'essentiel de la preuve de la proposition 4.6.5 réside dans la proposition ci-dessous.

Proposition 4.6.8. *Soit C et C' des sous-modules respectifs de M et de N , isomorphes via $\mathbf{f} = (f, f_v)$ qui préserve les formules de Θ_v . Alors \mathbf{f} s'étend en un plongement de module valué, préservant les formules de Θ_v , de la clôture divisible de $(M_{tor} + C)$ dans celle de $(N_{tor} + C)$.*

PREUVE. Remarquons tout d'abord que tout sous-module de M contenant M_{tor} admet un unique plus petit sous-module divisible le contenant. C'est exactement l'ensemble des $x \in M$ tels que, pour un certain $r \in R \setminus \{0\}$, $x.r \in C$. Cela justifie l'emploi de l'expression « clôture divisible » dans l'énoncé.

On commence par montrer que f_v admet un prolongement $g_v : v((C + M_{tor})^{div}) \rightarrow w((C + N_{tor})^{div})$. Il est facile de voir qu'on peut fermer $v(C)$ et $w(C')$ d'abord par τ^{-1} : si δ est tel que $\tau^n(\delta) \in v(C)$, et si n est le minimum des entiers k tel que $\tau^k(\delta) \in v(C')$, alors on prolonge la fonction f_v à $v(C) \cup \{\delta\}$ en choisissant dans $w(N)$ l'unique δ' tel que $\tau^n(\delta') = f_v(\tau^n(\delta))$. Le prolongement obtenu en continuant ainsi est un isomorphisme de R -chaîne entre $v(A^t)$ et $w((C')^t)$. On peut donc supposer que $v(C)$ et $w(C')$ sont clos par τ^{-1} . Ceci implique que l'on a $v((C + M_{tor})^{div}) = v(C) \cup \text{Saut}_M(R)$. Par ailleurs, $v(M_{tor}) = \text{Saut}_M(R)$ et $w(N_{tor}) = \text{Saut}_N(R)$ et chaque saut est uniquement déterminé par une équation de la forme $\tau^i(-) \cdot a = (-)$, qui provient d'un élément de Q . Donc, si $\gamma \in \text{Saut}_M(R)$ vérifie une équation comme ci-dessus, puisque $\eta_M = \eta_N$, il existe $\delta \in w(N_{tor})$ vérifiant la même équation que γ ; alors en envoyant γ sur δ on prolonge f_v . On continue jusqu'à ce que l'on épuise $v(M_{tor})$. Le plongement obtenu est alors un plongement de R -chaîne en vertu de la proposition 4.1.9; notons le g_v . Vérifions que $(f, g_v) : (C, v((M_{tor} + C)^{div})) \rightarrow (C', w((N_{tor} + C')^{div}))$ préserve les formules de Θ_v : en effet, puisque f_v préserve toutes les L_V -formules, f_v est un isomorphisme de $L_V(v(C))$ -structures entre les chaînes $v(C)$ et $w(C')$. De plus chaque élément γ de $v((C + M_{tor})^{div})$ tel que $\tau^n(\gamma) \in v(C)$ pour un certain entier n , est $v(C)$ -définissable (respectivement chaque élément δ de $w((C' + N_{tor})^{div})$ tel que $\tau^n(\delta) \in w(C')$ pour cet entier n est $w(C)$ définissable). Donc γ et δ vérifient les mêmes L_V -formules. Par ailleurs, chaque saut est \emptyset -définissable, donc, il en va, a fortiori, de même pour les éléments de $v(M_{tor})$ et $w(N_{tor})$. En conséquence, g_v préserve toutes les L_V -formules et (f, g_v) préserve les formules de Θ_v .

Par la suite on supposera donc f_v est un isomorphisme de R -chaînes ordonnées prélevant les formules de Θ_v entre $v((M_{tor} + A)^{div})$ et $w((N_{tor} + B)^{div})$.

On va montrer par induction sur $n \in \mathbb{N}$ l'assertion suivante : Pour tout sous-module A ,

tel que $(M_{tor} + C)^{div} \supset A \supset C$, si \mathbf{f} est un isomorphisme partiel de domaine $(A, v(A))$ sur $(B, w(B))$, alors il se prolonge, en respectant f_v , à un sous-module $\bar{A} \subset (M_{tor} + A)^{div}$ tel que, pour tout $q \in R \setminus \{0\}$ de degré $\leq n$, \bar{A} contient tout $x \in M$ tel que $x.q \in \bar{A}$.

Il est clair que cela suffit pour obtenir la conclusion de la proposition.

Notons que, puisque tout sous-module est un K -espace vectoriel, l'assertion est trivialement vraie pour $n = 0$. Fixons un entier $n > 0$ et supposons que pour tout sous-module comme ci-dessus et pour tout entier $k < n$, l'assertion est vraie.

Soit alors $(C \subset A \subset M, v)$ isomorphe à $(C' \subset B \subset N, w)$ via $\mathbf{f} = (f, f_v)$. D'après la discussion ci-dessus, on suppose que f_v est un isomorphisme de R -chaîne entre $v((C + M_{tor})^{div})$ et $w(N_{tor} + C')^{div}$. On va donc prolonger f tel que \mathbf{f} soit un plongement de module valué. Notons que le prolongement à \bar{A} qui sera ainsi obtenu, préservera nécessairement les formules de Θ par le fait que $v(\bar{A}) \subset v((C + M_{tor})^{div})$ et $w(\bar{B}) \subset w((C + M_{tor})^{div})$.

On va séparer la démonstration en quatre étapes.

1ère étape. On va montrer que \mathbf{f} se prolonge à un sous-module \hat{A} tel que, pour tout r de degré n , pour tout $x \in M$ de valuation $> \max Saut_M(r)$ (en particulier tout tel x est régulier pour r), si $x.r \in \hat{A} \setminus \{0\}$, alors $x \in \hat{A}$. On convient que si $Saut_M(r)$ est vide alors pour tout $x \in M$, $v(x) > \max Saut_M(r)$.

Soit $q \in R$ de degré n , $a \in A \setminus \{0\}$ et $x \in M \setminus A$ vérifiant et $x.q = a$. Choisissons $y \in N \setminus B$, régulier pour q et tel que $y.q = f(a)$. En particulier $w(y) > \max Saut_N(q)$. D'abord remarquons que q est nécessairement premier : si $q = rr'$, avec $r, r' \notin K$, alors $(x.r).r' \in A$ et donc $x.r \in A$, par suite $x \in A$, contradiction. Donc q -quitte à le rendre unitaire- est le polynôme minimal de x sur A et de y sur B . Par conséquent, si $y.q = f(a)$, les modules $A + x.R$ et $B + y.R$ sont isomorphes par un isomorphisme étendant f et envoyant x sur y . Par ailleurs, d'une part puisque $f_v(v(x.q)) = w(f(a)) = w(y.q)$ et que x et y sont régulier pour q , on a $f_v(v(x)) = w(y)$; d'où pour tout a' tel que $v(x - a') = \min\{v(x), v(a')\}$, on a $f_v(v(x - a')) = w(y - f(a'))$. Par ailleurs, pour tout $a' \in A$, tel que $v(x - a') > v(x) = v(a')$, $x - a'$ est régulier pour q et on a $f_v(v(a - a'.q)) = f_v(v(x - a') \cdot q) = w(f(a) - f(a').q) = w(y - f(a')) \cdot q$. Donc $f_v(v(x - a')) = w(y - f(a'))$. Par conséquent, par le lemme 4.6.6, en envoyant x sur y , f se prolonge en un isomorphisme de module valué entre $(A + x.R, v)$ et $(B + y.R, w)$, de telle sorte que \mathbf{f} soit un plongement de module valué.

(*) Par l'hypothèse d'induction il existe un sous-module $A(x)_{<n} \supset A + x.R$ et contenant tout $x' \in M$ tel que $x'.s \in A(x)_{<n}$ pour un certain $s \neq 0$ de degré $< n$. En itérant le processus, on construit un sous-module $A_1 \supset A$ de M tel que, pour tout r de degré n et tout $x' \in M$, si $x'.r \in A \setminus \{0\}$ et si $v(x') > \max Saut_M(r)$, alors $x' \in A_1$. On construit de même pour tout entier i , A_{i+1} à partir de A_i . Alors $\hat{A} := \bigcup_{i \in \mathbb{N}} A_i$ vérifie la propriété voulue.

Par ce qui précède, on suppose désormais que $\hat{A} = A$. Remarquons que A est en particulier

divisible par tous les polynômes qui ne possèdent pas de sauts.

2ème étape. On va maintenant étendre \mathbf{f} à un sous-module A' qui contient tout élément $x \in M$ tel que $x.r \in A'$ pour un certain $r \in R$ de degré $\leq n$ et ayant au plus un seul saut.

2.1 On va ajouter à A les racines des polynômes de degré n ayant un seul saut, étendre \mathbf{f} . Choisissons un tel r , et $x \in M \setminus A$ tel que $x.r = 0$. Soit $y \in N$ une racine de r . Alors $f_v(v(x)) = w(y)$ par le fait que f_v envoie l'unique saut de r dans $v(M)$ sur l'unique saut de r dans $w(N)$. De plus, pour tout $a \in A$ tel que $v(x-a) > v(x) = v(a)$, on a, $x-a$ est de valuation $> \max \text{Saut}_M(r)$ donc appartient à A par l'étape précédente, donc $x \in A$: contradiction. D'où pour tout $a \in A$, $v(x-a) = \min\{v(x), v(a)\}$ et $f_v(v(x-a)) = w(y - f(a))$. Cela montre avec 4.6.6 que, en envoyant x sur y , on peut prolonger \mathbf{f} sur $(A + x.R, v)$. On applique alors le procédé (*).

2.2 On va maintenant ajouter tout $x \in M$ tel que $x.r \in A$ pour un certain r de degré n ayant un seul saut. Soit deux tels x et r . Alors, $v(x-a)$ est nécessairement régulier pour r , pour tout $a \in A$. En effet sinon pour un certain $a_0 \in \text{ann}_M(r)$, $v(x-a-a_0) > v(x-a)$ et $x-a-a_0$ est de valuation strictement plus grande que le seul saut de r , donc $x \in A$ comme ci-dessus : contradiction. Soit alors $y \in N$ tel que $y.r = f(x.r)$. Alors y est nécessairement régulier par ce qu'on vient de remarquer, et de même pour tout $a \in A$, $y - f(a)$ est régulier pour r . Par le lemme 4.6.7 f se prolonge sur $(A + x.R, v)$.

Par ce qui précède et par le procédé d'induction (*), on peut maintenant supposer que A contient toutes les racines des polynômes de degré n n'ayant qu'un seul saut et tout élément $x \in M$ tel que $x.r \in A$, pour un r n'ayant qu'au plus un seul saut, et x de valuation strictement plus grande que l'unique saut r . Alors A est en particulier résiduellement divisible, pour les polynômes de degré $\leq n$. C'est-à-dire que les conditions de la définition 4.5.7 sont vérifiées pour les polynômes r de degré $\leq n$ (cf. remarque 4.5.4).

3ème étape. On va maintenant ajouter les racines des polynômes arbitraires de degré n . Soit r de degré n et $x \in M \setminus A$ tel que $x.r = 0$. On va montrer que x est limite d'une suite pseudo-Cauchy $(a_\gamma)_\gamma$ de A , sans limite dans A , de type affine et telle que $a_\gamma.r$ converge vers 0 et que r est de degré minimal parmi les polynômes $q \in R$ tel que $(a_\gamma.q)_\gamma$ ait une limite dans A . Cela impliquera que $A + x.R$ est une extension immédiate de A , que son type d'isomorphisme est uniquement déterminé, et que \mathbf{f} se prolonge sur $(A + x.R, v)$. Soit $a_0 := \xi_r(x) \in \sum_{\gamma \in \text{Saut}_M(r)} \text{ann}_M(r_\gamma)$; alors $v(x-a_0) > v(x)$ et $x-a_0$ est régulier pour r . Remarquons que $\sum_{\gamma \in \text{Saut}_M(r)} \text{ann}_M(r_\gamma) \subset A$, par l'étape 2. Puisque A est résiduellement divisible pour les polynôme de degré n , par la remarque 4.5.4 il existe $a'_1 \in A$ régulier pour r tel que $v(a_0.r - a'_1.r) > v(a_0.r)$. Puisque $x-a_0$ et a'_1 sont régulier pour r , nécessairement $v(a_1) = v(x-a_0) > v(a_0)$. On pose $a_1 = a_0 + a'_1$. On continue de même en prenant pour tout entier $k \geq 1$, $a'_k \in A$ régulier pour r tel que $v((a_0 + a'_1 + \dots + a'_{k-1}).r + a'_k.r) > v((a_0 + a'_1 + \dots + a'_{k-1}).r)$, et en posant $a_k = a_{k-1} + a'_k$. Alors clairement $(a_k)_{k < \omega}$ est une suite pseudo-Cauchy convergeant vers x et $(a_k.r)$ converge vers 0. Si $(a_k)_k$ a une limite a_ω dans A , alors $v(x-a_\omega) > v(a_{k+1} - a_k)$

pour tout k , et donc on peut continuer de même pour en choisissant $a_{\omega+1}, a_{\omega+2} \dots$; et de même pour tout ordinal limite α , jusqu'à avoir construit une suite sans limite dans A . De plus, si q est de degré $< \deg(r)$ et $(a_\gamma \cdot q)_\gamma$ ait une limite $b \in A$, alors $(a_\gamma)_\gamma$ converge vers un élément $x' \in (M_{tor} + A)^{div}$ tel que $x' \cdot q \in A$, par le fait que $(M_{tor} + A)^{div}$ est affinement maximal et divisible. Mais alors x' devrait être dans A . Donc r est de degré minimal tel que $(a_\gamma \cdot q)_\gamma$ ait une limite dans A , pour un certain $q \in R$. Ce qu'il fallait montrer.

4ème étape. Il reste à ajouter les $x \in M \setminus A$ tels que $x \cdot r \in A \setminus \{0\}$, pour un certain r de degré n ayant $|Saut_M(r)| \geq 2$. On va supposer que $|Saut_M(r)| = 2$, le cas général se traite de même.

Puisque A contient les racines de r , quitte à changer x par $x - a_0$ pour un $a_0 \in \text{ann}_M(r)$ tel que $x - a_0$ est régulier pour r , on peut supposer que x est régulier pour r . Notons γ_1, γ_2 avec $\gamma_1 < \gamma_2$ les sauts de r dans $v(M)$. Si $v(x) > \gamma_1$ et s'il existe $a \in A$ tel que $x - a$ est irrégulier pour r , on a pour un certain $a_0 \in \text{ann}_M(r)$, $x - a - a_0$ est régulier de valuation $> \gamma_2$ donc par l'étape 1, $x \in A$. Contradiction. Par conséquent pour tout $a \in A$, $x - a$ est régulier pour r . Alors, par 4.6.7, en choisissant $y \in N \setminus \{0\}$ tel que $y \cdot r = f(a)$ et y régulier pour r , on peut prolonger f à $(A + x \cdot R, v)$, et donc \mathbf{f} , en envoyant x sur y . Maintenant on peut supposer que A contient tout élément z de valuation $> \gamma_2$, tel que $z \cdot r \in A$. Alors on procède de même manière. ■

Notons un résultat intermédiaire en rappelant que tout D -espace vectoriel régulier est affinement maximal par 4.5.15.

Corollaire 4.6.9. *Si A est un R -sous-module non nul des D -espaces vectoriels réguliers E_1 et E_2 , qui sont des clôtures divisibles de A , alors E_1 et E_2 sont isomorphes au dessus de A comme espaces vectoriels valués.*

Preuve de la proposition 4.6.5. Nous procédons par induction transfinie. Par la proposition ci-dessus, on peut supposer que A contient M_{tor} et est divisible et donc affinement maximal. Soit $\gamma \in v(M) \setminus v(A)$ et $x \in M$ de valuation γ . Alors pour tout $r \in R \setminus \{0\}$, $v(x) \cdot r \notin v(A)$ et donc les sous-modules $x \cdot R$ et A sont en somme valuation-indépendante. Par saturation et par le fait que f_v est un isomorphisme partiel préservant les L_V -formules, il existe $\delta \in w(N)$ satisfaisant les mêmes $L_V(v(A))$ -formules que γ . On prolonge f_v à $v(A) \cup \{\gamma \cdot r \mid r \in R \setminus \{0\}\}$ en envoyant $\gamma \cdot r$ sur $\delta \cdot r$ pour tout $r \in R$. Alors, pour tout $y \in N$ de valuation δ , B et $y \cdot R$ sont en somme valuation-indépendante. Donc on peut prolonger \mathbf{f} sur $A + x \cdot R$ en envoyant x sur y . Par suite par la proposition ci-dessus on peut prolonger \mathbf{f} sur l'unique clôture divisible de $A + x \cdot R$. De plus, par le choix de δ et y , \mathbf{f} préserve les formules de Θ_v .

Donc, par induction transfini, on peut supposer qu'on ait $v(M) = v(A)$, de plus du fait que A contient M_{tor} et affinement maximal. Soit $x \in M \setminus A$. Avec cela, tout isomorphisme partielle prolongeant \mathbf{f} préserve nécessairement les formules de Θ_v . Soit maintenant $x \in M$, limite sur A d'une suite pseudo-Cauchy $(x_\alpha)_{\alpha \in \Omega}$. Cette suite est nécessairement de type transcendant. Donc le type d'isomorphisme sur (A, v) de $(A + x \cdot R, v)$ est uniquement déterminé par $(x_\alpha)_\alpha$. Par saturation la suite $(f_v(x_\alpha))_\alpha$ admet une limite dans N , et donc $(A + x \cdot R, v)$ se plonge dans (N, w) par un isomorphisme prolongeant \mathbf{f} . Par le lemme 4.5.7, l'extension immédiate $(A + x \cdot R, v)$ de A est résiduellement divisible. Dans ce cas, peut prolonger \mathbf{f} sur l'unique

extension affine et affinement maximale de $(A + x.R, v)$, qui n'est que la clôture divisible $A + x.R$.

Enfin si x n'est pas limite sur A , alors par le lemme 4.5.19 pour un certain $a \in A$ vérifiant $v(x - a) = \max\{v(x - a') \mid a' \in A\}$ les sous-modules A et $(x - a).R$ sont en somme valuation-indépendante. Alors par saturation il existe $y \in N \setminus B$ tel que $w(y - f(a)) = \max\{w(y - b) \mid b \in B\}$. Alors l'homomorphisme de module prolongeant f et envoyant x sur y définit un plongement du module valué $A + (x - a).R$ dans N ; on finit comme ci-dessus. \blacksquare

4.7 Unicité de l'extension immédiate maximale des modules résiduellement divisibles

Dans le procédé va-et-vient de la démonstration du théorème 4.6.3, on a du être plus fine que le résultat global ci-dessous.

Théorème 4.7.1. *Soit (M, v) un module valué résiduellement divisible. Alors*

1. *à isomorphisme près, (M, v) a une unique extension immédiate affine et affinement maximale;*
2. *à isomorphisme près, (M, v) a une unique extension immédiate maximale.*

PREUVE. 1. Soit M_1^* et M_2^* deux extensions immédiates, affines et affinement maximales de M . Soit $N_1 \subset M_1^*$ et $N_2 \subset M_2^*$ deux extensions immédiates affines de M , qui sont isomorphes, disons via f , au-dessus de M . Par le lemme de Zorn et par le corollaire 4.3.17, il suffit de montrer que, si $(x_\rho)_\rho$ est une suite pseudo-Cauchy de type affine de N_1 sans limite dans N_1 , alors il existe une limite x de $(x_\rho)_\rho$ dans M_1^* et une limite y de $(f(x_\rho))_\rho$ dans M_2^* , telles que f se prolonge en un isomorphisme entre $N_1 + x.R$ et $N_2 + y.R$. Soit $r \in R \setminus \{0\}$ de degré minimal tel que $(x_\rho.r)_\rho$ converge vers un élément a de N_1 . Remarquons que $(f(x_\rho).r)_\rho$ converge vers $f(a)$ et que r est degré minimal tel que $(f(x_\rho).r)_\rho$ admet une limite dans N_2 . Par le lemme 4.3.18, N_1 a une extension immédiate affine contenant une limite x de $(x_\rho)_\rho$, extension dont le type d'isomorphisme est déterminé par $(x_\rho)_\rho$, r et a , et qui est telle que r est le polynôme minimal de x sur N_1 , et $x.r = a$. Il suffit de trouver dans M_1^* une limite x de la suite $(x_\rho)_\rho$ vérifiant $x.r = a$ (respectivement une limite $y \in M_2^*$ de la suite $(f(x_\rho))_\rho$ vérifiant $y.r = f(a)$). On peut clairement supposer $N_1 = N_2 = M$ et il reste à montrer que, si $(x_\rho)_\rho$, r et a sont comme ci-dessus, alors toute extension immédiate, affine et affinement maximale de M contient une limite x de $(x_\rho)_\rho$ qui vérifie $x.r = a$.

Soit (M^*, v) une extension immédiate, affine et affinement maximale de M , $(x_\rho)_{\rho < \lambda}$ une suite pseudo-Cauchy de M , de type affine et sans limite dans M , et $r \in R \setminus \{0\}$ de degré minimal tel que $x_\rho.r$ a une limite dans M , que nous noterons a . On va montrer que M^* contient une limite de la suite $(x_\rho)_{\rho < \lambda}$ qui est solution de l'équation $x.r = a$. On définit une suite $(y_\rho)_{\rho < \lambda}$ de M^* en choisissant, pour tout $\rho < \lambda$, un élément $y_\rho \in M^*$, dont l'existence est donnée par le lemme 4.5.9, régulier pour r et tel que $y_\rho.r = x_\rho.r - a$. Remarquons que la suite $(v(y_\rho))_\rho$ est strictement croissante. Si $a = 0$, alors $(v(x_\rho.r))_\rho$ converge vers 0. Donc, avec le fait que x_ρ est

sans limite dans M , tous les x_ρ sont irréguliers pour r à partir d'un certain rang. C'est-à-dire que, quand ρ est assez grand, x_ρ s'écrit comme $y_\rho + a_\rho^0$ avec y_ρ régulier pour r et, nécessairement $v(a_\rho^0) = v(x_\rho)$ car, puisque y_ρ est régulier pour r , on a $v(y_\rho) > v(x_\rho)$. Puisque la suite $(x_\rho)_\rho$ est pseudo-Cauchy, la suite $(v(a_{\rho+1}^0 - a_\rho^0))_\rho$ ou bien est asymptotiquement strictement croissante ou bien prend asymptotiquement la valeur ∞ . Or la suite $(a_{\rho+1}^0 - a_\rho^0)_\rho$ vit dans $\text{ann}_{M^*}(r)$, donc la suite de ses valuations vit dans $\text{Saut}_{M^*}(r)$ qui est fini. Donc nécessairement $a_{\rho+1}^0 = a_\rho^0$ à partir d'un certain rang. En choisissant ρ_0 suffisamment grand, la suite $(x_\rho)_\rho$ converge vers $a_{\rho_0}^0$.

Supposons maintenant $a \neq 0$. Soit $b \in M^*$ régulier pour r et tel que $b.r = a$. Chaque x_ρ s'écrit alors comme $y_\rho + b + a_\rho^0$ avec $a_\rho^0.r = 0$. Puisque $(x_\rho)_\rho$ est sans limite dans M , la suite $(v(x_\rho))_\rho$ est constante à partir d'un certain rang, ainsi que la suite $(v(x_\rho.r))_\rho$, qui prend la valeur ultime $v(a)$. Comme $(x_\rho.r)_\rho$ converge vers a on a pour tout ρ suffisamment grand, $v(x_\rho.r - a) > v(a)$ c'est à dire $v(y_\rho.r) > v(b.r)$. Puisque y_ρ est régulier pour r , $v(y_\rho) > v(b)$ pour ρ assez grand. De plus, le fait que b est régulier pour r entraîne que, pour tout $a_\rho^0 \in \text{ann}_{M^*}(r)$, on a $v(b + a_\rho^0) = \min\{v(b), v(a_\rho^0)\}$ pour ρ suffisamment grand. D'où $v(x_\rho) = v(b + a_\rho^0) < v(y_\rho)$ pour ρ assez grand. Mais, $(x_\rho)_\rho$ étant une suite pseudo-Cauchy, la suite des valuations des éléments $x_{\rho+1} - x_\rho = y_{\rho+1} - y_\rho + a_{\rho+1}^0 - a_\rho^0$ est strictement croissante. Puisque $\text{Saut}_M(r)$ est fini, on doit avoir nécessairement $v(a_{\rho+1}^0 - a_\rho^0) > v(y_{\rho+1} - y_\rho) = v(y_\rho)$ pour ρ assez grand. Si la suite $(a_\rho^0)_\rho$ devient constante alors on a fini, car dans ce cas la suite $(x_\rho)_\rho$ admet $b + a_{\rho_0}^0$ comme limite. Supposons que ce n'est pas le cas. Alors, pour tout ρ assez grand, on a $\max \text{Saut}_M(r) \geq v(a_{\rho+1}^0 - a_\rho^0) > v(y_\rho)$. Traitons le cas où $\text{Saut}_M(r) = \{\gamma_1, \gamma_2\}$ avec $\gamma_1 < \gamma_2$, le cas général se traite de même. On décompose chaque a_ρ^0 sur une même base valuation-indépendante de $\text{ann}_{M^*}(r)$ comme $a_\rho^0 = a_{\rho, \gamma_1}^0 + a_{\rho, \gamma_2}^0$ avec $v(a_{\rho, \gamma_1}^0) = \gamma_1$ et $v(a_{\rho, \gamma_2}^0) = \gamma_2$. On a $\gamma_2 > v(x_{\rho+1} - x_\rho) = v(y_\rho) > v(b)$ pour ρ assez grand. Alors, si $v(b) < \gamma_1$, b est limite de $(x_\rho)_\rho$. Si $\gamma_1 \leq v(b) < \gamma_2$ alors nécessairement $a_{\rho+1, \gamma_1}^0 = a_{\rho, \gamma_1}^0$ à partir du moment où $v(x_{\rho+1}) = v(x_\rho)$. Par conséquent, si on choisit ρ_0 suffisamment grand, $(x_\rho)_\rho$ converge vers $b + a_{\rho_0, \gamma_1}^0$.

2. Soit N_1 et N_2 deux extensions de M incluses respectivement dans deux extensions immédiates maximales de M_1 et M_2 de M . Supposons que N_1 et N_2 sont isomorphes au-dessus de M , disons via $f : N_1 \rightarrow N_2$. Par le lemme de Zorn, il suffit de pouvoir prolonger f à un sous-module de M_1 contenant M et un élément de $M_1 \setminus N_1$. Comme ci-dessus il est clair que l'on peut supposer $N_1 = N_2 = M$ et f l'identité. On peut de plus supposer M affinement maximal par le point 1. Soit $x \in N_1 \setminus M$. Alors x est limite d'une suite pseudo-Cauchy de type transcendant sans limite dans M . Cette même suite admet une limite $y \in M_2$ et par le lemme 4.3.16, $M_1 \oplus x.R$ et $M_2 \oplus y.R$ sont isomorphes au-dessus de M , ce qu'il fallait montrer. ■

4.8 Un théorème de structure

Durant toute cette section, sauf mention contraire, (M, v) désignera un module résiduellement divisible et maximal. De plus on supposera que dans (M, v) chaque $r \in R \setminus \{0\}$ a un nombre fini de racines. Par 4.5.14 on sait que tout sous-module divisible de M contenant M_{tor} est affinement maximal.

Par la suite on supposera que φ est un automorphisme de K . On rappelle que, dans ce cas, R est aussi euclidien à gauche; en particulier c'est un anneau d'Ore à gauche. On remarquera également que si K est de caractéristique $p > 0$ alors, en notant K_p sa clôture parfaite, la structure de $K_p[t, x \mapsto x^p]$ -module de K_p est induite par la structure de $K[t, \mapsto x^p]$ -module de K_p .

Notre résultat impliquera en particulier que si K est un sous-corps parfait d'un corps de Kaplansky (U, v) , qui est maximal, alors, en tant que $K[t; x \mapsto x^p]$ -module U s'écrit comme $K_{imm}^{alg} \oplus U'$, où K_{imm}^{alg} est une extension immédiate maximale de la clôture algébrique de K dans U , U' est un sous-module régulier divisible de U et où K_{imm}^{alg} et U' sont en somme valuation indépendante.

Rappelons que l'on désigne par D , le corps des fractions de R . Notons d'abord une observation simple qu'on a déjà utilisé plusieurs fois localement.

Lemme 4.8.1. *Soit a un élément régulier de M . Alors $a.R$ a une clôture divisible régulière, unique à isomorphisme de module valué près.*

PREUVE. Par le lemme 4.5.16 le sous-module $a.R$ est régulier. Soit N un sous-module sans torsion de M contenant $a.R$. Remarquons d'abord la chose suivante :

Si $z \in a.R$ est non-divisible dans N par un certain $0 \neq r' \in R$, alors il existe $q \in R \setminus \{0\}$ tel que a est non divisible par q dans N :

On écrit $a.r = z$ avec $r \in R \setminus \{0\}$. Puisque R est un anneau d'Ore à gauche, il existe $q, q' \in R$ tels que, $qr = q'r'$. Alors a est non-divisible dans N par q . En effet sinon soit $z' \in N$ tel que $z'.q = a$. Il vient $z = (z'.q).r = z'.qr = z'.q'r' = (z'.q').r'$: i.e. z est divisible par r' dans N . Contradiction.

Le paragraphe ci-dessus implique en particulier que N contient une clôture divisible de $a.R$ si et seulement si a est divisible dans N par tout $r \in R \setminus \{0\}$, si et seulement si a divisible dans N par tous les polynômes premiers et par t .

On procède par induction. Énumérons l'ensemble $\{p \in R \mid p \text{ premier } p\} \cup \{t\}$, à K -conjugaison près (cf chapitre 2). comme $(p_\alpha)_{\alpha < \kappa}$. On va construire une chaîne d'extensions $X_{\alpha < \kappa}$ telle que dans X_α a est divisible par p_β pour tout $\beta \leq \alpha$.

Puisque $a.R$ est sans-torsion, a n'est divisible dans $a.R$ par aucun des p_α . Soit $x_0 \in M$ régulier pour p_0 tel que $x_0.p_0 = a$. Par le point 2. du lemme 4.5.16 x_0 est régulier. On pose $X_0 := x_0.R$ qui est un sous-module régulier aussi par 4.5.16. Remarquons maintenant que a est divisible par p_1 dans X_0 si et seulement si x_0 est divisible par q_0 ; car, puisque R est aussi un anneau d'Ore à gauche, il existe $q_0, q_1 \in R \setminus \{0\}$ tels que $q_0 p_0 = q_1 p_1$. Soit $x_1 \in M$ régulier pour q_0 tel que $x_1.q_0 = x_0$. Alors $x_1.q_1 p_1 = a$ et donc a est divisible dans $x_1.R$ par p_1 . En

continuant ainsi, pour tout $n < \omega$, on définit $X_n \supseteq X_{n-1}$ de la forme $x_n.R$, avec a divisible par p_0, \dots, p_n dans X_n . Soit $X := \bigcup X_n$. Supposons que a n'est pas divisible par p_ω dans X . On va montrer que'il existe $x_\omega \in M$ régulier tel que $x_\omega.p_\omega = a$ et $X + x_\omega.R$ est régulier. Soit

$$Z := \{z \in M \mid z \text{ est régulier pour } p_\omega \text{ et } z.p_\omega = a\} = \{z_1, \dots, z_k\}.$$

Tous les $z_i.R$ contiennent $a.R$ et sont des sous-modules réguliers. Et puis comme ci-dessus, pour tout $n < \omega$, X_n a une extension régulière X'_n telle que, dans X'_n , a est divisible par $p_0, \dots, p_n, p_\omega$ et le type d'isomorphisme au dessus de X_n de X'_n est uniquement déterminé. Puisque Z est fini et $X_n \subset X_{n+1}$ ($n < \omega$), il existe un i_0 tel que tout X_n a une extension régulière contenant z_{i_0} . En particulier, pour tout n , $X_n + z_{i_0}.R$ est un sous-module régulier, c'est à dire, en posant $x_\omega := z_{i_0}$, $x_\omega.R + X$ est régulier et on pose $X_\omega := x_\omega.R + X$.

Plus généralement, si α est un ordinal limite, et si pour tout $\beta < \alpha$, X_β a une extension X'_β régulière dans laquelle a est divisible par p_α , alors, pour un certain x_α régulier tel que $x_\alpha.p_\alpha = a$, $\bigcup_{\beta < \alpha} X_\beta + x_\alpha.R$ est régulier. Soit μ un ordinal successeur de la forme $\alpha + n$ avec $n < \omega$ et supposons que $X_{\alpha+n-1}$ est de la forme $(\bigcup_{\beta < \alpha} M_\beta) + x_{\alpha+n-1}.R$. Si a n'est pas divisible dans $M_{\alpha+n-1}$ par $p_{\alpha+n}$, alors $x_{\alpha+n-1}$ n'est divisible pas par un certain $p'_{\alpha+n}$. Donc, comme ci-dessus, il existe un $x_{\alpha+n}$ vérifiant $x_{\alpha+n}.p'_{\alpha+n} = x_{\alpha+n-1}$, régulier et tel que tout M_β a une extension régulier contenant $x_{\alpha+n}$. On continue alors en posant $X_{\alpha+n} = M_\alpha + x_{\alpha+n}.R$.

Enfin l'unicité est affirmée par 4.6.9. ■

Le résultat suivant est une sorte de réciproque au corollaire 4.4.25.

Lemme 4.8.2. *Toute extension immédiate d'un sous-module régulier N de M est régulière. De plus, si N est un sous-module divisible de M et si $N' := N \oplus x.R$ est une extension immédiate de N , alors les clôtures divisibles régulières de N' en sont des extensions immédiates.*

PREUVE. Soit $N \subset A \subset M$ avec N régulier et A une extension immédiate de N . Soit $x \in A \setminus N$ que l'on suppose irrégulier pour un certain $0 \neq r \in R$. Prenons une suite pseudo-Cauchy de N , $(x_\gamma)_{\gamma < \lambda}$ convergeant vers x et sans limite dans N . Alors, pour γ suffisamment grand on devrait avoir $v(x - x_\gamma) > v(x) = v(x_\gamma)$. Or, par le corollaire 4.5.18, puisque x_γ est régulier mais x irrégulier on a $v(x - x_\gamma) = v(x)$. Contradiction.

Alors l'extension immédiate affine affinement maximale de N' est régulière. Elle est de plus divisible par 4.5.9. C'est une clôture divisible de N car c'est une extension affine. ■

Lemme 4.8.3. *Soit $N \subset M$ un sous-module régulier divisible et z un élément de M vérifiant pour un certain $z_0 \in M_{\text{tor}} \oplus N$, $v(z - z_0) = \max\{v(z - z') \mid z' \in M_{\text{tor}} \oplus N\}$. Alors avec $x := z - z_0$, $N + x.R$ est régulier. De plus, pour toute clôture divisible régulière $\langle x \rangle^{\text{div}}$ de $x.R$, $N \oplus \langle x \rangle^{\text{div}}$ est régulier.*

PREUVE. Notons $L = M_{\text{tor}} \oplus N$. Par le lemme 4.5.19, x est régulier et les modules L et $x.R$ sont valuation-indépendants. De plus $N \oplus x.R$ est régulier. En effet, soit $x.r + y$ que l'on

suppose irrégulier avec $y \in N$. Remarquons que, puisque y et $x.r$ sont tous les deux réguliers, si $v(x.r) > v(y)$, ou $v(x.r) < v(y)$ alors $x.r + y$ est régulier. Sinon $v(x.r) = v(y) = v(x.r + y)$ par la valuation indépendance de L et $x.R$. Puisque $x.r + y$ est irrégulier, pour un certain $y_0 \in M_{tor}$ on a $v(x.r + y - y_0) > v(x.r + y) = v(x.r)$. Ceci est contradictoire avec le fait que L et $x.R$ soit valuation-indépendants.

Maintenant soit $\langle x \rangle^{div}$ une clôture divisible régulière de $x.R$. Soit $y \in \langle x \rangle^{div}$. Soit $z \in L$ de même valuation que y et q le polynôme minimal de y sur $x.R$. On a $v((y-z).q) = v(y.q - z.q) = \min\{v(y.q), v(z.q)\} = v(y.q) = v(y) \cdot q$. Donc $v(z - y) = v(z) = v(y) = \min\{v(z), v(y)\}$. C'est-à-dire que L et $\langle x \rangle$ sont en somme valuation-indépendante. Cela montre alors comme ci-dessus que $N \oplus \langle x \rangle^{div}$ est régulier. \blacksquare

Théorème 4.8.4. *Supposons que (M, v) est un module valué maximal et résiduellement divisible. Alors M s'écrit comme $M_{tor}^* \oplus N$, où N un sous-module régulier de M , M_{tor}^* une extension immédiate maximale de M_{tor} et où la somme est valuation-indépendante.*

PREUVE. Après avoir (partiellement) ordonné par l'inclusion les sous-modules divisibles réguliers de M , on peut en choisir un qui est maximal. Appelons-le N comme dans l'énoncé. Par maximalité de M contient une extension immédiate maximale M_{tor}^* de M_{tor} . Par le lemme 4.5.16 M_{tor} et N sont en somme valuation-indépendante, donc également M_{tor}^* et N . Supposons $M \neq M_{tor}^* \oplus N$. Il existerait $z' \in M \setminus (M_{tor}^* \oplus N)$ et on va montrer qu'il existerait N' contenant strictement N , régulier, divisible et tel que $M_{tor}^* \oplus N' \ni z'$, et aboutir ainsi à une contradiction. Puisque $z' \notin M_{tor}^*$, il existe $y_0 \in M_{tor}^*$ tel que $v(z' - y_0) = \max\{v(z' - y') \mid y' \in M_{tor}^*\}$. On pose $z := z' - y_0$. En particulier z est régulier.

(1) Si $z.R + N$ est une extension immédiate de N , alors par le lemme 4.8.2 z est régulier et $N \oplus z.R$ a une extension régulière divisible. Contradiction. Donc on a fini.

(2) Si $z.R$ n'est pas immédiate sur N et si $z - z''$ est régulier pour tout $z'' \in N$, alors, pour tous $z'' \in N$ et $z_0 \in M_{tor}$, $v(x - z'' - z_0) = \min\{v(z - z''), v(z_0)\} \leq v(z - z'')$. Puisque $z.R$ n'est pas immédiate sur N , il existe un $z_d \in N$ tel que, $v(z - z_d) = \max\{v(z - z'') \mid z'' \in N\}$. En posant $x := z - z_d$, $v(x) = \max\{v(x - y') \mid y' \in M_{tor} \oplus N\}$. Alors par le lemme 4.8.3 pour toute clôture divisible régulière $\langle x \rangle^{div}$ de x , $N \oplus \langle x \rangle^{div}$ est régulier. Donc on a fini.

(3) Si on n'est pas dans les cas précédents, alors $z.R$ n'est pas immédiate sur N et il existe $z_{rg}^0 \in N$ tel que $z - z_{rg}^0$ est irrégulier pour un certain r_0 . D'où il existe un $z_{tor}^0 \in M_{tor}^*$ tel que, $v(z - z_{rg}^0 - z_{tor}^0) = \max\{v(z - y') \mid y' \in M_{tor}^*\} > v(z - z_{rg}^0) = v(z_{tor}^0)$. En effet on peut supposer $z_{tor}^0 \in M_{tor}$ car $z - z_{rg}^0$ n'est pas limite sur M_{tor} par hypothèse. Donc $z - z_{rg}^0 - z_{tor}^0$ est régulier, $v(z) = v(z_{rg}^0)$ (car sinon $z - z_{rg}^0$ serait régulier) et $v(z_{rg}^0) \leq v(z_{tor}^0)$. En particulier $z_0 := z_{rg}^0 + z_{tor}^0$ est régulier et $v(z_0) = \min\{v(z_{rg}^0), v(z_{tor}^0)\} = v(z_{rg}^0)$. On teste les étapes 1 et 2 ci-dessus avec l'élément régulier $z - z_0$, qui est de valuation $> v(z)$. Si elles ne sont pas vérifiées il existe $z'_{rg} \in N$ et $z'_{tor} \in M_{tor}$ comme ci-dessus. Il vient, avec $z'_{tor} := z_{tor}^0 + z'_{tor}$,

$$z_{rg}^1 := z_{rg}^0 + z'_{rg} \text{ et } z_1 := z_{tor}^1 + z_{rg}^1 :$$

$$v(z - z_1) > v(z - z_0) ; \quad v(z_{rg}^0 - z_{rg}^1) > v(z_{rg}^0) \quad \text{et} \quad v(z_{tor}^1 - z_{tor}^0) > v(z_{tor}^0).$$

On itère le processus. Si on n'entre pas dans le cas 1 ou 2 en une étape finie, on obtient des suites pseudo-Cauchy $(z_{tor}^i)_{i < \omega}$ de M_{tor} , $(z_{rg}^i)_{i < \omega}$ de N et $(z_i = z_{tor}^i + z_{rg}^i)_{i < \omega}$. Alors z est clairement une limite de $(z_i)_i$. Soit $z_{tor}^* \in M_{tor}^*$ une limite de $(z_{tor}^i)_i$. Alors $z - z_{tor}^*$ est une limite de la suite $(z_{rg}^i)_i$. En effet il suffit d'écrire :

$$v(z - z_{tor}^* - z_{rg}^i) = v(z - z_i + (z_{tor}^i - z_{tor}^*)).$$

Si la suite $(z_{rg}^i)_i$ n'a pas de limite dans N on a terminé : par le lemme 4.8.3 $N \oplus (z - z_{tor}^*)$ est régulier. Sinon on pose $z_\omega = z - z_{tor}^* - z_{rg}^*$, avec $z_{rg}^* \in N$ une limite de $(z_{rg}^i)_i$, et on continue avec z_ω .

Ce processus doit terminer, puisque la cardinalité d'une suite pseudo-Cauchy de M est bornée par la cardinalité de $v(M)$. ■

Chapitre 5

$K[t; \varphi]$ -modules C-minimaux

Dans ce chapitre les modules valués (trivialement, K -trivialement et K -non trivialement) sont considérés dans le formalisme des C-relations. Une C-relation est une relation ternaire satisfaisant les axiomes suivants :

1. $\forall x, y, z \ C(x, y, z) \rightarrow C(x, z, y)$,
2. $\forall x, y, z \ C(x, y, z) \rightarrow \neg C(y, x, z)$,
3. $\forall x, y, z, w \ C(x, y, z) \rightarrow (C(w, y, z) \vee C(x, w, z))$,
4. $\forall x, y \ x \neq y \rightarrow C(x, y, y)$.

Une C-relation interprète toujours un arbre (cf. [AdNe]) : pour des chaînes maximales x, y et z , $C(x, y, z)$, exprime que y et z branchent au-dessus de là où x et y (ou z) branchent. Une distance ultramétrique induit la C-relation

$$C(x, y, z) \Leftrightarrow d(x, y) = d(x, z) > d(y, z).$$

Donc un groupe abélien ou un corps valué porte en particulier la C-relation canonique

$$C(x, y, z) \Leftrightarrow v(x - y) = v(x - z) < v(y - z).$$

Une valuation triviale, c'est-à-dire prenant au plus deux valeurs, induit la C-relation triviale définie comme : $C(x, y, z) \Leftrightarrow x \neq y = z$.

La notion de C-minimalité, introduite dans [MacSt] et [HaMac], est un analogue de l'ordinalité¹.

Définition 5.0.5. On dit qu'une expansion $\mathcal{U} = (U, C, \dots)$ d'une C-relation est C-minimale si, pour tout $\mathcal{U}' = (U', C, \dots)$, élémentairement équivalente à \mathcal{U} , tout sous-ensemble définissable (avec paramètres) de U' , est définissable sans quantificateur en n'utilisant que la relation ternaire C.

Remarque 5.0.6. En présence d'une distance ultramétrique, la C-minimalité se traduit par le fait que tout sous-ensemble (de la structure elle-même) définissable est une combinaison booléenne de boules «ouvertes» ou «fermées».

1. Noter que la définition que l'on vient de donner n'inclut pas l'axiome ci-dessous, dit de densité, classiquement admis dans les publications comme [MacSt] et [AdNe] :

$$\forall xy \ x \neq y \rightarrow \exists z \neq y \ C(x, y, z),$$

mais le remplace par l'axiome 4.

Le groupe additif de \mathbb{Q}_p , muni de sa valuation p -adique, est C-minimal mais le corps \mathbb{Q}_p ne l'est pas, par exemple l'ensemble des carré n'y est pas définissable sans quantificateur dans le langage des corps valués, donc dans le langage des corps équipés de la C-relation non plus. De fait, un corps valué est C-minimal si et seulement s'il est algébriquement clos (cf. [HaMac]).

Une structure $\mathcal{M} = (M, \dots)$ est appelée fortement minimale si pour tout M' élémentairement équivalent à M , tout sous-ensemble définissable de M' avec des paramètres, est fini ou cofini (i.e définissable sans quantificateur en n'utilisant que l'égalité); elle est appelée o-minimale si c'est une structure totalement ordonnée et telle que tout sous-ensemble définissable de M est une union finie d'intervalles². La C-minimalité apparaît comme une généralisation commune de la minimalité forte et de l'o-minimalité. Par exemple, une structure munie de la C-relation triviale est C-minimale si et seulement si elle est fortement minimale. Plus généralement ces trois notions sont étroitement liées. Notons également que les théories C-minimales sont dépendantes, i.e elles ont la propriété NIP, comme les théories fortement minimales, o-minimales et p-minimales (on pourra consulter [Mac] pour les définitions des théories o-minimales, C-minimales et p-minimales, dont le théorème 4.2.6 et la discussion qui le précède pour le résultat concernant NIP).

Dans ce chapitre, on va caractériser les R -modules valués C-minimaux. Les résultats se résument dans les trois théorèmes ci-dessous.

Théorème 5.0.7. *Un R -module trivialement valué infini M est C-minimal (i.e. fortement minimal dans ce cas, justifiant la notation M , à la place de (M, v)) si et seulement si l'une des conditions ci-dessous est vérifiée :*

1. M est divisible et, pour tout $r \in R \setminus \{0\}$, $\text{ann}_M(r)$ est fini
2. l'idéal annulateur de M , $\{q \in R \mid x.q = 0, \forall x \in M\}$, est engendré par un polynôme premier r , R/rR est un corps et M est un (R/rR) -espace vectoriel.

Rappelons que $L_V = \{<, (\cdot r)_{r \in R}, \infty\}$, $L'_V = L_V \cup \{(R_n)_{n \in \mathbb{N}}\}$, $L'_{V_0} = \{<, \tau, \infty, (R_n)_{n \in \mathbb{N}}\}$ et que par la remarque 4.1.8 la L'_{V_0} -structure $v(M)$ d'un module K -trivialement valué et non-trivialement valué (M, v) est une R -chaîne telle que la valuation induite v_K sur K soit triviale. Cela permet d'énoncer les deux résultats suivants dans le formalisme du chapitre 4.

Théorème 5.0.8. *Soit (M, v) un module K -trivialement valué infini et non-trivialement valué. Alors (M, v) est C-minimal si et seulement si $v(M)$ est o-minimal dans le langage L'_V , pour tout $r \in R \setminus \{0\}$, $\text{ann}_M(r)$ est fini, (M, v) est henselien et si l'une des conditions ci-dessous est vérifiée :*

1. (M, v) est divisible,
2. $M_{>\theta.t}$ contient une boule d'indice fini et $M = M_{\text{tor}} \oplus M_{>\theta}$, où M_{tor} est divisible et fortement minimal s'il n'est pas fini.

Théorème 5.0.9. *Soit (M, v) un module valué non K -trivialement. Alors il est C-minimal si et seulement s'il est affinement maximal, résiduellement divisible et tel que $v(M)$ soit une L_V -structure o-minimale.*

2. Pour nous, un intervalle de M est un sous-ensemble convexe de M ayant des bornes dans $M \cup \{-\infty, \infty\}$. En particulier tout segment initial (ou final) et tout singleton de M est considéré comme un intervalle. Si on modifie cette définition, en remplaçant le mot «intervalles» par le mot «convexes», on obtient la définition d'une structure faiblement o-minimale. Noter que si une structure est o-minimale, alors il va de même pour sa théorie complète, i.e. toute structure qui lui est élémentairement équivalente est o-minimale. Cette dernière propriété est fautive pour les structures fortement minimales (et par voie de conséquence pour les structures C-minimales) ou faiblement o-minimales (cf. [Mac] section 4).

5.1 Cas fortement minimal

Lemme 5.1.1. *Si M est un module fortement minimal infini sur un anneau S quelconque, alors, pour tout $r \in S \setminus \{0\}$,*

$$\text{ann}_M(r) \text{ fini} \Leftrightarrow (M.r \neq 0) \Leftrightarrow M.r = M.$$

PREUVE. Pour tout $r \in S \setminus \{0\}$, $\text{ann}_M(r)$ et $M.r$, étant définissables, sont finis ou cofinis. Étant des sous-groupes, ils ne peuvent être cofinis propres. Si tous les deux sont finis, en considérant l'application $M \rightarrow M, x \mapsto x.r$, qui a comme noyau $\text{ann}_M(r)$, on devrait avoir M fini. Donc la seule possibilité restante est celle qui est énoncée. ■

Lemme 5.1.2. *Soit I un idéal bilatère non nul de R . Si $\varphi^n = 1$ pour un certain $n \in \mathbb{N}$, alors il existe q à coefficients dans $\text{Fix}(\varphi)$ (i.e. $q \in \text{Fix}(\varphi)[t]$) tel que $I = q(t^n)R$. Si φ n'est pas d'ordre fini, alors I est de la forme $t^k R$ pour un certain $k \in \mathbb{N}$.*

PREUVE. Voir la proposition 2.2.8 dans [Co]. ■

Corollaire 5.1.3. *Soit (M, v) un module valué trivialement, infini et fortement minimal. Soit $I = \{r \in R \mid M.r = 0\}$. Alors, ou bien $I = \{0\}$ et dans ce cas M est divisible et les annulateurs $\text{ann}_M(r)$ sont finis, ou bien $I \neq \{0\}$ et dans ce cas, $I = rR$ pour un $r \in R$ premier et M est un R/rR -espace vectoriel.*

PREUVE. Le cas où $I = \{0\}$ découle du lemme 5.1.1. Supposons donc $I \neq \{0\}$. Remarquons que I est un idéal bilatère et que, par le lemme 5.1.2, il existe $r \in K_0[t; \varphi]$ (rappelons que $K_0 = \text{Fix}(\varphi)$) tel que $I = rR$. Soit d le degré de r . Alors pour tout q de degré $< d$ vérifiant $r = qs$ on a $M.q \neq 0$ d'où par 5.1.1, $M.q = M$. Par conséquent $M.r = M.qs = M.s = 0$, d'où $s \in I$. Donc $q \in K$. C'est-à-dire que r est premier. Par l'existence du ppcm, et par le théorème de Bézout, le quotient R/rR est un corps. ■

Lemme 5.1.4. *Si M est un R -module fortement minimal, si l'action de t est injective et si φ n'est pas d'ordre fini, alors l'idéal I ci-dessus est nul.*

PREUVE. Si φ n'est pas d'ordre fini et si $I \neq \{0\}$, par le lemme 5.1.2, I est engendré par t^k , pour un certain $k \in \mathbb{N}_{>0}$. Puisque la multiplication par t est injective ceci n'est pas possible.

Remarque 5.1.5. Rappelons que dans notre définition d'un module valué, t agit nécessairement injectivement.

Preuve du théorème 5.0.7. Par ce qui précède il suffit de montrer qu'un R -module satisfaisant 1 ou 2 est fortement minimal. Si M est un R -module satisfaisant 1, alors, par 1.1.2, et par la proposition, 2.2.1, toute partie définissable de M est finie ou cofinie. Si M satisfait 2, alors la structure de R -module sur M coïncide avec sa structure de R/rR -espace vectoriel. Or un espace vectoriel est fortement minimal. ■

5.2 Interlude : conséquences de la C-minimalité

Comme on l'a remarqué, la définition originale incluait l'axiome de densité, mais cette propriété n'intervient pas dans la démonstrations des résultats classiques ci-dessous.

On utilisera très fréquemment la proposition ci-dessous.

Proposition 5.2.1. *Si G est un groupe valué C-minimal alors, pour tout sous-groupe définissable infini propre F de G , il existe $\gamma \in v(G)$, tel que F contient $G_{\geq \gamma}$ (ou $G_{> \gamma}$), et $G_{\geq \gamma}$ (ou $G_{> \gamma}$) est d'indice fini dans F .*

PREUVE. Voir [MacSt] ou [Sim] 1.6(ii). ■

Proposition 5.2.2. *Soit $\mathbb{G} = (G, v, \dots)$ un groupe valué, porteur de structure additionnelle, et C-minimal. Alors*

1. *pour tout $\gamma \in v(G)$, le groupe $G_{\geq \gamma}/G_{> \gamma}$ muni de la structure induite par \mathbb{G} est fortement minimal,*
2. *la chaîne $v(G)$ munie de la structure induite par \mathbb{G} est o-minimale.*

PREUVE. Voir [MacSt].

Corollaire 5.2.3. *Soit (M, v) un R -module valué C-minimal. Alors,*

1. *pour tout $\gamma \in v(M)$, $M_{\geq \gamma}/M_{> \gamma}$ est un (K/v_K) -espace vectoriel fortement minimal et,*
2. *la R -chaîne $v(M)$ est o-minimale.*

Définition 5.2.4. On dira qu'un groupe (ou module) valué (M, v) est non trivialement valué si $v(M)$ n'est pas de la forme $\{\gamma, \infty\}$.

Remarque 5.2.5. Dans le point 1 ci-dessus, si (M, v) est K -trivialement valué, i.e. si v_K est triviale, alors $K/v_K = K$ et donc tout $M_{\geq \gamma}/M_{> \gamma}$ est un K espace-vectoriel.

5.3 Cas d'une valuation non triviale et K -triviale

Une des implications du théorème 5.0.8 est contenue dans la proposition suivante, qui découle du théorème 3.3.7.

Proposition 5.3.1. *Si (M, v) est un module K -trivialement valué divisible hensélien, si pour tout $q \in R \setminus \{0\}$, $\text{ann}_M(q)$ est fini et si $v(M)$ est o-minimal dans le langage L'_V , alors (M, v) est C-minimal.*

PREUVE. Nous renvoyons à la preuve de la proposition 5.4.1 dont la présente proposition n'est qu'un cas particulier. ■

Lemme 5.3.2. *Soit (M, v) un module K -trivialement valué, tel que*

1. *M_{tor} est fini et $M = M_{\text{tor}} \oplus M_{> \theta}$, et*
2. *$M_{> \theta}$ est divisible et $v(M)$ est o-minimal.*

Alors (M, v) est C-minimal.

PREUVE. Si $M_{tor} = 0$ alors, $M = M_{>\theta}$ est divisible henselien donc C-minimal par la proposition précédente. Sinon, soit N' une clôture divisible de M_{tor} . Posons $N := N' \oplus M_{>\theta}$ et on étend v à N en posant $v(x_{tor} + x_{>\theta}) = \theta$ si x_{tor} est non nul. D'où (N, v) est divisible henselien et $v(N) = v(M)$, donc (N, v) est C-minimal, toujours par la proposition précédente. Alors $M = \bigcup_{a \in M_{tor}} M_{>\theta} + a$, est une union finie de boules de N , par conséquent il est C-minimal. ■

Une conséquence immédiate des deux résultats précédents est :

Corollaire 5.3.3. *L'anneau de valuation d'un corps de caractéristique $p > 0$, parfait, muni d'une valuation henselienne, de corps résiduel fini ou p -clos, et de groupe de valuation divisible, est C-minimal en tant que $\mathbb{F}_p[t; x \rightarrow x^p]$ -module valué.*

PREUVE. Un groupe abélien ordonné divisible est o-minimal, donc a fortiori sa restriction à la structure de $\mathbb{F}_p[t; x \rightarrow x^p]$ -chaîne. Le corollaire découle donc du lemme 3.2.2 avec la proposition 5.3.1 si le corps résiduel est p -clos et avec le lemme 5.3.2 si le corps résiduel est fini. ■

Exemple 5.3.4. Soit $R = \mathbb{F}_p[t; x \mapsto x^p]$. L'anneau des séries de Puiseux sur F_p ou sur un corps p -clos est C-minimal en tant que R -module valué mais le corps des séries de Puiseux ne l'est pas.

Le lemme ci-dessous, avec le résultat du lemme précédent, montreront que la condition 2. cité dans le théorème 5.0.8, implique la C-minimalité.

Lemme 5.3.5. *Soit (M, v) un module K -trivialement valué henselien et tel que*

1. M_{tor} est fini et $M = M_{tor} \oplus M_{>\theta}$,
2. $M_{>\theta}.t$ contient une boule de la forme $M_{\geq\gamma}$ ou $M_{>\gamma}$, qui est d'indice fini dans $M_{>\theta}.t$ et $v(M_{>\theta})$ est o-minimal.

Alors (M, v) est C-minimal.

PREUVE. Si $M_{>\theta}$ est divisible, alors l'assertion suit de lemme ci-dessus.

Montrons d'abord que la valuation sur $M_{>\theta}$ détermine une et une seule valuation sur chacune de ses clôtures divisibles (toutes isomorphes en tant que modules). Soit N une clôture divisible de $M_{>\theta}$. Alors, puisque $M_{>\theta}$ est divisible par tous les polynômes séparables, $x \in N$ si et seulement si $x.t^n \in M_{>\theta}$ pour un certain $n \in \mathbb{N}$. Soit alors $x \in N \setminus M_{>\theta}$ et n minimal tel que $x.t^n \in M_{>\theta}$. Soit $\gamma = v(x.t^n)$. On définit $\bar{v}(x)$ comme le couple (γ, n) . Si $y \in N \setminus M_{>\theta}$ est tel que $\bar{v}(y) = (\delta, k)$, on décrète que $\bar{v}(x) < \bar{v}(y)$ si et seulement si $\tau^k(\gamma) < \tau^n(\delta)$. Il est immédiat de vérifier que (N, \bar{v}) est un module K -trivialement valué, et que \bar{v} prolonge v .

Montrons maintenant que $M_{>\theta}$ s'identifie à une union finie de boules de (N, \bar{v}) . Soit B la boule de M , d'indice fini dans $M_{>\theta}.t$, dont l'existence est donnée par l'hypothèse du corollaire. Montrons que B est en fait une boule de N . Soit γ le rayon de B , i.e. $B = M_{>\gamma}$ ou $B = M_{\geq\gamma}$. Soit $x \in N \setminus M_{>\theta}$, avec $v(x) > \gamma$, et soit $k \geq 1$ minimal tel que $\bar{x}.t^k \in M_{>\theta}$. On a, $v(x.t^k) > \tau^k(\gamma) > \gamma$. Or $M_{>\theta}.t \supset B$ implique $x.t^{k-1} \in M_{>\theta}$. Contradiction. D'où $B = N_{\geq\gamma}$ ou $B = N_{>\gamma}$. En écrivant $M_{>\theta}.t = \bigcup_i B + a_i$, on a $M_{>\theta} = B.t^{-1} + a.t^{-1}$, où $B.t^{-1}$ est nécessairement la

boule ouverte ou fermée de rayon $\tau^{-1}(\gamma)$ et $a_i.t^{-1}$ est l'unique $b_i \in N$ tel que $b_i.t = a_i$. Par conséquent, $M_{>\theta}$ est une union finie de boules de N donc M est une union finie de boules de $N \oplus M_{tor}$ et il suffit de montrer que $N \oplus M_{tor}$ est C-minimal. Puisque (N, \bar{v}) est divisible henselien sans-torsion, le lemme 5.3.2 dit qu'il suffit de montrer que $\bar{v}(N)$ est o-minimal.

Montrons d'abord que $\bar{v}(N)$ est la clôture de $v(B)$ par τ^{-1} . Soit $x \in M_{>\theta}$, tel que $x.t \notin B$. On a $v(x.t - a_i) > v(x.t) = v(a_i)$ pour un certain $i \in \{1, \dots, n\}$. Dans ce cas, $v(x.t^2) > v(x.t)$ et donc pour tout i , $v(x.t^2 - a_i) = v(a_i)$. Alors $x.t^2 \in B$ nécessairement. Par ailleurs, si $x.t \in B$ de même pour $x.t^2$. Donc N est aussi la clôture divisible de B . D'où $\bar{v}(N)$ est la clôture de $v(B)$ par τ^{-1} , $\bar{v}(N) = \bigcup_{i \in \mathbb{N}} \tau^{-i}v(B)$, et chaque $\tau^{-i}v(B)$ est isomorphe à $v(B)$ donc ils sont tous o-minimaux. Puisque $v(M)$ est o-minimal $v(M) \setminus \{\theta, \infty\}$ est dense ou discret : Soit DE l'ensemble des points ayant un voisinage dense et DI l'ensemble des points ayant un prédécesseur et un successeur ; par o-minimalité, $v(M)$ se partitionne comme $DE \cup DI \cup F$, avec F fini, plus précisément DE et DI sont des unions finies d'intervalles séparés par au moins un point de F ; par ce que τ est strictement croissant, il préserve chacun des trois ensembles, DE , DI et F , et parce qu'il n'admet aucun point fixe sur $v(M) \setminus \{\theta, \infty\}$, $F \setminus \{\theta, \infty\} = \emptyset$, par conséquent $v(M) \setminus \{\theta, \infty\} = DE$ ou $v(M) \setminus \{\theta, \infty\} = DI$.

Maintenant, par [PiSt], si $v(M)$ est discret alors τ est une translation sur $v(M)$ et donc $\bar{v}(N)$ est discret et τ reste une translation. Sinon si $v(M)$ est dense, par construction $\bar{v}(N)$ est dense. Dans le deux cas, la $\bar{v}(N)$ est une D -chaîne (au sens de la définition 4.1.1) et est o-minimal par le corollaire 1.16 de [Maa]. ■

Les lemmes qui suivent montrent établissent des réciproques aux résultat ci-dessus et ainsi complètent la preuve du théorème 5.0.8.

Lemme 5.3.6. *Soit (M, v) un module K -trivialement valué, C-minimal, infini. S'il existe $a \in M$ tel que $v(a) < \theta$ alors M est divisible.*

PREUVE. Soit $q \in R$, non nul. S'il existe un $a \in M$ comme ci-dessus, alors $v(M.q)$ n'a pas de premier élément. Si $M.q \neq M$ alors par la proposition 5.2.1 il contient un sous-groupe H de la forme $M_{\geq \gamma}$ ou de la forme $M_{> \gamma}$ qui est d'indice fini dans $M.q$. Alors $M.q$ est la réunion disjointe finie des $H + a_i$ et donc $v(M.q)$ a un premier élément. Contradiction. ■

Lemme 5.3.7. *Soit (M, v) un module non trivialement valué qui est K -trivialement valué et C-minimal. Alors, pour tout $r \in R \setminus \{0\}$, $\text{ann}_M(r)$ est fini.*

PREUVE. Si $\text{ann}_M(r)$, est une partie propre infini de M , alors par la proposition 5.2.1 il existe $\gamma \in \Delta$ tel que $\text{ann}_M(r)$ contient une boule de la forme $M_{\geq \gamma}$ ou $M_{> \gamma}$ qui est d'indice fini dans $\text{ann}_M(r)$. Comme $v(\text{ann}_M(r)) = \{\theta\}$, on obtient $\gamma = \theta$; dans ce cas là, on a nécessairement $M_{>\theta} = 0$ et donc $\text{ann}_M(r) = M_{\geq \theta} = M_{tor}$. Cela implique en particulier ∞ est l'unique élément qui est strictement $> \theta$. Puisque (M, v) est non trivialement valué, il existe donc des éléments de valuation $< \theta$. Par le lemme ci-dessus M est alors divisible ; d'où M_{tor} est divisible. Or ceci contredit le fait que M_{tor} est annulé par un seul élément. ■

Corollaire 5.3.8. *Soit (M, v) non trivialement valué, K -trivialement valué et C -minimal. Si M_{tor} est infini alors M_{tor} est divisible et fortement minimal.*

PREUVE. M_{tor} se plonge dans le R -module $M_{\geq \theta}/M_{> \theta}$ qui est fortement minimal, on a la divisibilité de $M_{\geq \theta}/M_{> \theta}$ par le lemme ci-dessus et par le lemme 5.1.1, d'où la divisibilité de M_{tor} . Alors par le lemme 2.2.1, tout sous-ensemble définissable de M_{tor} est une combinaison booléenne d'ensembles du type $\text{ann}_M(r)$, avec $r \in R \setminus \{0\}$. D'où, par le théorème 5.1.1, la forte minimalité de M_{tor} par le fait que chaque annulateur est fini. \blacksquare

Lemme 5.3.9. *Soit (M, v) un module K -trivialement valué C -minimal. Alors (M, v) est henselien.*

PREUVE. On va considérer 2 cas :

a. $v(M_{> \theta})$ n'a pas de premier élément. Par la proposition 5.2.1, si $M_{> \theta}.r$ ($r \in R \setminus 0$) n'est pas égal à $M_{> \theta}$, alors il contiendrait une boule ouverte ou fermée d'indice fini. En particulier, ou bien $v(M_{> \theta}.r)$ aurait un plus petit élément ou bien pour un certain $\gamma > \theta$ on aurait $M_{> \theta}.r = M_{> \gamma}$. Ces deux cas sont impossibles car si r est séparable et $x \in M_{> \theta}$, on a $v(x.r) = v(x)$.

b. $v(M_{> \theta})$ a un plus petit élément. Soit γ_0 ce plus petit élément $> \theta$. Soit $s \in R_{sep}$. Écrivons s comme $tq + a$ avec $a \in K$. Encore par le lemme 5.2.1, si $M_{> \theta}.s \neq M_{> \theta}$ alors il contient un certain $M_{> \gamma}$ ou $M_{\geq \gamma}$ qui est d'indice fini dans $M_{> \theta}.s$. Supposons que c'est $M_{> \gamma}$, l'autre cas se traite de même. Puisque $M_{> \gamma}$ est d'indice fini dans $M_{> \theta}.s$, il existe $\gamma_1, \dots, \gamma_k$ tel que $\gamma_0 < \gamma_1 < \dots < \gamma_k = \gamma$ avec γ_{i+1} le successeur de γ_i dans $v(M)$. Soit x de valuation γ_0 , alors $x_0 := (x - x.a^{-1}(tq + a)) = (x - x.a^{-1}s)$ est de valuation $\geq \gamma_1 > \gamma_0$. Ainsi on définit $x_i := (x_{i-1} - x_{i-1}.a^{-1}s)$, avec $v(x_i) > \gamma_i$, pour $1 \leq i \leq k$. Donc $v(x_k) > \gamma$. Par conséquent x_k est divisible par s , et donc x aussi. On a montré que $M_{> \theta}$ est divisible par les polynômes séparables, i.e. (M, v) est henselien. \blacksquare

Par ce qui précède, on peut supposer que $M = M_{\geq \theta}$ et que M_{tor} est fini. Il nous reste alors à montrer le résultat suivant, avec lequel s'achève la preuve du théorème 5.0.8.

Lemme 5.3.10. *Soit (M, v) un module K -trivialement valué C -minimal non divisible et tel que $M_{\geq \theta} = M$ et M_{tor} est fini. Alors $M = M_{tor} \oplus M_{> \theta}$.*

PREUVE. Puisque M_{tor} est fini la multiplication par t induit une bijection de M_{tor} . Donc $M_{tor} = \text{ann}_M(t^k - 1)$ pour un certain $k \in \mathbb{N} \setminus \{0\}$. Par conséquent, M_{tor} n'est pas divisible donc M non plus. Donc $M.(t^k - 1)$ contient une boule (ouverte ou fermée) qui y est d'indice fini, d'après le lemme 5.2.1. En particulier le quotient $M.(t^k - 1)/(M_{> \theta} \cap M.(t^k - 1))$ est fini ; de plus il est sans torsion. Or, puisque R est infini, le seul module sans torsion fini est le module 0. Cela implique que $M.(t^k - 1) \subset M_{> \theta}$. On a l'inclusion réciproque $M_{> \theta} \subset M.(t^k - 1) : (M, v)$ est henselien par le lemme ci-dessus ; en particulier $M_{> \theta}$ est divisible par le polynôme $t^k - 1$; cela implique que la suite ci-dessous est exacte (et clairement scindée) :

$$0 \longrightarrow M_{tor} \longrightarrow M \xrightarrow{.(t^k - 1)} (M_{> \theta}) \longrightarrow 0.$$

D'où $M_{>\theta}$ est facteur direct dans M . ■

5.4 Cas d'une valuation non K -triviale

Les propositions ci-dessous établissent la preuve du théorème.

Proposition 5.4.1. *Un module valué (M, v) affinement maximal, résiduellement divisible, ayant sa chaîne $v(M)$ o-minimale et tel que, pour chaque $r \in R \setminus \{0\}$, $\text{ann}_M(r)$ est fini, est C-minimal.*

PREUVE. Par le théorème 4.6.3, on sait que toute formule à une seule variable libre x , avec paramètres, est équivalente à une formule de la forme

$$\phi(x) \wedge \psi(v(t_1(x)), \dots, v(t_k(x)), \bar{\gamma}),$$

où ϕ est une formule sans quantificateur et avec paramètres de L_R , ψ est une formule sans paramètres de L'_V , les t_i sont des L_R -termes avec paramètres, et $\bar{\gamma}$ est un n -uplet d'éléments de $v(M)$. Donc ϕ est une combinaison booléenne de formules de la forme $x.r = b$. Puisque $\text{ann}_M(r)$ est fini, elle définit un ensemble fini ou cofini. On se ramène donc à montrer que $\psi(v(t_i(x))_i)$ décrit une combinaison booléenne de boules ouvertes ou fermées. On se contentera de montrer que l'on peut remplacer les termes $v(t_i(x))$ par des termes de la forme $\tau^k(v(x - c_i))$ où $k \in \mathbb{N}$ et $c_i \in M$. Ainsi ψ sera de la forme $\psi'(v(x - c_1), \dots, v(x - c_n))$. La C-minimalité de (M, v) suit alors de l'o-minimalité de la R -chaîne $v(M)$ par des considérations ultramétrique générales (comme il a été explicité dans la preuve de la proposition 36 de [Maa]).

Les termes $t_i(x)$ sont de la forme $x.r_i - a_i$ ($r_i \in R$, $a_i \in M$). Par divisibilité de M , il existe $b_i \in M$ tel que $b_i.r_i = a_i$. Ainsi chaque terme $t_i(x)$ est égal à un terme de la forme $(x - b_i).r_i$. La preuve sera donc achevée dès que nous aurons prouvé l'assertion suivante :

Etant donné $r \in R \setminus \{0\}$, il existe un recouvrement fini de M par des ensembles dont chacun, disons D , est une combinaison booléenne de boules de M et tel que pour un certain paramètre d , $(M, v) \models \forall x \in D, v(x \cdot r) = v(x - d) \cdot r$.

En effet, d'une part par le résultat 4.5.9, on a

$$\forall x \quad \bigvee_{c \in \text{ann}_M(r)} v(x.r) = v((x - c).r) = v(x - c) \cdot r.$$

Et d'autre part, pour tout $c_0 \in \text{ann}_M(r)$, l'ensemble $\{x \in M \mid v((x - c_0).r) = v(x - c_0) \cdot r\}$ est exactement l'ensemble des éléments x tel que $x - c_0$ est régulier pour r , et est égal, par le corollaire 4.5.10, à l'ensemble $\{x \mid v(x - c_0) = \max\{v(x - c_0 - c); c \in \text{ann}_M(r)\}\}$. Ce dernier ensemble est clairement une combinaison booléenne de boules. ■

Proposition 5.4.2. *Soit (M, v) un module valué non K -trivialement et C-minimal. Alors*

(M, v) est affinement maximal et résiduellement divisible, et pour tout $r \in R \setminus \{0\}$, $\text{ann}_M(r)$ est fini.

PREUVE. Puisque v_K est non triviale sur K , $v(M)$ n'est pas minoré. Or $\text{Saut}_M(r)$ est fini pour tout $r \in R \setminus \{0\}$ donc $\text{ann}_M(r)$ ne peut pas contenir de boule propre d'indice fini et doit être fini. De plus, pour les mêmes raisons, $v(M.r)$ n'est pas minoré, donc $M.r$ ne peut contenir de boule propre d'indice fini et $M.r = M$. D'où M est divisible.

Supposons que (M, v) n'est pas affinement maximal. Alors par le théorème 4.5.12 il existe $r \in R \setminus \{0\}$ et $y \in M \setminus \{0\}$ tels que pour tout x vérifiant $x.r = y$, x est irrégulier pour r . Donnons-nous un couple (r, y) comme ci-dessus. Puisque M est divisible l'ensemble $A := \{x \in M \mid x.r = y\}$ est non-vide et puisque $\text{ann}_M(r)$ est fini il s'écrit comme $A = \{x_1, \dots, x_k\}$. Posons $\gamma = \max_i \{v(x_i)\}$ et prenons $x \in A$ de valuation γ . Alors $y \in M_{>\gamma.r} \setminus (M_{>\gamma}).r$. On va montrer que ceci conduit à une contradiction. Puisque γ est un saut, il est limite inférieure dans $v(M)$ des éléments $\delta \in v(M) \setminus \text{Saut}_M(r)$, par le lemme 4.1.9 et par la finitude de $\text{Saut}_M(r)$; donc il est limite des éléments δ tel que $v((M_{>\delta}.r))$ et $v(M_{>\delta.r})$ définissent le même segment final de $v(M)$. Cela impose que $M_{>\gamma.r} = (M_{>\gamma}).r$. Contradiction. \blacksquare

Enfin, on donne une conséquence du résultat ci-dessus dans le cas des corps valués : par le lemme 4.1.9 une R -chaîne o-minimale est dense et pleine; par la remarque 4.1.20 un groupe abélien ordonné plein comme R -chaîne est divisible, et enfin par 4.3.20 un corps valué (K, v) de caractéristique $p > 0$ est algébriquement maximal si et seulement s'il est affinement maximal comme $K[t; x \mapsto x^p]$ -module valué. Donc :

Corollaire 5.4.3. *Soit (K, v) un corps valué infini et de caractéristique $p > 0$. Alors (K, v) est C -minimal comme $K[t; x \mapsto x^p]$ -module valué si et seulement s'il est algébriquement maximal avec un corps résiduel p -clos et un groupe de valuation divisible.*

Chapitre 6

Modules avec une filtration valuationnelle

Dans ce chapitre on va considérer les R -modules comme des structures à une seule sorte, avec des prédicats unaires additionnels qui seront interprétés comme des sous-groupes. Si par exemple (M, v) est un module valué, ce chapitre permet de considérer la structure

$$(M, +, 0, (.r)_{r \in R}, (M_{>\gamma})_{\gamma \in v(M)}).$$

On vise ainsi à étudier la structure de module des corps locaux en caractéristique $p > 0$, sur un anneau de polynômes additifs. Cette approche est celle de Thomas Rohwer dans sa thèse (cf. [Ro]). Nous allons nous intéresser à des modules qui ne sont pas t -divisibles, analogues des corps non-parfaits. Cette situation nous amène à introduire les fonctions λ comme dans le cas des corps séparablement clos et à nous référer à l'article de Dellunde, Delon et Point, dans lequel elles étudient la structure de module des corps séparablement clos (cf. [DDP1]). La première section de ce chapitre est en effet une adaptation du cas séparablement clos au cas henselien. La propriété de Hensel peut se traduire comme la divisibilité asymptotique, et le résultat d'élimination des quantificateurs de l'article [DDP1] se transfère à notre cas comme une propriété d'élimination des quantificateurs asymptotique (cf. théorème 6.5.2).

6.1 La cas parfait

Avant d'étudier le cas des corps locaux, on commence par regarder le cas "parfait", pour motiver le lecteur.

Théorème 6.1.1. *Soit (K, v) un corps de caractéristique $p > 0$, parfait, non-trivialement valué henselien, et de corps résiduel fini \mathbb{F}_q , où $p^n = q$. Soit pour tout $k \geq 1$, tel que k divise n , $R_k := \mathbb{F}_{p^k}[t; x \mapsto x^p]$. Alors la théorie de \mathcal{O}_K en tant que R_k -module est \aleph_1 -catégorique et décidable. Cette théorie est axiomatisée par les axiomes suivants :*

1. les axiomes de R_k -modules à droite et le fait que la multiplication par t est injective,
2. les axiomes disant que le sous-module de torsion est isomorphe à \mathbb{F}_q en tant que R_k -module,
3. $\forall y (\exists x x.(t^n - 1) = y) \Rightarrow (\exists z y = z.(t^n - 1).r)$ pour tout $r \in R_k \setminus \{0\}$.

PREUVE. Soit T le système d'axiomes ci-dessus et D le corps de fractions de R_k . Comme toujours dans le cas des corps, on interprète $x.t$, par x^p . Alors les axiomes 1 sont trivialement vérifiés. Voyons les axiomes 2. Trivialement \mathbb{F}_q est contenu dans la torsion. Réciproquement, si un élément $x \in \mathcal{O}_K \setminus \{0\}$ est annulé par un polynôme additif à coefficients dans R_k , alors x est nécessairement de valuation 0; cela implique aussi que si y est tel que $v(x - y) > 0$, et si y est annulé par le même polynôme que celui qui annule x , alors $x - y$ n'est pas annulé par ce polynôme, d'où $x = y$. D'où le sous-module torsion de \mathcal{O}_K est isomorphe à \mathbb{F}_q . Enfin, quand (K, v) est henselien, \mathcal{M}_K est exactement l'image de \mathcal{O}_K par le polynôme $X^{p^n} - X$. Comme de plus K est parfait, par le lemme 3.2.2, \mathcal{M}_K est divisible en tant que R_k -module. Cela montre que \mathcal{O}_K vérifie l'axiome 3. ci-dessus.

Montrons la catégoricité de T . D'abord par le schéma d'axiomes 2., un modèle M de T a son sous-module de torsion isomorphe à \mathbb{F}_q . Si M' est l'image de l'application $x \mapsto x.(t^n - 1)$ alors $M = \mathbb{F}_q \oplus M'$ comme R_k -module. Le troisième schéma d'axiomes dit que M' est divisible en tant que R_k -module. De plus, M' est sans torsion par le premier point ci-dessus. Donc, M' est un espace vectoriel sur le corps D . Alors si N et M sont de modèles de T de cardinalité \aleph_1 , en définissant M' et N' comme ci-dessus, puisque R_k est dénombrable, N' et M' sont isomorphes en tant que D -espaces vectoriels, donc comme R_k -modules. Donc M et N sont isomorphes. Ainsi T est \aleph_1 -catégorique, donc complète. Comme elle est clairement récursivement énumérable elle est décidable. \blacksquare

6.2 Le $\varphi(K)$ -espace vectoriel K

Soit K un corps, φ un endomorphisme de $(K, +, \times, 1, 0)$ et R comme dans les préliminaires.

Dans tout ce qui suit on supposera que K est une extension finie de $\varphi(K)$ de degré d . Par la suite on notera plutôt K^{φ^n} l'image $\varphi^n(K)$ et, pour $a \in K$, l'expression a^{φ^n} désignera l'image de a par φ^n . Fixons une base $\alpha = \{\alpha_0, \dots, \alpha_{d-1}\}$ du K^{φ} -espace vectoriel K . En décomposant K suivant la base α dans chaque facteur direct $K^{\varphi}\alpha_i$ de $K = \bigoplus_{i=0}^{d-1} K^{\varphi}\alpha_i$ et en itérant ce processus, on voit que α induit pour chaque n une base $\alpha(n)$ du K^{φ^n} -espace vectoriel K . Plus précisément, si $\alpha_j(n-1)$ désigne le j -ième élément de $\alpha(n-1)$, alors, en tant que $K^{\varphi^{n-1}}$ -sous-espace vectoriel de K , $K^{\varphi^{n-1}}\alpha_j(n-1)$ s'écrit comme :

$$K^{\varphi^{n-1}}\alpha_j(n-1) = \left(\bigoplus_{\alpha_i \in \alpha} K^{\varphi}\alpha_i \right)^{\varphi^{n-1}} \alpha_j(n-1) = \bigoplus_{\alpha_i \in \alpha} K^{\varphi^n}\alpha_i^{\varphi^{n-1}}\alpha_j(n-1).$$

On en déduit

$$\alpha(n) = \left((\alpha_i^{\varphi^{n-1}}\alpha_j(n-1))_{i \in d} \right)_{j \in d^{n-1}},$$

où l'ensemble d'indices d^{n-1} est identifié à l'ensemble des fonctions de $\{0, \dots, n-1\}$ dans $\{0, \dots, d-1\}$. Ainsi, dans l'expression ci-dessus, chaque choix d'un couple (i, j) , avec $i \in d$ et $j \in d^{n-1}$, définit une unique fonction $k \in d^n$. Ceci permet de noter d'une manière cohérente l'élément $\alpha_i^{\varphi^{n-1}}\alpha_j(n-1) \in \alpha(n)$ comme $\alpha_k \in d^n$.

Lemme 6.2.1. *a. Chaque polynôme $q \in R$ s'écrit de manière unique comme $\sum_{i \in d^n} q_i \alpha_i(n)$ avec $q_i \in R$.*

b. Pour tout entier $n > 0$, il y a un endomorphisme de $(R, +)$, que l'on notera φ^n , tel que pour tout $q = \sum_{i \in d^n} q_i \alpha_i(n) \in R$,

$$t^n q = \sum_{i \in d^n} \varphi^n \overline{q_i} t^n \alpha_i.$$

De plus, si q est séparable alors, pour chaque n , il y a un certain $i \in d^n$ tel que $\varphi^n \overline{q_i}$ soit séparable.

PREUVE.

a. Soit $0 \leq k \leq s = \deg q$. En décomposant a_k dans la base $\alpha(n)$, chaque monôme $t^k a_k$ de q s'écrit de manière unique comme $t^k \sum_{i \in d^n} a_{k,i}^{\varphi^n} \alpha_i$. On pose $q_{k,i} = t^k a_{k,i}^{\varphi^n}$ et $q_i = \sum_{0 \leq k \leq s} q_{k,i}$. D'où $q = \sum_{i \in d^n} q_i \alpha_i$.

b. Pour $a = \sum_{i \in d^n} a_i^{\varphi^n} \alpha_i \in K$, on définit $\varphi^n \overline{a}$ par $\sum_{i \in d^n} a_i \alpha_i$ et on étend à $q \in R$ en appliquant φ^n à chaque coefficient de q . Par construction, φ^n préserve l'addition. Pour voir l'égalité $t^n q = \sum_{i \in d^n} \varphi^n \overline{q_i} t^n \alpha_i$ il suffit de montrer que $t^n q_i = \varphi^n \overline{q_i} t^n$. On remarque que $\varphi^n \overline{q_{k,i}} = t^k a_{k,i}$ et donc $\varphi^n \overline{q_{k,i}} t^n = t^{n+k} a_{k,i}^{\varphi^n} = t^n q_{k,i}$. Par l'additivité de φ^n on établit : $\varphi^n \overline{q_i} t^n = t^n q_i$. Enfin, si aucun des $\varphi^n \overline{q_i}$ n'est séparable, alors pour tout i , $\varphi^n \overline{q_i}$ s'écrit comme $t q'_i$ avec $q'_i \neq 0$. Donc, par ce qu'on vient de faire, $t^n q$ est la somme des $t q'_i t^n \alpha_i$, des polynômes de degré $\geq n+1$, i.e. $t^n q \in t^{n+1} R$, d'où $q \in tR$. Donc q n'est pas séparable. ■

Corollaire 6.2.2. *Le K -sous-espace vectoriel $t^n K$ de R , est de dimension d^n , et $t^n \alpha(n) = \{t^n \alpha_i(n)\}_{i \in d^n}$ en est une base. En conséquence, le K -sous-espace vectoriel des polynômes de degré $\leq n$ est de dimension $\sum_{0 \leq i \leq n} d^i = \frac{d^{n+1}-1}{d-1}$.*

PREUVE. Le résultat ci-dessus montre en particulier que, pour $a \in K$,

$$t^n a = \sum_{i \in d^n} \varphi^n \overline{a_i} t^n \alpha_i. \blacksquare$$

Définition 6.2.3. On appellera t -libre, un R -module t -injectif et qui admet la décomposition suivante la famille $t\alpha$:

$$M = \bigoplus_{i \in d} M.t\alpha_i.$$

Alors, pour tout $i \in d$ on définit $\lambda_i : M \rightarrow M$, $x \mapsto x_i$, où les x_i sont donnés par l'équation :

$$x = x_0.t\alpha_0 + \dots + x_i.t\alpha_i + \dots + x_{d-1}.t\alpha_{d-1}.$$

En particulier, par nos hypothèses sur K , K est t -libre comme $K[t; \varphi]$ -module (en interprétant $x.t$ par x^φ). Si M est un module t -libre alors, comme ci-dessus, pour tout entier $n > 0$, M s'écrit comme

$$M = \bigoplus_{i \in d^n} M.t^n \alpha_i.$$

et on définit de manière analogue les fonctions λ_i de niveau supérieur pour $i \in d^n$.

Remarque 6.2.4. Les fonctions λ_i sont définissables dans le langage L_R , par une formule exis-

tentielle et par une autre universelle :

$$y = \lambda_i(x) \longleftrightarrow \forall x_1, \dots, \forall x_i, \dots, \forall x_d \quad x = \sum_{j=1}^d x_j \cdot t \cdot \alpha_j \longrightarrow x_i = y \quad (6.1)$$

et

$$y = \lambda_i(x) \longleftrightarrow \exists x_1, \dots, \exists x_{i-1}, \exists x_{i+1}, \dots, \exists x_d \quad x = \sum_{j=1}^{i-1} x_j \cdot t \alpha_j + y \cdot t \alpha_i + \sum_{j=i+1}^d x_j \cdot t \alpha_j. \quad (6.2)$$

Définition 6.2.5. Soit L_R le langage des $K[t; \varphi]$ -modules. Alors L_λ désignera le langage $L_R \cup \{\lambda_i \mid i \in d\}$.

6.3 R -modules filtrés

Ici, on présente un système d'axiomes dont les modèles incluent en particulier les corps locaux en caractéristique $p > 0$, et qui permettra de montrer la proposition 6.5.2 qui est un résultat d'élimination des quantificateurs au voisinage de 0.

Dans tout le reste on ne va considérer que des modules t -libres.

Pour la suite, on fixe une R -chaîne $(\Delta, <, \infty, (\cdot r)_{r \in R})$ telle que K agit non trivialement sur Δ , i.e. K admet une valuation non triviale v_K provenant de son action sur Δ comme dans le chapitre 4. On notera cette valuation v_K . De plus, on supposera que, pour tout $r \in R_{sep}$, $Hens_v(r)$ et $H_v(r)$ sont des segments finaux de la forme $]\gamma, \infty[$, où $\gamma \in \Delta \setminus \{\infty\}$. Alors on introduit une (méta-)fonction $h : R_{sep} \rightarrow \Delta \setminus \{\infty\}$ telle qu'on ait $H_v(r) =]h(r), \infty[$. Donc, dans ce cas, on a $Hens_v(r) =]h(r) \cdot a, \infty[$ où a est le coefficient constant de r . Enfin, on supposera que la fonction τ (i.e. $\cdot t$) est d'image non bornée dans Δ .

On va munir un R -module M d'une chaîne infinie de sous-groupes indexés par la R -chaîne Δ . Pour étudier ces structures on va considérer le langage $L = L_\lambda \cup \{P_\delta \mid \delta \in \Delta\}$, où chaque P_δ est un prédicat unaire.

Définition 6.3.1. On appelle module non trivialement filtré une $L_R \cup \{P_\delta \mid \delta \in \Delta\}$ -structure qui est un R -module, dans lequel P_∞ est le sous-groupe nul, les prédicats $(P_\delta)_\delta$ sont tous des sous-groupes, $P_\gamma \subsetneq P_\delta$ pour tous γ, δ avec $\delta < \gamma$, et vérifiant les deux schémas d'axiomes ci-dessous :

1. $\forall x \in P_\delta \longleftrightarrow x \cdot t \mu \in P_{\delta \cdot t \mu}$, pour tous $\delta \in \Delta$ et $\mu \in K \setminus \{0\}$
2. $\forall x \in P_\delta \longrightarrow x \cdot r \in P_{\delta \cdot r}$, pour tous $\delta \in \Delta$ et $r \in R \setminus \{0\}$.

On veut en particulier axiomatiser la théorie du $K[t; \varphi]$ -module (K, v_K) . Dans ce cas précis on souhaite interpréter les prédicats $(P_\gamma)_{\gamma \in \Delta}$ comme les boules ouvertes centrées en 0.

Les modèles que l'on va considérer satisferont de plus le schéma d'axiomes suivant, qui est un analogue de la propriété de Hensel :

3. $\forall x \in P_{h(q) \cdot a} \longrightarrow \exists! y (y \in P_{h(r)}) \wedge (x = y \cdot r)$, pour tout r séparable de coefficient constant a .

Puisque l'action d'un $r \in R$, non nul, est strictement croissante, et que son image est non bornée par le fait que l'image de $\cdot t$ est non bornée, avec le schéma 2 ci-dessus on a que pour tout $\delta \in \Delta \setminus \{\infty\}$, il existe γ tel que pour tout $x \in P_\gamma$, $x \cdot r \in P_\delta$.

Dans un module valué henselien (M, v) , au sens du chapitre 4, on sait en particulier que pour tout élément $r \in R_{sep}$, si $x \in H_v(r)$ alors x est nécessairement régulier. Cela implique que si B est une boule ouverte (respectivement fermée) de rayon γ centrée en 0 alors $B \cdot r$ est la boule ouverte (respectivement fermée) centrée en 0 de rayon $\gamma \cdot r$. Le schéma d'axiomes ci-dessous est une traduction de ce fait.

4. $\forall x \neq 0 \ x \in P_\gamma \iff x \cdot r \in P_{\gamma \cdot r}$, pour tous $r \in R_{sep} \setminus \{0\}$, et $\gamma > h(r)$.

Enfin, on veut contrôler la «valuation» des composantes $\lambda_i(x)$ en fonctions de celle de x , donc on introduit de nouveau des (méta-)fonctions $\xi_i : \Delta \rightarrow \Delta$ et on impose les axiomes ci-dessous :

5. $\forall x \ x \in P_\gamma \implies \bigwedge_{i \in d} \lambda_i(x) \in P_{\xi_i(x)}$.

Les axiomes ci-dessus impliquent facilement leur généralisation pour les fonctions λ_i de niveau supérieur, i.e. pour $i \in d^s$, pour tout entier s .

Définition 6.3.2. On appellera module non trivialement filtré henselien un R -module M , t -libre, qui est modèle des axiomes ci-dessus.

Exemple 6.3.3. Soit $(K \subset M, v)$ une extension non ramifiée de corps valués de caractéristique $p > 0$, où la valuation v est discrète, L est de corps résiduel fini, et complet. Notons $\pi \in K^\times$ une uniformisante (i.e. $v(\pi)$ est un générateur de $v(K^\times)$). Posons $\Delta := v(M)$ ($= v(K)$, car $\pi \in K$) et interprétons les prédicats P_δ par les boules ouvertes centrées en 0 de (M, v) . Alors M est un $R := K[t; x \mapsto x^p]$ -module non trivialement filtré henselien :

La (méta-)fonction h est déterminée par la structure de R -chaîne de $v(M)$, de la façon suivante ; soit $r \in R_{sep}$, et a son coefficient constant ; l'ensemble $H_v(r) = \{\gamma \in v(M) \mid \gamma \cdot (r - a) > \gamma \cdot r\}$ est non-vide a donc un premier élément, dont $h(r)$ doit être le prédécesseur. Comme le corps (M, v) est complet de valuation discrète il est henselien. Donc c'est un module non K -trivialement valué henselien au sens du chapitre 4. Alors, pour tout $r \in R_{sep}$, $P_{h(r) \cdot a} = Hens_M(r)$ et $P_{h(r)} = H_M(r)$. Donc les axiomes 1 – 4 ci-dessus sont satisfaits par M . De plus, (M^p, v) est complet, et si $\pi \in K^\times$ est une uniformisante pour v , alors $\{1, \pi, \dots, \pi^{p-1}\}$ est une base de M comme M^p -espace vectoriel (cf. par exemple [FeVo], la proposition 2.4). En posant $d := p$ et $\alpha := \{1, \pi, \dots, \pi^{p-1}\}$, M est t -libre comme $K[t; x \mapsto x^p]$ -module et on a l'interprétation naturelle des fonctions λ_i . Dans (M, v) on a l'équivalence

$$v(x) > \delta \text{ si et seulement si } \bigwedge_{i \in p} v(\lambda_i(x)) > (\delta - i)/p.$$

Donc on choisit comme (méta-)fonction ξ_i la partie entière de la fonction $\gamma \mapsto (\gamma - i)/p$, ainsi M est un modèle des axiomes 5, donc de la théorie considérée.

6.4 Matrices sur $K[t; \varphi]$

Définition 6.4.1. Soit $M_R(n, m)$ l'ensemble des matrices à n lignes et à m colonnes à coefficients dans R . On a :

- i. Une matrice $A = (q_{i,j}) \in M_R(n, m)$ est dite triangulaire inférieure si, $j > i$ implique $q_{i,j} = 0$.
- ii. Une matrice $A \in M_R(n, m)$ est dite triangulaire inférieure séparable de co-rang l si les colonnes $l + 1, \dots, m$ de A sont toutes nulles, les autres forment une matrice triangulaire telle que pour tout $i \leq l \leq \min\{n, m\}$, l'élément q_{ii} est séparable.

Proposition 6.4.2. *Étant donné $A \in M_R(m, n)$ il existe une matrice de permutation P à coefficients dans $\{0, 1\}$ et une matrice Q inversible tels que PAQ est triangulaire inférieure.*

PREUVE. Voir proposition 6.1 dans [DDP1]. ■

Soit $q = (q_0, \dots, q_{n-1})$ un n -uplet non nul de R et $e = \min\{d_{is}(q_i)\}$, i.e. l'entier naturel $k > 0$ tel que q appartient à $t^k R \setminus t^{k+1} R$ si aucun des q_i n'est séparable et 0 sinon. On appelle e le degré d'inséparabilité de q et on le note $\deg_{is}(q)$. Supposons $e > 0$. Donc $q_i = t^e q'_i = \sum_{k \in d^e} \sqrt[e]{q'_{ik}} t^e \alpha_k$. Puisqu'au moins un des q'_i est séparable, par le lemme 6.2.1, pour un certain couple (i, k) , le polynôme $\sqrt[e]{q'_{ik}}$ est séparable.

Ces observations permettent de montrer le résultat suivant :

Corollaire 6.4.3. *Soit A une matrice de taille $n \times k$, à coefficients dans R . Alors le système d'équation $y.A = u$ est équivalent à un système*

$$y.P.B = t(u)$$

où P est une matrice de permutation, B une matrice triangulaire inférieure séparable et t un uplet de L_λ -termes.

PREUVE. C'est le lemme 6.4.4 dans [DDP1]. ■

6.5 Élimination des quantificateurs au voisinage de 0

Dans cette section, M désignera un module non trivialement filtré henselien.

Définition 6.5.1. Une boule dans M^k est un sous-ensemble W de M^k de la forme

$$P_{\delta_1} \times \dots \times P_{\delta_k}.$$

On dira qu'une boule est propre si aucun des P_{δ_i} apparaissant dans l'expression de W n'est égal à $\{0\}$. Un sous-ensemble borné de M^n désignera un sous-ensemble inclus dans une boule propre.

Dans cette section, on va établir le résultat suivant :

Proposition 6.5.2. *Soit $\phi(x_1, \dots, x_m)$ une p.p. formule de $L_R \cup \{P_\delta \mid \delta \in \Delta\}$ que l'on écrit comme $\exists y_1 \dots y_k x.B - y.A \in W$ avec A, B des matrices à coefficients dans R de taille convenable et W une boule de M^m . Alors il existe une boule propre V de M^m telle que l'ensemble $\phi(M^m) \cap V$ est définissable sans quantificateurs dans le langage L .*

Ce résultat sera une conséquence du corollaire 6.4.3, et du corollaire 6.5.4 qui s'établit grâce à l'observation suivante :

Lemme 6.5.3. *Pour toute boule propre U de M et pour tout polynôme séparable $r \in R$, il existe une boule propre V telle que pour tout $x \in V$, il existe $y \in U$ tel que $y.r = x$.*

PREUVE. Soit $\gamma \in \Delta$ tel que $U = P_\gamma$. Si $\gamma \leq h(r)$ alors $P_\gamma \supset P_{h(r)}$. Dans ce cas, en prenant $\delta \geq h(r) \cdot a$ avec a le coefficient constant de r , et en posant $V = P_\delta$, on obtient, par les axiomes

3., pour tout $x \in V$ l'existence d'un $y \in P_{h(r)} \subset P_\gamma$ tel que $y.r = x$. Supposons maintenant $\gamma > h(r)$. Donc, $\gamma \in H_v(r)$. Dans ce cas là, $\gamma \cdot r \in \text{Hens}_v(r)$. Alors si $x \in P_{\gamma \cdot r}$ alors, par les axiomes 4. il existe (dans ce cas un unique) $y \in P_{h(r)}$ tel que $y.r = x$; $y \in P_\gamma$ par le fait que $\gamma > h(r)$ et par les axiomes 4. ▮

Corollaire 6.5.4. *Soit $A = (a_{ij})$ une matrice à m lignes et k colonnes triangulaire inférieure séparable avec $k \leq m$. Alors, pour toute boule propre W de M^m , il existe une boule propre W_1 de M^k telle que $W.A \supset W_1$.*

PREUVE. On écrit $W = \prod_{i=1}^m P_{\delta_i}$. Puis on choisit des $\gamma_i \in \Delta$ tel que

$$\sum_{j \neq i} P_{\gamma_i} \cdot a_{ji} \subset P_{\delta_i}.$$

Soit $\gamma = \sup_i \{\gamma_i\}$. Grâce au lemme ci-dessus il existe des boules propres $(U_i)_i$ telles que pour tout $x_i \in U_i$, il existe $y_i \in P_{\gamma_i}$ tel qu'on ait $x_i = y_i \cdot a_{ii}$. On obtient ainsi $x_i - \sum_{i=1}^n y_i \cdot a_{ji} \in P_{\delta_i}$ pour tout $1 \leq j \leq k$. Alors on peut prendre $W_1 = \prod_i U_i$. ▮

Preuve de la proposition 6.5.2. On écrit W comme $\prod_{0 \leq i \leq m-1} P_{\delta_i}$. Soit $I = \{0 \leq i \leq m-1 \mid P_{\delta_i} = \{0\}\}$, J le complémentaire de I dans $\{0, \dots, m-1\}$ et $V_J = \prod_{j \in J} P_{\delta_j}$. On note A_J (respectivement par A_I) la matrice constituée par les colonnes $(C_j)_{j \in J}$ (respectivement par les colonnes $(C_i)_{i \in I}$) de A . Pour x dans M^m , notons $u(x) := x.B$, $u_I(x)$ le $|I|$ -uplet qui est la composante de $u(x)$ sur I et $u_J(x)$ le $|J|$ -uplet de sa composante sur J . Donc ϕ est équivalent à la formule

$$\exists y_1 \dots y_k \quad (u_I(x) = y.A_I \wedge u_J(x) - y.A_J \in V_J).$$

Par le corollaire 6.4.3 il existe une matrice triangulaire inférieure séparable $\widetilde{A}_I = (S, 0)$ de co-rang l , où S est une $k \times n-l$ matrice avec des éléments séparables sur sa diagonale, telle que la formule $u = y.A_I$ est équivalente à la formule

$$(t_1(u_I(x)), \dots, t_{n-l}(u_I(x))) = y.PS \wedge (t_{n-l+1}(u_I(x)), \dots, t_n(u_I(x))) = 0,$$

où P est une matrice de permutation et $t_i(u_I(x))$ un terme de L . Maintenant soit U' une boule propre telle que $U'.A_J \subseteq V_J$, et V' une boule propre donnée par le lemme 6.5.4 telle que $V' \subseteq U'.PS$. Enfin, grâce aux axiomes 2. et 5., on choisit une boule propre V telle que pour tout $x = (x_1, \dots, x_m) \in V$, on a $(t_1(u_I(x)), \dots, t_{n-l}(u_I(x))) \in V'$ et $u_J(x) \in V_J$. Soit $x \in V$. Alors,

$$(t_1(u_I(x)), \dots, t_{n-l}(u_I(x))) \in V'.$$

Donc, il existe $y \in U'$ tel que $(t_1(u_I(x)), \dots, t_{n-l}(u_I(x))) = y.PS$. Par ailleurs, $y \in U' \Rightarrow y.A_J \subset V_J$, par le choix de U' . Ainsi $u_J(x) - y.A_J \in V_J$ car $u_J(x) \in V_J$ aussi. Il vient que la théorie des modules non trivialement filtrés henséliens implique :

$$\forall x \in V, \quad (\phi(x) \leftrightarrow (t_{n-l+1}(u_I(x)), \dots, t_n(u_I(x))) = 0).$$
▮

Bibliographie

- [AdNe] Adeleke S. A. ; Neumann, P. M. : Relations Related to Betweenness : Their Structures and Automorphisms. Mem. AMS 623 (1998)
- [BéPo] Bélair L. ; Point F. : Quantifier elimination in valued Ore modules. J. Symbolic Logic 75 no. 3 (2010), 1007-1043.
- [Co] Cohn P. M. : Skew Fields : Theory of General Division Rings (Encyclopedia of Mathematics and its Applications)
- [DDP1] Dellunde P. ; Delon F. ; Point F. : The theory of modules of separably closed fields I. J. Symbolic Logic 67 (2002), 997-1015.
- [DDP2] Dellunde P. ; Delon F. ; Point F. : The theory of modules of separably closed fields II. Ann. Pure Appl. Logic 129 (2004), 181-210.
- [Del] Delon F. : C-minimal structures without density assumption, in Motivic Integration and its Interactions with Model Theory and Non-Archimedean Geometry, London Mathematical Society Lecture Note Series 383 Vol 1, Cambridge University Press 2011, (Edited by Raf Cluckers ; Johannes Nicaise, Julien Sebag)
- [Ef] Efrat I. : Valuations, orderings, and Milnor K-theory Volume 124 of Mathematical surveys and monographs, American Mathematical Soc., (2006)
- [FeVo] Fesenko I. B. ; Vostokov, S.V. : Local fields and their extensions : a constructive approach ; translation of mathematical monographs, Ams, volume 121
- [Fl] Fleischer I. : Maximality and Ultracompleteness in Normed Modules, Proceedings of the American Mathematical Society Vol. 9, (1958) 151-157.
- [HaMac] Haskell D. ; Macpherson H.D. : Cell decomposition of C-minimal structures, APAL 66 (1994) 113-162
- [Ho] Hodges W. : Model theory, Volume 42 of Encyclopedia of mathematics and its applications, ,Cambridge University Press, (1993)
- [HrPo] Hrushovski E. ; Point F. : On von Neumann regular rings with an automorphism. J. Algebra 315 (2007) 76-120.
- [Ja] Jacobson N. : Basic Algebra II, Dover books on mathematics, Volume 2 of Basic Algebra, Dover Publications, (2009)
- [Ka] Kaplansky I. : Maximal fields with valuations. Duke Math. J. 9 (1942) 303-321.
- [Ku1] Kuhlmann F. : Additive polynomials and their role in the model theory of valued fields. Logic in Tehran, Lect. Notes Log., 26, Assoc. Symbol. Logic, La Jolla, CA, (2006)
- [Ku2] Kuhlmann F. : Elementary properties of power series fields over finite fields. J. Symbolic Logic 66 (2001) 771-791.
- [Ku3] Kuhlmann, Franz-Viktor : Valuation Theory (in preparation)
<http://math.usask.ca/fvk/Fvkbook.htm>

- [KuSa] Kuhlmann S. : Valuation bases for extensions of valued vector spaces. *Forum Math.* 8 (1996) 723-735.
- [Ma] Marker D : *Model Theory : An Introduction*, New York : Springer-Verlag (2002)
- [Maa] Maalouf F. : Espaces vectoriels C-minimaux, *J. Symbolic Logic* 75 (2010) 741-758.
- [MacSt] Macpherson, D. ; Steinhorn, C. : On variants of o-minimality. *Ann. Pure Appl. Logic* 79 (1996) 165-209.
- [Mac] Macpherson, D. : Notes on o-Minimality and Variations, *Model theory, Algebra, and Geometry*, MSRI Publications – Volume 39, (Edited by Deirdre Haskell, Anand Pillay, and Charles Steinhorn)
- [Ore] Ore O. : On a special class of polynomials, *Transactions of the American Mathematical Society*, Vol. 35, (1933) 81-94.
- [Ph] Pheidas, T. : An undecidability result for power series rings of positive characteristic, *Proc. Ams.* Vol 100, (1987) 364-366.
- [PiSt] Pillay A. ; Steinhorn C. : Discrete o-minimal structures, *Stability in model theory* (Trento, 1984). *APAL* 34, (1987) 275-289.
- [Ro] Rohwer T. : Valued difference fields as modules over twisted polynomial rings, *Thèse de Doctorat* (2003) (University of Illinois at Urbana-Champaign)
- [Sa] Sabbagh G. : Sous-modules purs, existentiellement clos et élémentaires, *C. R. Acad. Sci. Paris Sér. A-B* (1971) A1289-A1292.
- [Sim] Simonetta P. : Abelian C-minimal groups, *Ann Pure Appl. Logic* 110 (2001) 1-22.
- [VdDKu] Van den Dries L. ; Kuhlmann, F. : Images of additive polynomials in $\mathbb{F}_q((t))$ have the optimal approximation property, *Canad. Math. Bull.*, vol. 45 (2002) 71-79.
- [Wh] Whaples G. : Galois cohomology of additive polynomial and nthpower mappings of fields, *Duke Math. J.* Volume 24, Number 2 (1957), 143-150.
- [Zi] Ziegler M. : Model theory of modules, *Ann. Pure Appl. Logic* 26 (1984), 149-213.