Numéro d'ordre : 40637

UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE
LABORATOIRE PAUL PAINLEVÉ

THESE DE DOCTORAT

Spécialité : **Mathématiques Pures**

Présentée par : **Luca Demangos**

Minoration de hauteurs canoniques et conjecture de Manin-Mumford

Soutenue le 5 Décembre 2012 devant le jury constitué de :

Michel WALDSCHMIDT	(Université Paris VII)	
Laurent DENIS	(Université Lille 1)	directeur de thèse
Sinnou DAVID	(Université Paris VII)	
Pierre DEBES	(Université Lille 1)	
Federico PELLARIN	(Université Jean Monnet)	rapporteur
Dragos GHIOCA	(University of British Columbia)	rapporteur

Minoration de hauteurs canoniques et conjecture de Manin-Mumford

Luca Demangos

5 Dcembre 2012

Table des matières

Résumé

Ce travail a pour cadre les modules de Drinfeld et plus généralement certains T-modules. On y regarde deux problèmes de nature diophantienne. Dans une première partie on démontre sur les modules de Drinfeld des résultats autour du problème de Lehmer. Plus précisément, nous donnons une minoration de la hauteur canonique des points algébriques en fonction de leur degré. Dans la seconde partie on s'intéresse aux répartitions de points de torsion des $T-$modules dans les sous-variétés algébriques d'un espace affine dans l'esprit des conjectures de Manin-Mumford.

0.1 Minoration de hauteurs canoniques

Soit q une puissance d'un nombre premier p quelconque. On note :

$$A := \mathbb{F}_q[T] \texttt{ et } k := \mathbb{F}_q(T);$$

respectivement l'anneau principal des polynômes à une indéterminée T à coefficients dans $\mathbb{F}_q$ et son corps des fractions. La place à l'infini de k est représentée par la valuation $1/T-$adique $v_{1/T} = v_\infty = -\deg_T$ dont la valeur absolue sur k est :

$$|.|_\infty := q^{-v_\infty(.)}.$$

Nous notons :

$$k_\infty := \mathbb{F}_q((1/T));$$

le complété $1/T-$adique de k. Nous désignons également par $\overline{k}$ et $\overline{k_\infty}$ une clôture algébrique de k et, respectivement, de k_∞, initialement choisies et telles qu'elles contiennent toute extension finie de k que nous allons considérer. Nous convenons également d'appeler :

$$\mathcal{C} := (\overline{k_\infty})_\infty;$$

le complété $1/T-$adique de $\overline{k_\infty}$, de manière qu'il soit un corps non seulement algébriquement clos, mais aussi complet par rapport à la valuation $1/T-$adique. Toute extension finie de k se trouve ainsi plongée dans $\mathcal{C}$. On notera finalement τ l'automorphisme de Frobenius de $\mathcal{C}$ d'exposant q et $\overline{k}\{\tau\}$ l'anneau des endomorphismes de $\mathcal{C}$ correspondant aux polynômes additifs à coefficients dans $\overline{k}$.

Dans ce premier chapitre nous allons nous occuper des **modules de Drinfeld**, qui sont les objets mathématiques suivants.

Définition 0.1.1. *Un* ***module de Drinfeld*** *de* ***rang*** d*, où* $d \in \mathbb{N} \setminus \{0\}$*, défini sur* $\overline{k}$*, est la donnée d'un couple :*

$$\mathbb{D} = (\mathbb{G}_a, \Phi),$$

où $\mathbb{D}$ *est le groupe additif* $\mathbb{G}_a(\mathcal{C})$ *et* Φ *est l'homomorphisme injectif de* $\mathbb{F}_q-$*algèbres suivant :*

$$\Phi : A \to \overline{k}\{\tau\},$$

ayant pour expression :

$$\Phi(T) = \sum_{i=0}^{d} a_i \tau^i;$$

où :

$$a_0(T) = T \;\; \texttt{et} \;\; a_d(T) \neq 0.$$

On définit $k(\Phi) := k(a_1, ..., a_d)$ *le* ***corps des coefficients*** *ou* ***corps de définition*** *de* $\mathbb{D}$*.*

On appelle **point de torsion** du module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ tout point $x \in \overline{k}$ tel qu'il existe un élément $a \in A \setminus \{0\}$ tel que :

$$\Phi(a)(x) = 0.$$

On notera dorénavant avec la notation $\mathbb{D}(\overline{k})_{tors.}$ l'ensemble de tous les points de torsion de $\mathbb{D}$ et par $\mathbb{D}(\overline{k})_{NT} := \mathbb{D}(\overline{k}) \setminus \mathbb{D}(\overline{k})_{tors.}$ l'ensemble des points pas de torsion du module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$.

Les modules de Drinfeld dont nous allons nous occuper dans le premier chapitre de cette thèse sont ceux d'une famille particulière que nous définissons ici. Nous adoptons les notations suivantes. Etant donné $N \in \mathbb{N} \setminus \{0\}$, on définit :

$$P_N(k) := \{l \in A \;\; \texttt{irréductibles et unitaires} \;, \deg_T(l) = N\}.$$

On dira aussi qu'un polynôme irréductible unitaire $l \in A$ **respecte la propriété RV** [1] par rapport à Φ si :

1. Pour toute place w de $k(\Phi)$ divisant v_l (place sur k associée à l) dans l'extension $k(\Phi)/k$, les coefficients a_i de Φ sont tels que $w(a_i) \geq 0$ et :

$$\Phi(l)(X) \equiv X^{q^{d \deg_T(l)}} \;\; \texttt{mod} \;\; (w);$$

   dans l'anneau des polynômes $\mathcal{A}_w/(w)[X]$, où $\mathcal{A}_w$ est l'anneau des $w-$entiers dans $k(\Phi)$;
2. l a degré d'inertie 1 dans l'extension $k(\Phi)/k$ (nous disons dans ce cas que l n'est **pas inerte** dans cette extension).

Définition 0.1.2. *Soit* $r \in]0, 1]$ *un nombre réel. Un module de Drinfeld* $\mathbb{D} = (\mathbb{G}_a, \Phi)$ *est dit* ***RV(r)****, ou, à* ***bon*** r***-relèvement*** *de son anneau des endomorphismes, si pour tout nombre naturel* $N > 0$ *:*

$$|\{l \in P_N(k), l \;\; \texttt{est} \;\; RV\}| \geq \frac{q^{rN}}{2rN}.$$

1. Terminologie choisie puisqu'on va imposer des conditions de **r**éduction suivant certaines **v**aluations

Le résultat que nous proposons dans le premier chapitre est une minoration de la **hauteur canonique** des points non de torsion d'un module de Drinfeld de type RV(r), pour tout $r \in]0,1]$ fixé, dans le cadre du **problème de Lehmer**. Ce problème, que nous expliquerons en détail au cours de la première partie de ce chapitre, peut se résumer comme il suit. On définit :

$$h(x) := \frac{1}{[k(x):k]} \sum_{w \texttt{ places sur } k(x)/k} n_w \max\{0, -w(x)\};$$

la **hauteur logarithmique** d'un point $x \in \overline{k}$. La **hauteur canonique** de x par rapport au module de Drinfeld $\mathbb{D}$ est alors définie comme il suit :

$$\widehat{h}_{\mathbb{D}}(x) = \lim_{n \to \infty} \frac{h(\Phi(T^n)(x))}{q^{dn}}.$$

Il est possible de remarquer que x est un point de torsion par rapport à $\mathbb{D}$ si et seulement si :

$$\widehat{h}_{\mathbb{D}}(x) = 0.$$

Le **problème de Lehmer** dans sa version relative aux modules de Drinfeld propose alors de trouver une minoration de $\widehat{h}_{\mathbb{D}}(x)$, où $x \in \overline{k}$ est un point pas de torsion par rapport à $\mathbb{D}$, en fonction du degré D de x sur k. On conjecture qu'elle pourrait être de l'ordre de grandeur de $1/D$ qui serait optimal (voir [Den1]).

Soit $x \in \overline{k}$ tel que $D = [k(x) : k]$. Nous appellons $D_{sep.}$ le degré séparable de x sur k et $D_{p.i.}$ le degré purement inséparable de x sur k. Il s'ensuit que $D = D_{sep.}D_{p.i.}$.

Ce que nous montrons est alors le Théorème suivant.

Théorème 0.1.3. *Soit $\mathbb{D} = (\mathbb{G}_a, \Phi)$ un module de Drinfeld de type RV(r). Pour tout $x \in \mathbb{D}(\overline{k})_{NT}$ de degré $D = D_{sep.}D_{p.i.}$ sur k on a une minoration de la hauteur canonique de x sous la forme suivante :*

$$\widehat{h}_{\mathbb{D}}(x) \geq C \frac{(\log\log_+ D)^{2+\frac{d}{r}\alpha(\Phi)}}{D D_{p.i.}^{1+\frac{2d}{r}\alpha(\Phi)} (\log_+ D)^{1+\frac{2d}{r}\alpha(\Phi)}};$$

où $\alpha(\Phi)$ est une valeur ≥ 1 ne dépendant que du choix de Φ mais pas de d et de r, C est une constante strictement positive qu'on calculera explicitement et :

$$\log_+(.) := \max\{1, \log_q(.)\};$$

et :

$$\log\log_+(.) := \max\{1, \log_q \log_q(.)\}.$$

Nous obtenons une minoration d'ordre de grandeur polynomial en $1/D$ en général, et l'exposant de $1/D$ est optimal dans le cas séparable. Nous montrons un tel résultat en adaptant la méthode de M. Laurent pour une courbe elliptique à multiplication complexe dans [Lau1] : on suppose par l'absurde que pour tout $C > 0$ il existe $x \in \mathbb{D}(\overline{k})_{NT}$ tel que la valeur $\widehat{h}_{\mathbb{D}}(x)$ soit strictement inférieure à celle indiquée avant ; avec le Lemme de Siegel (voir Lemme 1.2.13) on construit un polynôme auxiliaire s'annulant en x et ayant une nature telle qu'il ne peut être qu'identiquement nul. La condition d'avoir assez de premiers à réduction supersingulière est essentielle pour le fonctionnement de la méthode et en raison de cela nous nous proposons de montrer qu'une classe raisonnablement grande de modules de Drinfeld, comme celle des modules de Drinfeld à **multiplication complexe** respecte une propriété analogue à RV(1), qui nous permettera d'en déduire une minoration de $\widehat{h}_{\mathbb{D}}(x)$, pour tout $x \in \mathbb{D}(\overline{k})_{NT}$, du même ordre de grandeur en D, à des changements de la constante C près.

0.2 Points de torsion et variétés

L'objet de notre étude dans le deuxième chapitre est un problème géométrique sur les $T-$modules. Ces derniers sont une généralisation naturelle des modules de Drinfeld en dimension supérieure. Nous prendrons la définition suivante qui prend son origine dans le texte de G. Anderson ([A]). Nous garderons les notations introduites dans la section précédente pour tous les sous-anneaux de $\mathcal{C}$ considérés. Si K est un corps et n, m deux entiers naturels pas nuls, la notation $K^{n,m}$ indiquera aussi l'anneau des matrices définies sur K, à n lignes et m colonnes.

Définition 0.2.1. *Un $T-$module $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ de degré $\widetilde{d}$ et dimension $m \geq 1$ défini sur un corps $\mathcal{F} \subset \overline{k}$ est le groupe algébrique $\mathbb{G}_a^m$, qui a une structure de $A-$module donnée par l'homomorphisme de $\mathbb{F}_q-$algèbres :*

$$\Phi : A \to \mathcal{F}^{n,n}\{\tau\}$$

$$T \mapsto \sum_{i=0}^{\widetilde{d}} a_i(T)\tau^i;$$

*où $a_0(T)$ (la **différentielle** de $\Phi(T)$) est sous la forme :*

$$a_0 = TI_m + N;$$

où N est une matrice nilpotente, et $a_{\widetilde{d}} \neq 0$. Ce qui montre d'ailleurs que Φ est injectif, tout comme dans le cas d'un module de Drinfeld (qui n'est qu'un $T-$module de dimension 1).

A tout $T-$module, G. Anderson (voir [Goss], Proposition 5.9.2) associe une unique fonction $\overline{e}$ de $\mathcal{C}^m$ dans lui même vérifiant :

$$\overline{e}(a_0\overline{x}) = \Phi(T)(\overline{e}(\overline{x}));$$

telle que :

$$\overline{e}(\overline{x}) = \overline{x} + \sum_{i\geq 1} B_i \overline{x}^{q^i};$$

où $B_i \in \mathcal{F}^{m,m}$ pour tout $i \in \mathbb{N}\setminus\{0\}$ et $\overline{x}^{q^i}$ est obtenu par élévation à la puissance q^i de chaque composante de $\overline{x}$. On l'appelle l'**exponentielle** du $T-$module.

Définition 0.2.2. *L'ensemble des points de torsion dans $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ est :*

$$\mathcal{A}_{tors.} := \{\overline{x} \in \overline{k}^m, \exists a(T) \in A \setminus \{0\}, \Phi(a)(\overline{x}) = \overline{0}\}.$$

Dans ce chapitre on développe une stratégie qui a pour but la preuve d'une version de la Conjecture de Manin-Mumford spécifiquement adaptée au cas d'une classe particulière de $T-$modules. Rappellons brièvement les origines de cette conjecture.

La conjecture de Manin-Mumford classique, traitant la situation d'une courbe elliptique plongée dans sa Jacobienne a été prouvée (voir [R1]) et ensuite généralisée (voir [R2]) dans la formulation qui suit :

Théorème 0.2.3. *Soit X une sous-variété algébrique d'une variété abélienne $\mathcal{A}$, les deux étant définies sur un corps de nombres. Si X contient un ensemble Zariski-dense de points de torsion, alors X est la translatée d'une sous-variété abélienne de $\mathcal{A}$ par un point de torsion.*

La version faible montrée dans [PZ] est une conséquence du Théorème 0.2.3 et se formule de cette manière :

Théorème 0.2.4. *Sous les mêmes hypothèses que le Théorème 0.2.3, si X ne contient pas de translatées de sous-variétés abéliennes de $\mathcal{A}$ de dimension > 0 par un point de torsion, alors X n'a qu'un nombre fini de points de torsion.*

Dans le cadre des $T-$modules, pour expliquer notre travail on utilisera les définitions suivantes.

Définition 0.2.5. *Un sous-$T-$module $\mathcal{B}$ d'un $T-$module $\mathcal{A}$ est un sous-groupe algébrique connexe de $(\mathcal{A}, +)$ tel que $\Phi(T)(\mathcal{B}) \subset \mathcal{B}$.*

Remarque 0.2.6. *On indiquera dorénavant par* ***dimension*** *d'un sous-$T-$module, sa dimension en tant que variété algébrique. On remarque qu'un sous-$T-$module $\mathcal{B} < \mathcal{A}$ non trivial (donc, $\mathcal{B} \neq \mathcal{A}, 0$) a une dimension strictement inférieure à celle de $\mathcal{A}$. Les sous-$T-$modules d'un $T-$module ne sont donc pas forcément des $T-$modules (bien qu'habituellement ce sont des sous-groupes algébriques isomorphes à des puissances de $\mathbb{G}_a$, voir par exemple [T] pour les sous-$T-$modules des puissances d'un module de Drinfeld) mais cette terminologie fréquente est suffisante pour notre propos.*

Une formulation analogue du Théorème 0.2.4 a été montrée par T. Scanlon dans [Sc] pour les $T-$modules qui sont la puissance d'un module de Drinfeld (que nous allons définir ici tout de suite), en utilisant la théorie des modèles et se basant sur un précédent résultat de L. Denis (voir [Den3]), où le même résultat est montré pour une puissance d'un module de Drinfeld, mais sous une hypothèse supplémentaire sur la nature de ce dernier. Etant donné $\mathbb{D}_1$ et $\mathbb{D}_2$ deux modules de Drinfeld de rangs respectifs d_1 et d_2 et définis respectivement sur les corps $\mathcal{F}_1$ et $\mathcal{F}_2$ contenus dans $\overline{k}$, dont la structure de $A-$module est donnée respectivement par les morphismes de $\mathbb{F}_q-$algèbres :

$$\Phi_1 : T \mapsto T + \sum_{i=1}^{d_1} \alpha_i(T)\tau^i;$$

et :

$$\Phi_2 : T \mapsto T + \sum_{i=1}^{d_2} \beta_i(T)\tau^i;$$

le **module produit** $\mathbb{D}_1 \times \mathbb{D}_2 = (\mathbb{G}_a^2, \Phi_1 \times \Phi_2)$ de $\mathbb{D}_1$ et $\mathbb{D}_2$, est le $T-$module de dimension 2 défini sur le compositum des corps $\mathcal{F}_1$ et $\mathcal{F}_2$ selon le morphisme produit qui suit (on suppose que $d_1 \leq d_2$) :

$$\Phi_1 \times \Phi_2 : T \mapsto TI_2 + \sum_{i=1}^{d_1} \begin{pmatrix} \alpha_i(T) & 0 \\ 0 & \beta_i(T) \end{pmatrix} \tau^i + \sum_{i=d_1+1}^{d_2} \begin{pmatrix} 0 & 0 \\ 0 & \beta_i(T) \end{pmatrix} \tau^i.$$

Par récurrence, on étend une telle définition au produit de n modules de Drinfeld avec $n > 2$.

Le résultat de Scanlon est le suivant.

Théorème 0.2.7. *Soit $\mathcal{A} := \mathbb{D}^m = (\mathbb{G}_a^m, \Phi^m)$ un $T-$module puissance d'un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ donné, défini sur le corps $\mathcal{F} \subset \overline{k}$. Soit X une sous-variété algébrique irréductible de $\mathcal{A}$. Si $X(\mathcal{F})_{tors.}$ est Zariski-dense dans X, alors X est une translatée d'un sous-$T-$module de $\mathcal{A}$ par un point de torsion.*

La classe de $T-$modules à laquelle nous nous sommes intéressés est celle des $T-$modules à la fois **abéliens** et **uniformisables**. Un $T-$module $\mathcal{A}$ abélien, défini sur un corps $\mathcal{F} \subset \overline{k}$, est un $T-$module comme dans notre Définition précédente, dont le **rang** (le rang sur $\mathcal{F}[T]$ du $\mathcal{F}[T]-$module $Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a)$, voir Définition 2.1.7) est fini. Un $T-$module est dit d'ailleurs uniformisable si la fonction exponentielle qu'on lui associe est surjective. Ce sont des hypothèses de régularité classiques hors desquelles il semble dangereux de s'aventurer.

Le Théorème 0.2.7 est valable pour une puissance d'un module de Drinfeld et on peut montrer qu'un tel $T-$module est abélien et uniformisable. Nous verrons toutefois lors de la première partie du chapitre 2 que les seules hypothèses abéliens et uniformisables ne sont pas suffisantes. Par exemple nous établirons qu'il existe des $T-$modules vérifiant ces deux hypothèses mais qui admettent des sous-T^j-modules pour un $j \in \mathbb{N} \setminus \{0\}$, donc qui contiennent une infinité de points de torsion, mais qui ne contiennent pas de translatés de sous-$T-$modules non triviaux. De plus on verra que les produits de deux modules de Drinfeld de rangs différents posent également problème.

Du côté des sous-$T-$modules, les exemples semblent montrer que pour un $T-$module $\mathcal{A}$ donné, les sous-$a(T)-$modules (c'est à dire, les sous-groupes algébriques connexes et stables par l'action de $\Phi(a(T))$ pour $a(T) \in \mathbb{F}_q[T] \setminus \mathbb{F}_q$) soient toujours des sous-T^j-modules pour un certain $j \in \mathbb{N} \setminus \{0\}$ ne dépendant que du choix de $\mathcal{A}$. C'est pourquoi on sera amené à la conjecture suivante :

Conjecture 1. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module uniformisable de dimension m et rang d, tel qu'il existe $i \in \mathbb{N} \setminus \{0\}$ tel que la matrice coefficient dominant de l'itéré $\Phi(T^i)$ est inversible. Il existe alors $j(\mathcal{A}) \in \mathbb{N} \setminus \{0\}$ tel qu'on ait la propriété suivante. Soit X une sous-variété algébrique irréductible de $\mathcal{A}$, telle que $\dim_{\mathcal{C}}(X) > 0$, définie sur $\overline{k}$. Si X ne contient pas de translatés de sous-$T^{j(\mathcal{A})}-$modules de $\mathcal{A}$ de dimension > 0 par des points de torsion, alors X ne possède qu'un nombre fini de points de torsion de $\mathcal{A}$.*

On verra dans le deuxième chapitre que l'hypothèse que le coefficient dominant de $\Phi(T^i)$, pour un $i \in \mathbb{N} \setminus \{0\}$, soit inversible implique le fait que $\mathcal{A}$ est abélien.

La suite du deuxième chapitre sera consacrée à présenter une attaque possible de cette conjecture. La méthode que nous nous sommes proposés de suivre est analogue à celle contenue dans le travail de J. Pila et U. Zannier [PZ] : en supposant que $\mathcal{A}$ soit un $T-$module abélien et uniformisable nous ramenons le problème dans l'espace tangent $Lie(\mathcal{A})$ de $\mathcal{A}$ en observant qu'il existe un isomorphisme d'espaces vectoriels sur k_∞ sous la forme suivante :

$$Lie(\mathcal{A}) \simeq \mathcal{C}^m \simeq k_\infty^d \oplus Lib;$$

où k_∞^d est la partie de torsion de $Lie(\mathcal{A})$ et Lib sa partie libre vis à vis du quotient de cet espace par le réseau des périodes (c'est à dire l'ensemble des zéros de l'exponentielle) Λ, qui est isomorphe à A^d en tant que $A-$module. Par conséquent, les points de torsion de $\mathcal{A}$ correspondent aux points $k-$rationnels dans k_∞. En appelant $\pi_1 : Lie(\mathcal{A}) \twoheadrightarrow k_\infty^d$ la projection de l'espace tangent dans sa partie de torsion, tout se ramène à l'étude de l'ensemble analytique $Z := \pi_1(\overline{e}^{-1}(X)) \subset k_\infty^d$. La méthode consiste à prouver les trois points suivants. Nous ne prouverons ici que le premier de ces points.

1. Majorer le nombre de points de torsion de $Z \setminus Z^{alg.}$ (où $Z^{alg.}$ est la partie algébrique de Z, soit, l'union de tous les sous-ensembles semi-algébriques de Z) en nous inspirant de certaines techniques contenues dans les travaux de J. Pila [P] et de J. Pila et J. Wilkie [PW].
2. Montrer que $Z^{alg.}$ est exactement l'union des ensembles algébriques dans Z de la forme $\overline{z} + \pi_1(\overline{e}^{-1}(\mathcal{B}))$, où $\overline{z} \in Z(k)$ et $\mathcal{B}$ varie dans la famille des sous-T^j-modules de $\mathcal{A}$, avec $j \in \mathbb{N} \setminus \{0\}$ fixé par le choix de $\mathcal{A}$.
3. Minorer le degré algébrique de points de torsion de manière incompatible avec l'estimation obtenue du point 1 si le nombre de ces points de torsion tend à l'infini.

Le résultat contenu dans le deuxième chapitre est donc l'obtention du point 1, et plus précisément de l'énoncé suivant.

Théorème 0.2.8. *Pour tout $\epsilon > 0$ il existe une constante $c(\epsilon) > 0$ telle que le nombre des points de $a(T)-$torsion contenus dans l'ensemble $Z \setminus Z^{alg.}$, pour n'importe quel $a(T) \in A \setminus \{0\}$, est au plus :*

$$c(\epsilon)|a(T)|_{1/T}^{\epsilon}.$$

Un passage décisif de la preuve consiste à prouver une version $1/T-$adique du Théorème de la Fonction Implicite Analytique. Bien que la preuve ait été trouvée indépendamment, ce résultat se trouve déjà dans [I], Theorem 2.1.1, page 18. Nous proposons également une telle démonstration pour garantir un caractère complet du texte présent. Ce résultat sera prouvé lors de la deuxième partie de ce chapitre. On en déduira le Théorème 0.2.8 dans une troisième partie. Enfin les deux derniers points suivants de la méthode seront discutés brièvement lors de la quatrième et dernière partie.

Remerciements

Ecrire en Français ces remerciements est ma façon déjà de remercier la France de m'avoir accueilli pendant ces cinq années durant les quelles j'ai non seulement étudié des Mathématiques mais aussi veçu dans un pays qui m'a toujours mis à disposition tous les services et les possibilités prévus pour ses citoyens. Je m'excuse en avance des nombreux erreurs de grammaire et d'ortographe qui suivront.

Je souhaite remercier tout d'abord mon directeur de thèse, Mr. Laurent DENIS, qui a accepté d'encadrer ma thèse en 2008 bien qu'à l'époque je n'étais pour lui qu'un complet inconnu et que je n'avais la moindre connaissance d'aucun des sujets qu'il aurait pu me proposer. Son geste de confiance à mon égard a eté mon premier appui pour sortir d'une période très difficile. Je le remercie également pour la patience qui a eu (notamment au début) à me suivre, à se faire charge d'un travail très lourd et parfois pénible, mais absolument indispensable, de correction de cette thèse. Travailler sous sa direction m'a permis de connaître un sujet de recherche totalement nouveau et extremement intéressant, auquel il a su me faire acceder avec la plus grande claireté. Sans son aide mon doctorat n'aurait jamais pu aboutir.

Je remercie également Mr. Sinnou DAVID pour l'incroyable disponibilité qui à montré envers moi pendant ma permanence à Paris, en me consacrant une quantité absolument remarquable de son temp et se montrant toujours très intéressé à mes progrès et toujours disponible à m'aider de la manière la plus totale et satisfaisante. Sa contribution à ce travail a eté fondamentale.

Je remercie Mr. Federico PELLARIN d'avoir accepté d'être rapporteur de cette thèse et surtout du travail considérable qu'il a fait avec la plus grande précision pour me permettre de pouvoir présenter des résultats corrects et bien rédigés. Ses remarques m'ont beaucoup appris au niveau des méthodes d'aborder un problème et de dévélopper les calculs.

Je remercie Mr. Pierre DEBES, qu'en tant que responsable à Lille du projet éuropéen de recherche GTEM (du quel m'avait mis à connaissance lui-même) a decidé de retenir ma candidature pour un poste de doctorant au sein de l'USTL en me donnant ainsi l'importante opportunité de venir faire un doctorat en France en 2007. Il a eté un repère fondamental pour moi pendant mes premières années à Lille, se montrant toujours totalement disponible à m'aider en toute difficulté, non seulement mathématique, que j'ai rencontré pendant les cinq derniers ans.

Je remercie Mr. Dragos GHIOCA d'avoir accepté d'être rapporteur de ma thèse et de ses conseils et indications sur sa rédaction.

Je remercie aussi Mr. Michel WALDSCHMIDT d'avoir accepté de faire partie du jury.

Je remercie Mr. Vincent BOSSER, qui a montré le plus grand interêt vers mes résultats et m'a aidé à dévélopper plusieurs points très importants et délicats dans le premier chapître.

Un grand merci à Hugues BAUCHERE aussi, qui a mis à ma disposition son propre travail afin de m'aider à surmonter certaines difficultés techniques, ce qui m'aurait pris sinon un temp beaucoup plus long.

Je remercie Mr. Lorenzo RAMERO, qui pendant ma première année à Lille a répondu à toutes mes questions concernant les techniques et les propriétés fondamentales en Géométrie non-Archimédienne, en m'indiquant plusieurs bouquins qui m'ont etés indispensables pour arriver à contourner l'un des obstacles techniques les plus durs que j'ai rencontré dans mon travail.

Je remercie mes anciens copains à Pise et en particulier Alessio MARTINI et Alessandro COBBE, qui ne m'ont jamais nié leur aide et dont les conseils mathématiques et méthodologiques m'ont permis de surmonter un grand nombre de difficultés durant mon doctorat.

Je remercie Mr. Paltin IONESCU, qui a tenu un cours d'eté superbe en Géométrie Algébrique à Perugia en juillet et aout 2008 dans le cadre de la "Scuola Matematica Interuniversitaria", en jouant un rôle décisif dans ma formation mathématique et dans mes progrès.

Un remerciement particulier est dû à Orlando CAU, qui s'est pris la charge de surveiller mon Français, et non seulement dans ces remerciements.

Je remercie finalement ma famille et mes parents pour le soutien total et sans conditions qu'ils m'ont toujours donné durant ces longues années, et sans le quel cette thèse de doctorat n'aurait jamais eté possible.

Chapitre 1

Minoration de hauteurs canoniques

1.1 Introduction

On se propose d'étudier une version du Problème de Lehmer dans le cas des modules de Drinfeld dont l'anneau des endomorphismes respecte les propriétés de bon relèvement $\mathrm{RV}(r)$ et $\mathrm{RV}(r)^*$ (en gros, qu'il y a assez de polynômes irréductibles et unitaires à réduction supersingulière, dans le cas $\mathrm{RV}(r)$ quelque soit leur degré, dans le cas plus faible $\mathrm{RV}(r)^*$ seulement pour une valeur assez grande de ce degré, voir les définitions 3 et 4 pour les énoncés précis) dans la situation qu'on va décrire. On notera $A := \mathbb{F}_q[T]$ l'anneau des polynômes à une variable sur le corps fini à q éléments, sa caractéristique étant le nombre premier p. On notera par ailleurs k son corps de fractions.

Toute étude à caractère diophantien développée sur un module de Drinfeld, ainsi que sur un $T-$module, repose sur d'importants parallèles avec le cas des corps de nombres : respectivement, sur une courbe elliptique et une variété abélienne. Evidemment, l'anneau A et son corps de fractions k sont les analogues, respectivement, de l'anneau des entiers $\mathbb{Z}$ et de son corps de fractions $\mathbb{Q}$. De la même manière on définit l'analogue k_∞ de $\mathbb{R}$, qui est la complétion archimédienne de $\mathbb{Q}$, comme la complétion de k par rapport à la valeur absolue $|.|_{1/T}$ correspondant à la place à l'infini. On fixe alors une clôture algébrique de k contenant toute extension finie de k que nous allons considerer, qu'on appelera $\overline{k}$, ainsi qu'une clôture algébrique $\overline{k_\infty}$ de k_∞, respectant la même condition par rapport à ce dernier. Comme la clôture algébrique d'un corps complet ne reste pas forcément complète l'analogue de $\mathbb{C}$ ne sera donc pas $\overline{k_\infty}$, mais sa complétion $\mathcal{C} := (\overline{k_\infty})_\infty$.

Définition 1.1.1. *Soit :*

$$\tau : \mathcal{C} \to \mathcal{C}$$

$$z \mapsto z^q;$$

*l'automorphisme de Frobenius sur $\mathcal{C}$ et $\overline{k}\{\tau\}$ l'anneau des endomorphismes de $\mathcal{C}$ correspondant aux polynômes additifs à coefficients dans $\overline{k}$. Un **module de***

Drinfeld *de* ***rang*** d*, où* $d \in \mathbb{N} \setminus \{0\}$*, défini sur* $\overline{k}$*, est la donnée d'un couple :*

$$\mathbb{D} = (\mathbb{G}_a, \Phi),$$

où $\mathbb{D}$ *est le groupe additif* $\mathbb{G}_a(\mathcal{C})$ *et* Φ *est l'homomorphisme injectif de* $\mathbb{F}_q-$*algèbres le suivant :*

$$\Phi : A \to \overline{k}\{\tau\},$$

ayant pour expression :

$$\Phi(T) = \sum_{i=0}^{d} a_i \tau^i;$$

où :

$$a_0(T) = T \ \texttt{et} \ a_d(T) \neq 0.$$

On définit $k(\Phi) := k(a_1, ..., a_d)$ *le* ***corps des coefficients*** *ou* ***corps de définition*** *de* $\mathbb{D}$*.*

On appelle **point de torsion** du module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ tout point $x \in \overline{k}$ tel qu'il existe un élément $a \in A \setminus \{0\}$ tel que :

$$\Phi(a)(x) = 0.$$

On appelle d'ailleurs :

$$\Phi[a];$$

le $\mathbb{F}_q-$espace vectoriel des points de $a-$torsion via l'action de Φ. On notera dorénavant :

$$\mathbb{D}(\overline{k})_{NT} := \overline{k} \setminus \bigcup_{a \in A \setminus \{0\}} \Phi[a];$$

l'ensemble des points pas de torsion du module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$.

Définition 1.1.2. *Le* ***module de Carlitz*** *est un cas particulier de module de Drinfeld, de rang* 1*. Plus précisément, l'expression définissant ce dernier est :*

$$\Phi(T) = T + \tau.$$

La **Conjecture de Lehmer** dans le cas des modules de Drinfeld (voir [Den1]) est le problème que nous nous proposons d'attaquer dans ce travail. Elle prend naissance à partir de la Conjecture de Lehmer originelle, liée à l'étude du groupe multiplicatif $\mathbb{G}_m(\overline{\mathbb{Q}})$ (voir le deuxième paragraphe). Il s'agit d'une minoration de la hauteur canonique (voir l'introduction ou le deuxième paragraphe pour la définition) des points algébriques x sur un module de Drinfeld quelconque en fonction de la dimension de x sur k, sous la forme suivante :

Conjecture 2. *Il existe une constante* $c > 0$ *effective, ne dépendant que du module de Drinfeld* $\mathbb{D} = (\mathbb{G}_a, \Phi)$*, telle que, tout point* $x \in \mathbb{D}(\overline{k})_{NT}$ *de degré* D *sur* k *respecte l'inégalité suivante :*

$$\widehat{h}_{\mathbb{D}}(x) \geq \frac{c}{D}.$$

On verra plus loin que si on ne considère que les points $x \in \mathbb{D}(\overline{k})_{NT}$ ayant un degré D inférieur à une constante M donnée explicitement, cet énoncé est, dans ce cas spécifique, une conséquence directe du Théorème de Northcott, qu'on énoncera plus loin dans le texte et permet d'obtenir une constante effective meilleure que celle qui apparaît dans notre résultat final. Il suffira donc d'établir une minoration de la hauteur pour $D \geq M$ et nous obtiendrons une minoration de la hauteur canonique qui ne diffère de celle de la conjecture que par une puissance de $\log_q D$ dans le cas séparable et par une de D dans le cas général, pour une classe de modules étendue.

Voici un rappel des notations fondamentales pour les fonctions logarithmiques utilisées :

$$\log(.) := \log_q(.);$$

fonction logarithme toujours en base q sauf précision ultérieure ;

$$\log_+(.) := \max\{\log(.), 1\};$$

$$\log\log_+(.) := \max\{\log\log(.), 1\}.$$

Par convention on indiquera dorénavant le degré en T de tout polynôme $a \in A = \mathbb{F}_q[T]$ par le symbole $\deg_T(a)$.

On va noter :

$$S(A) := \{l \in A, \ \texttt{unitaires et irréductibles}\}.$$

Nous posons aussi, étant donné $N \in \mathbb{N} \setminus \{0\}$:

$$P_N(k) := \{l \in S(A), \deg_T(l) = N\}.$$

On dira, d'ailleurs, que $l \in S(A)$ **respecte la propriété RV** par rapport à Φ si :

1. Pour toute place w divisant v_l (place associée à l sur k) dans l'extension $k(\Phi)/k$, les coefficients a_i de Φ sont tels que $w(a_i) \geq 0$ et :

   $$\Phi(l)(X) \equiv X^{q^{d \deg_T(l)}} \ \texttt{mod}\ (w);$$

   dans l'anneau des polynômes $\mathcal{A}_w/(w)[X]$, en appellant $\mathcal{A}_w$ l'anneau des $w-$entiers dans $k(\Phi)$;

2. l a degré d'inertie 1 dans l'extension $k(\Phi)/k$ (nous disons dans ce cas que l n'est **pas inerte** dans cette extension).

Définition 1.1.3. *Soit $r \in]0,1]$ un nombre réel et c_1 une constante positive fixée. Un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ est dit **RV(r, c_1)**, ou, à **bon r-relèvement** de son anneau des endomorphismes si pour tout nombre naturel $N > 0$:*

$$|\{l \in P_N(k), l \ \ \texttt{est}\ RV\}| \geq c_1 \frac{q^{rN}}{N}.$$

Définition 1.1.4. *Un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ est dit **RV(r, c_1)***, avec $r \in]0,1]$ et $c_1 > 0$ une constante fixée, s'il existe un nombre $N(\Phi) \in \mathbb{N} \setminus \{0\}$ tel* *que, pour tout $N \geq N(\Phi)$ (on adoptera parfois aussi la notation plus pratique $N >> 0$ pour indiquer les N assez grands en fonction des paramètres donnés) :*

$$|\{l \in P_N(k), l \texttt{ est } RV\}| \geq c_1 \frac{q^{rN}}{N}.$$

Définition 1.1.5. *Soit $r \in]0,1]$ un nombre réel. Un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ est dit **RV(r)** s'il est RV($r, 1/2r$).*

Définition 1.1.6. *Soit $r \in]0,1]$ un nombre réel. Un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ est dit **RV(r)*** s'il est RV($r, 1/2r$)*.*

Le choix du terme $c_1 = 1/2r$ dans la propriété RV(r) est fait pour fixer les idées, au vu de la dépendance finale en r dans la minoration qu'on obtient de la hauteur elle est peu significative. On pourra bien sûr remarquer que si RV(r, c_1) est satisfaite pour un module de Drinfeld alors RV(r', c_1') l'est aussi pour tout $r' \leq r$ et $c_1' \leq c_1$.

La Proposition 1.2.12 nous donnera la possibilité d'une existence effective, au moins en théorie, des modules de Drinfeld de type RV($1, 1/2$), ainsi $c_1 = 1/2$ est le choix maximal possible de c_1 quand $r = 1$.

Un tout premier exemple de module de Drinfeld de type RV(1) est donné par le module de Carlitz. On peut en effet montrer (voir [Hayes], Proposition 2.4) que tout $l \in S(A)$ est à réduction supersingulière par rapport au module de Carlitz. En particulier, le module de Carlitz est de type RV(1) et satisfera donc nos Théorèmes.

Un résultat connu pour les modules de Drinfeld de rang 2, voir [Dav], montre aussi comment, en moyenne, de tels modules (supposés à coefficients dans k) satisfont l'analogue de la Conjecture de Lang-Trotter dans le cas des modules de Drinfeld, nous donnant ainsi l'existence effective d'un nombre considérable d'exemples, en rang 2, satisfaisants la condition RV(r, c_q)*, avec $r = 1/d = 1/2$ et $c_q > 0$ une constante ne dépendant que de q. On souligne néanmoins comment cette Conjecture dans son analogue aux modules de Drinfeld s'est révélée fausse (tout en restant ouverte dans le cas classique des courbes elliptiques), pour toute valeur possible du rang, grâce au travail de B. Poonen, [Pn].

Les méthodes contenues dans l'Appendice montrerons aussi comment la classe des modules de Drinfeld de type CM (ou, à multiplication complexe) et de rang d premier ou 1 est contenue dans une qui ne diffère de RV($1, 1/2d$)* que sur le fait qu'on ne prend que des premiers de $S(A)$ de degré congru à 1 modulo η, où η est une certaine constante qu'on définira plus tard, ne dépendant que du module de Drinfeld Φ choisi.

Ce que nous proposons dans ce travail, étant donné un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ de type RV(r) et, plus généralement, de type RV(r)*, est une minoration de la hauteur canonique de tout point $x \in \mathbb{D}(\overline{k})_{NT}$ dont le degré algébrique sur k est D et le degré purement inséparable est $D_{p.i.}$, sous la forme suivante :

$$C\frac{(\log\log D)^{\mu}}{DD_{p.i.}^{\lambda}(\log D)^{\kappa}};$$

les constantes positives C, κ, μ et λ explicitées en fonction des trois grandeurs arithmétiques du module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$: la dimension $c(\Phi)$ du corps $k(\Phi)$ engendré par les coefficients du module de Drinfeld sur k (dont on indique $A[\Phi]$ son anneau des entiers algébriques sur k), la hauteur $h(\Phi)$ du module de Drinfeld Φ (c'est la hauteur naïve du polynôme $\Phi(T)$ qu'on rappellera, voir définition 1.2.2), et le rang d. On appellera aussi $\alpha(\Phi) = \alpha := c(\Phi)h(\Phi)$. Ceci se résume dans les théorèmes généraux, qui suivent. On notera les dimensions des corps concernés :

$$D = [k(x) : k];$$
$$c(\Phi) := [k(\Phi) : k];$$
$$D' := [k(\Phi, x) : k(\Phi)].$$

Nous appellons également :

$$D_{p.i.} := [k(x) : k]_{p.i.};$$

le degré inséparable de x sur k. On a alors deux résultats en fonction de la séparabilité de x sur k.

Cas séparable :

Théorème 1.1.7. *Soit $\mathbb{D} = (\mathbb{G}_a, \Phi)$ un module de Drinfeld de type RV(r) ou RV(r)*, r compris dans l'intervalle $0 < r \leq 1$, de rang d, de hauteur $h(\Phi)$. On pose :*

$$c_0 := 6500dh(\Phi)^3c(\Phi)^3q^{d+rh(\Phi)c(\Phi)}.$$

Soit :

$$C_0 := \min\{q^{-5d(2(d+1)h(\Phi)+1)((q^{q+d+1}-1)c(\Phi))^2}, \frac{h(\Phi)c(\Phi)}{768rq^dc_0^{1+\frac{4d}{r}h(\Phi)c(\Phi)}}\}.$$

Pour tout $x \in \mathbb{D}(\overline{k})_{NT}$ séparable de degré D sur k :

$$\Phi \texttt{ de type } RV(r) \Longrightarrow \widehat{h}_{\mathbb{D}}(x) \geq C_0\frac{(\log\log_+ D)^{2+\frac{d}{r}h(\Phi)c(\Phi)}}{D(\log_+ D)^{1+\frac{2d}{r}h(\Phi)c(\Phi)}}.$$

$$\Phi \texttt{ de type } RV(r)^* \Longrightarrow{}^{1}\ \exists 0 < C \leq C_0,\ \widehat{h}(x) \geq C\frac{(\log\log_+ D)^{2+\frac{d}{r}h(\Phi)c(\Phi)}}{D(\log_+ D)^{1+\frac{2d}{r}h(\Phi)c(\Phi)}}.$$

Cas général :

Théorème 1.1.8. *Soit $\mathbb{D} = (\mathbb{G}_a, \Phi)$ un module de Drinfeld respectant les mêmes hypothèses que dans le Théorème 1.1.7. On appelle :*

$$c_0 := 35000dh(\Phi)^3c(\Phi)^3q^{d+rh(\Phi)c(\Phi)}.$$

Soit :

$$C_0 := \min\{q^{-5d(2(d+1)h(\Phi)+1)((q^{q+d+1}-1)c(\Phi))^2}, \frac{h(\Phi)c(\Phi)}{384rq^dc_0^{\frac{4h(\Phi)c(\Phi)d}{r}+1}}\}.$$

1. Voir la Remarque 1.3.8 pour une explicitation effective de C en fonction du nombre inconnu $N(\Phi) \in \mathbb{N} \setminus \{0\}$, dépendant du choix de Φ, à partir duquel la valeur des degrés des premiers à réduction supersingulière de Φ garantit que ces premiers sont en quantité suffisante.

Pour tout $x \in \mathbb{D}(\overline{k})_{NT}$ de degré D sur k avec degré de $k-$inséparabilité $D_{p.i.} > 1$:

$$\widehat{h}(x) \geq C\frac{(\log\log_+ D)^{\mu}}{DD_{p.i.}^{\lambda}(\log_+ D)^{\kappa}};$$

où :

$$\mu := 2 + \frac{d}{r}h(\Phi)c(\Phi);$$

$$\kappa := 1 + \frac{3d}{r}h(\Phi)c(\Phi);$$

$$\lambda := 1 + \frac{2d}{r}h(\Phi)c(\Phi);$$

et :

$$C = C_0 \texttt{ sous l'hypothèse } RV(r);$$

$$\exists 0 < C \leq C_0 \texttt{ sous l'hypothèse } RV(r)^*.$$

La majoration $D_{p.i.} \leq D$ nous donne alors le résultat suivant :

Corollaire 1.1.9. *Sous les mêmes hypothèses et définitions du Théorème 1.1.8 on a la minoration suivante :*

$$\widehat{h}(x) \geq C\frac{(\log\log_+ D)^{\mu}}{D^{1+\lambda}(\log_+ D)^{\kappa}}.$$

Nous remarquons que de telles minorations sont valables, grâce à la notation $\log_+(.)$ et $\log\log_+(.)$ introduite auparavant, pour toute valeur de $D \in \mathbb{N} \setminus \{0\}$.

Il est clair que la condition RV$(r)^*$ est impliquée par la RV(r) quelque soit $r \in]0,1]$. Nous nous contenterons cependant d'examiner le cas RV(r) dans la plupart des calculs, la méthode étant presque la même dans le cas RV$(r)^*$, quitte à modifier un point important (voir Lemme 1.3.7 et Remarque 1.3.8) à la fin de cette démarche.

Remarque 1.1.10. *Soient $\mathbb{D}_1 = (\Phi_1, \mathbb{G}_a)$ et $\mathbb{D}_2 = (\Phi_2, \mathbb{G}_a)$ deux modules de Drinfeld définis respectivement sur les corps de coefficients $k(\Phi_1)$ et $k(\Phi_2)$, ayant des hauteurs canoniques respectives $\widehat{h}_{\mathbb{D}_1}$ et $\widehat{h}_{\mathbb{D}_2}$. Soit $\mathcal{F} := k(\Phi_1)k(\Phi_2)$ le compositum des deux corps des coefficients. Dire que $\mathbb{D}_1$ et $\mathbb{D}_2$ sont isomorphes (voir [Goss], Proposition 4.7.1, page 79) c'est affirmer l'existence d'un élément u non nul dans $\mathcal{C}$ tel que (en identifiant u avec l'homothétie de rapport u) :*

$$u \circ \Phi_1(T) = \Phi_2(T) \circ u.$$

$\mathbb{D}_1$ et $\mathbb{D}_2$ sont alors nécessairement de même rang d et u appartient à une extension $\mathcal{E}$ de $\mathcal{F}$ de degré $\leq q^d - 1$. On a donc (voir [Den1], Corollaire 2, page 217) que :

$$\widehat{h}_{\mathbb{D}_1}(x) = \widehat{h}_{\mathbb{D}_2}(ux);$$

pour tout $x \in \overline{k}$. Minorer $\widehat{h}_{\mathbb{D}_1}(x)$ revient donc à minorer $\widehat{h}_{\mathbb{D}_2}(ux)$. Si on applique les Théorèmes précédents au module $\mathbb{D}_2$, au point ux et donc à son degré :

$$[k(ux) : k] \leq [k(x) : k][\mathcal{E} : \mathcal{F}][\mathcal{F} : k] \leq [k(x) : k](q^d - 1)c(\Phi_1)c(\Phi_2);$$

on obtient une minoration de $\widehat{h}_{\mathbb{D}_1}(x)$ similaire à celle des Théorèmes précédents.

Par conséquent si un module de Drinfeld est isomorphe à un module vérifiant une de nos condition $\mathrm{RV}(r)$ ou $\mathrm{RV}(r)^*$, on a également pour celui -ci une minoration de sa hauteur canonique du même ordre de grandeur. C'est en particulier le cas pour les modules de rang 1 qui sont tous isomorphes au module de Carlitz.

Nous allons prouver d'abord le Théorème 1.1.7 au cour du paragraphe 3.1. On montrera ensuite, dans le paragraphe 3.2, le Théorème 1.1.8, dont le Théorème 1.1.7 est conséquence directe.

1.2 Résultats préliminaires

Dans cette partie on trouvera les résultats de base nécessaires au bon déroulement de la preuve. Il s'agit essentiellement de théorèmes bien connus et dont la plupartie sont démontrés par L. Denis dans [Den1].

De façon analogue à l'existence des fonctions abéliennes dont l'image définit une variété abélienne, dans le cas des modules de Drinfeld il existe aussi une *fonction exponentielle*, entière sur $\mathcal{C}$,

$$e : \mathcal{C} \twoheadrightarrow \mathbb{D}$$

dont le noyau est un $A-$réseau Λ de rang d dans $\mathcal{C}$. Cette fonction est compatible avec la structure de module de Drinfeld de $\mathbb{D} = (\mathbb{G}_a, \Phi)$ de la façon suivante :

$$e(az) = \Phi(a)(e(z)), \texttt{ pour tout } a \in A.$$

Observons que la non-compacité de $\mathbb{D}$ par rapport à la topologie $1/T-$adique empêche que ce Λ satisfasse un analogue du "'Principe des tiroirs"', qui est en revanche une propriété des variétés abéliennes [2].

Soit $\mathbb{P}^n(\overline{k})$ l'espace projectif de dimension n défini sur $\overline{k}$. La *hauteur logarithmique* ou *hauteur de Weil* de tout point $P = [P_0 : ... : P_n] \in \mathbb{P}^n(\overline{k})$ est la fonction h définie de la manière suivante :

$$h(P) := \frac{1}{[k(P) : k]} \sum_{w \texttt{ sur } k(P)} n_w \max_{i=0,\dots,n} \{-w(P_i)\};$$

où w indique une extension à $k(P)$ de la place v sur k, qu'on associe à un premier $l \in A \setminus \{0\}$ ou au point $\infty \in \mathbb{P}^1(k)$ comme il suit : si l est un élément $l \in k$, on a :

$$v(x) := \deg_T(l) v_l(x) \ \ \forall x \in k;$$

si au contraire cette v représente le point ∞ de $\mathbb{P}^1(k)$, on a :

$$v(x) := v_\infty(x) := -\deg_T(x) \ \ \forall x \in k.$$

On rappelle également qu'étant donné $x \in \overline{k}$, pour toute place normalisée w sur $k(x)/k$ dont la restriction à k est la place v, on définit :

$$n_w := [k(x)_w : k_v];$$

2. Voir après la Conjecture 4

où k_v et $k(x)_w$ sont, respectivement, les complétés de k par rapport à v et de $k(x)$ par rapport à w. On remarquera également que :

$$n_w = e_w f_w;$$

où e_w et f_w sont, respectivement, l'indice de ramification et le degré d'inertie de $w|v$. .

On remarque que, par définition même d'un espace projectif, un point $P \in \mathbb{P}_n(\overline{k})$ est en effet une classe d'équivalence dans $\overline{k}^{n+1}$ par rapport à la relation suivante :

$$(P_0, ..., P_n) \sim (P'_0, ..., P'_n) \Longleftrightarrow \exists \lambda \in \overline{k}^* / (P'_0, ..., P'_n) = (\lambda P_0, ..., \lambda P_n).$$

L'expression $\mathbb{P}_n(K)$, avec K souscorps de $\overline{k}$, n'est donc pas bien définie. On dit alors que P **est un point** $K-$**rationnel dans** $\mathbb{P}_n(K)$ (ou, de façon équivalente, $P \in \mathbb{P}_n(K)$), si et seulement si toutes les composantes du représentant de P ayant sa première composante $P_0 = 1$, sont dans K.

La hauteur logarithmique d'un point $\overline{x} = (x_1, ..., x_n)$ dans l'espace affine $\overline{k}^n$ algébrique de degré D sur k, est définie en plongeant $\overline{k}^n$ dans $\mathbb{P}^n(\overline{k})$ de façon que $\overline{x}$ corresponde à la classe d'équivalence $[1 : x_1 : ... : x_n]$. On aura, donc :

$$h(\overline{x}) := \frac{1}{D} \sum_{w \ \mathtt{sur} \ k(x)} n_w \max_{i=1,...,n} \{0, -w(x_i)\}.$$

La définition de **hauteur logarithmique**, ou **hauteur de Weil** d'un point $x \in \overline{k}$, de degré D sur k est, alors, obtenue en voyant x en tant que classe d'équivalence $[1 : x] \in \mathbb{P}^1(\overline{k})$:

$$h(x) := \frac{1}{D} \sum_{w \ \mathtt{sur} \ k(x)/k} n_w \max\{0, -w(x)\}.$$

Nous donnons ici les propriétés principales de la hauteur logarithmique sur $\overline{k}^n$, quelque soit $n \in \mathbb{N} \setminus \{0\}$, dont on servira dans le passages fondamentaux à venir.

Proposition 1.2.1. *1. Soient $\overline{\alpha}, \overline{\beta} \in \overline{k}^n$. Alors :*

$$h(\overline{\alpha} + \overline{\beta}) \leq h(\overline{\alpha}) + h(\overline{\beta}). \tag{1.1}$$

2. Soient $\overline{\alpha}, \overline{\beta} \in \overline{k}^n$. Soit $\overline{\alpha}\overline{\beta} \in \overline{k}^n$ le produit terme à terme de $\overline{\alpha}$ et $\overline{\beta}$. Alors :

$$h(\overline{\alpha}\overline{\beta}) \leq h(\overline{\alpha}) + h(\overline{\beta}). \tag{1.2}$$

3. Soient $\overline{\alpha}, \overline{\beta} \in \overline{k}^n$. Soit $(\overline{\alpha}, \overline{\beta}) \in \overline{k}^{2n}$ le vecteur à $2n$ composantes obtenu en prolongeant $\overline{\alpha}$ avec les cordonnées de $\overline{\beta}$. Alors :

$$h(\overline{\alpha} + \overline{\beta}) \leq h(\overline{\alpha}, \overline{\beta}). \tag{1.3}$$

Il s'agit de propriétés impliquées de façon assez directe par les définitions.

En parallèle à la notion de hauteur d'un point algébrique dans un espace projectif, nous définissons ci-dessous la hauteur d'un polynôme, en voyant la bijection naturelle existant entre l'espace de polynômes à une variable de degré au plus D à coefficients dans l'extension finie K de k et les points de K^{D+1}.

Définition 1.2.2. *Soit $P(X) = b_0 + b_1X + ... + b_DX^D$ un polynôme de degré D (donc, tel que $b_D \neq 0$) à une variable à coefficients dans $\overline{k}$. La* ***hauteur de*** *$P(X)$ est :*

$$h(P(X)) := h([1 : b_0 : ... : b_D]).$$

La **hauteur du module de Drinfeld** Φ (dont les coefficients sont toujours $b_0, ..., b_d \in k(\Phi)$ comme dans la définition 1.1.1), qu'on indiquera avec la notation $h(\Phi)$ est définie comme il suit :

$$h(\Phi) := \frac{1}{c(\Phi)} \sum_{w \texttt{ sur } k(\Phi)/k} n_w \max_{i=0,\ldots,d}\{0, -w(b_i)\}.$$

Nous remarquons que :

$$h(\Phi) \geq 1.$$

En effet, on a que :

$$h(\Phi) = \frac{1}{c(\Phi)} \sum_{w \texttt{ sur } k(\Phi)/k} n_w \max_{i=0,\ldots,d}\{0, -w(b_i)\} \geq \frac{1}{c(\Phi)} \sum_{w \texttt{ sur } k(\Phi)/k} n_w \max\{0, -w(T)\} =$$

$$= \frac{1}{c(\Phi)} \sum_{v \texttt{ sur } k} \sum_{w|v} n_w \max\{0, -v(T)\} = \sum_{v \texttt{ sur } k} \max\{0, -v(T)\} = h([1 : T]) = 1.$$

La **hauteur de Néron-Tate**, ou **hauteur canonique** sur un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ de rang d est la forme polynomiale de degré d dans la décomposition de Néron-Tate de la hauteur logarithmique. Une telle décomposition existe en effet même dans le cas des modules de Drinfeld, n'incluant qu'une partie polynomiale à degré d et une partie bornée. L'expression explicite de cette hauteur canonique, définie dans le travail de L. Denis [Den1], est :

$$\widehat{h}_{\mathbb{D}}(x) = \lim_{n\to\infty} \frac{h(\Phi(T^n)(x))}{q^{dn}}.$$

Nous indiquerons dorénavant plus simplement avec la notation $\widehat{h}$ la hauteur canonique liée à un module de Drinfeld assigné, là où il y en a qu'un seul et on n'a pas donc de risque d'ambiguité.

En sachant que l'ensemble des points de torsion d'un module de Drinfeld est, comme dans le cas également des variétés abéliennes, le lieu des zéros de la hauteur canonique sur ce module, il est donc naturel de se demander s'il existe une borne inférieure pas nulle (fonction du degré de x) de la hauteur canonique de x point pas de torsion.

Ce problème n'est qu'une version très particulière du plus ancien Problème de Lehmer. Cette dernière est liée à une situation assez différente, où le domaine d'étude est celui des corps de nombres. Précisément, on définit sur le groupe multiplicatif $\mathbb{G}_m(\overline{\mathbb{Q}})$ un analogue de la hauteur de Weil absolue, qu'on appelle également h, dont les zéros sont les racines de l'unité (correspondants aux points de torsion), et on pose (voir [Leh], page 476) la conjecture suivante :

Conjecture 3. *Il existe une constante $c > 0$ telle que si P est un point algébrique de degré D sur $\mathbb{Q}$ qui n'est pas racine de l'unité :*

$$h(P) \geq \frac{c}{D}.$$

La meilleure minoration de h (vis à vis de la dépendance en D) actuellement connue a été obtenue par E. Dobrowolski [Dob] :

Théorème 1.2.3. *Il existe une constante $c > 0$ telle que pour tout $x \in \mathbb{G}_m(\overline{\mathbb{Q}})$, de degré D sur $\mathbb{Q}$ qui n'est pas une racine de l'unité :*

$$h(x) \geq \frac{c}{D}(\frac{\log\log(3D)}{\log(3D)})^3.$$

Comme le groupe multiplicatif est un exemple de groupe abélien doté d'une structure de variété algébrique sur lequel le Problème de Lehmer a un sens, c'est de la même manière naturel de se poser la question analogue dans le cas des courbes elliptiques. La Conjecture de Lehmer Elliptique prend alors (voir [AM]) la forme suivante :

Conjecture 4. *Soit E une courbe elliptique définie sur un corps de nombres K. Il existe une constante $c = c(E/K)$ ne dépendant que du choix de E, telle que, si P est un point pas de torsion de E :*

$$\widehat{h}(P) \geq \frac{c(E/K)}{[K(P):K]}.$$

Beaucoup de méthodes ont été développés pour parvenir à des bonnes minorations de la hauteur canonique dans le cadre des variétés abéliennes, comme on montrera dans le tableau qui suit. Un nombre important d'entre elles se basent cependant sur la compacité des variétés abéliennes en tant qu'espaces topologiques, le "Principe des Tiroirs" donnant une condition très puissante qui s'applique aux pré-images des points de la variété par les fonctions abéliennes, modulo le réseau. Grâce à cette condition, qui malheureusement n'est pas respectée par les $T-$modules, on observe, en gros, qu'on ne peut pas avoir trop de points de torsion modulo le réseau dans la "boîte" formée par les périodes de ce dernier et on parvient à l'estimation finale par contradiction (voir, par exemple, [Mas1]). C'est fondamentalement l'absence de cette condition qui pose les problèmes principaux avec les modules de Drinfeld (et, plus généralement, avec les $T-$modules), nous forçant à imposer la condition RV(r).

Le tableau qui suit résume l'histoire des trois principales minorations connues en fonctions des hypothèses qu'on ajoute éventuellement à la courbe elliptique E, parmi lequelles figure celle de la **multiplication complexe**, qu'on examinera plus attentivement dans l'Appendice, et qui peut très facilement être formulée même pour un module de Drinfeld. En particulier, il s'agit d'une condition beaucoup plus puissante que l'hypothèse RV (voir la définition 1.1.5), qui en est d'ailleurs conséquence sous certaines hypothèses (voir Appendice) .

$\widehat{h}(P) \geq$	RESTRICTION	REFERENCE
$\frac{c}{D}(\frac{\log\log D}{\log D})^3$	CM	M. Laurent (1983)[Lau1]
$\frac{c}{D^3(\log D)^2}$	aucune	D. Masser (1989)[Mas1]
$\frac{c}{D^2(\log D)^2}$	$j(E) \notin \mathbb{Z}$	M. Hindry-J. Silverman (1990)[HS]

Etant donné un module de Drinfeld, la Conjecture de Lehmer se reformule de façon similaire à celle elliptique dans ce cadre (voir Conjecture 2).

On dispose déjà de nombreux résultats dans ce cadre, dont certains sont relatifs à des conditions particulières respectées par les modules de Drinfeld qu'on examine. L'un des premiers est une consequénce du Théorème de Northcott dans le cas des modules de Drinfeld (voir Théorème 1.2.8) et offre une toute première minoration de la hauteur canonique, de l'ordre de $c_2^{-D^2}$, pour une constante $c_2 > 0$ à préciser (voir Théorème 1.2.10). Il s'agit donc encore d'une estimation assez mauvaise, mais qui conduira au résultat expliqué dans les Théorèmes 1.1.7 et 1.1.8.

Dans le cas particulier du module de Carlitz, un cas spécial où le rang du module est 1, L. Denis (voir [Den1]) obtient une minoration optimale à une puissance de $\log D$ près avec une hypothèse de séparabilité dont nous verrons plus loin qu'on peut l'amoindrir. Il s'agit d'un module de Drinfeld de type CM (ou, à **multiplication complexe**, voir l'Appendice pour la définition) et, en particulier, de type RV aussi (voir la définition 1.1.5 et les considérations successives pour la notation RV) :

Théorème 1.2.4. *Soit $\mathbb{D}$ un module de Carlitz. Il existe un réel $\eta > 0$ effectivement calculable en fonction de q tel que pour tout x algébrique et séparable de degré $\leq D$ sur k, pas de torsion par rapport à $\mathbb{D}$, on ait :*

$$\widehat{h}(x) \geq \frac{\eta}{D}\left(\frac{\log\log(qD)}{\log(qD)}\right)^3.$$

Dans une autre direction, sans hypothèse initiale sur le module de Drinfeld, sans hypothèse de séparabilité sur le point x mais en supposant vérifiée une condition locale sur x portant sur le comportement de ses valuations en une place au dessus de l'infini (plus précisément, l'hypothèse supplémentaire porte sur la hauteur locale en x qui dépend donc aussi du module de Drinfeld) D. Ghioca (voir [Gh], Theorem 6.2, Theorem 6.3) montre une minoration du type :

$$\widehat{h}(x) \geq \frac{C}{D^k};$$

pour un certain $k \geq 1$. Une condition supplémentaire sur la nature d'une telle extension de places amène à une borne du type $k \leq d$, où d est le rang du module de Drinfeld.

Un deuxième résultat a été récemment produit par S. David et A. Pacheco (voir [Dav-Pach]) qui ont montré une minoration de la forme suivante :

$$\widehat{h}(x) \geq c(\mathbb{D}, K);$$

pour un module de Drinfeld $\mathbb{D}$ défini sur un corps de fonctions $K \subset \overline{k}$, où $c(\mathbb{D}, K) > 0$ est une constante positive ne dépendant que de $\mathbb{D}$ et de K et $x \in K^{ab.}$, où $K^{ab.}$ est la clôture abélienne de K dans $\overline{k}$. Un tel résultat est l'analogue de celui de F. Amoroso et R. Dvornicich (voir [Am-Dv]) qui avaient montré une estimation sous une telle forme pour la hauteur d'un élément $x \in \mathbb{G}_m(\mathbb{Q}^{ab.}) \setminus \mathbb{G}_m(\mathbb{Q}^{ab.})_{tors.}$.

Proposition 1.2.5. *Si $x \in \overline{k}$, de degré D et de polynôme minimal $P(X) \in k[X]$,*

$$h(P(X)) = Dh(x).$$

Démonstration. Soit $P(X)=\prod_{j=1}^{D}(X-\beta_j)=\sum_{i=0}^{D-1}b'_iX^i+X^D=\frac{1}{b_D}\sum_{i=0}^{D}b_iX^i$ polynôme minimal de l'élément $x\in\overline{k}$, de degré D sur k. En général, les $b'_i\in k$, alors que les $b_i\in A$, $b_D\neq 0$ et ils sont premiers entre eux. Alors :

$$Dh(x)=\sum_{w\ \mathtt{sur}\ k(x)/k}n_w\max\{0,-w(x)\}=\sum_{i=1}^{D}\sum_{v\ \mathtt{sur}\ k}\max\{0,-v(\beta_i)\}.$$

En effet, toute valuation v sur k s'étend à r valuations w sur $k(x)/k$ distinctes, donc à $D=\sum_{i=1}^{r}e_if_i=\sum_{i=1}^{r}n_{w_i}$ valuations éventuellement égales ; d'ailleurs, en indiquant toujours par v l'extension canonique de v à $k(x)$ (v admet une unique extension à k_v, qui s'étend encore de façon unique à $k_v(x)=k(x)_v$, se restreignant finalement à une extension particulière de v à $k(x)$, que nous appelons **canonique**), toute $w|v$ sur $k(x)$ est nécessairement de la forme $w(x)=(v\circ\sigma_i)(x)=v(\alpha_i)$, pour un certain $\sigma_i\in\mathcal{I}(k(x)/k)$, ensemble des $k-$isomorphismes de $k(x)$ (i entre 1 et D) [3]. Nous rappelons que tout a'_i dans l'expression de $P(X)$ se calcule en tant que fonction symétrique élémentaire des racines β_i sous la forme :

$$b'_i=\sum_{j=1}^{\binom{D}{i}}\prod_{l_j=1}^{i}\beta_{l_j}.$$

Si, pour v sur k fixée, $v(\beta_i)>0$ pour tout i entre 1 et D, alors, toutes les racines de $P(X)$ sont dans l'idéal maximal $\mathcal{M}_v$ de l'anneau de valuation de $k(x)_v$, la structure algébrique d'un idéal implique nécessairement, alors, que tout leur produit et somme reste dans le même idéal, donc, aura toujours valuation strictement positive. Dans ce cas, l'expression de b'_i avec les β_i montre comment $v(b'_i)>0$ pour tout i entre 0 et $D-1$; on aura donc : $h(P(X))=0=h(x)$, ce qui est en accord avec l'affirmation qu'on veut montrer. On peut donc supposer, sans perte de généralité, qu'un nombre r_v compris entre 1 et D de racines β_i de $P(X)$ aient une valuation v strictement négative. Dans ce cas, b'_{r_v} est le coefficient de $P(X)$ de valuation v minimale, et telle que :

$$-v(b'_{r_v})=\sum_{i=1}^{r_v}-v(\beta_{v,i})=\sum_{i=1}^{D}\max\{0,-v(\beta_i)\},$$

avec $\beta_{v,i}$ les r_v racines de $P(X)$ à valuation négative. On a, alors, que :

$$h(P(X))=\sum_{v\ \mathtt{sur}\ k}\max_{i=0,\ldots,D-1}\{0,-v(b'_i)\}=\sum_{v\ \mathtt{sur}\ k}\max_{i=0,\ldots,D-1}\{0,-\sum_{j=1}^{D}v(\beta_j)\}=$$

$$=\sum_{v\ \mathtt{sur}\ k}\sum_{i=1}^{D}\max\{0,-v(\beta_i)\}=Dh(x).$$

□

On remarque que la même preuve, et donc le même résultat, ne reste pas valable dans le cas des corps de nombres, suite à la présence d'une valuation

3. Voir [BG] pour des preuves détaillées

archimédienne (correspondant à la place à l'infini) qui reste au contraire ultramétrique ($\deg_T$) dans notre situation. Le résultat reste néanmoins valable dans notre cas quelque soit l'hypothèse de séparabilité sur $k(x)/k$. En effet, on a que $D = D_{sep.} D_{p.i.}$, avec, respectivement, $D_{sep.}$ degré de séparabilité et $D_{p.i.}$ degré de pure inséparabilité de $k(x)/k$, et donc :

$$Dh(x) = \sum_{i=1}^{D_{sep.}} \sum_{v \text{ sur } k} D_{p.i.} n_v \max\{0, -v(\alpha_i)\};$$

pour $v(\alpha_i)$ extension unique de v sur α_i dans l'extension des corps $k(x)/k^{p.i.}$. Ce qui laisse inchangées les mêmes formules utilisées dans la preuve.

Proposition 1.2.6. *Soit $\mathbb{D} = (\mathbb{G}_a, \Phi)$ un module de Drinfeld fixé. Il existe alors une valeur $\gamma(\Phi) > 0$, ne dépendant que de Φ, telle que,*

$$\gamma(\Phi) := \sup_{x \in \overline{k}} |h(x) - \widehat{h}(x)|.$$

On sait qu'une telle valeur est liée à la hauteur du module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ et devient donc une donnée importante dont va dépendre la méthode de la démonstration. Dans le cas précis, on dispose du résultat suivant, par L. Denis [Den2].

Théorème 1.2.7. *Etant donné un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ de rang d, s'exprimant comme :*

$$\Phi(T)(\tau) = T + a_1(T)\tau + ... + a_d(T)\tau^d;$$

la constante $\gamma > 0$ qu'on lui associe est majorée de la façon suivante :

$$\gamma < \frac{q^d}{(q-1)(q^d-1)} h(a_1, ..., a_d, 1/a_1, ..., 1/a_d);$$

où on convient d'enlever de cette expression les éléments $1/a_i$ quand le a_i correspondant est 0.

On en tire l'estimation :

$$\gamma < 2(d+1)h(\Phi). \tag{1.4}$$

En effet, comme $q \geq 2$ et $d \geq 1$, on en a $\frac{q^d}{(q-1)(q^d-1)} \leq 2$; d'un autre côté :

$$h([1 : a_1 : ... : a_d : 1/a_1 : ... : 1/a_d]) =$$
$$= h([1 : a_1 : ... : a_d : 1 : ... : 1][1 : 1 : ... : 1 : 1/a_1 : ... : 1/a_d]) \leq$$
$$\leq h([1 : a_1 : ... : a_d]) + h([1 : 1/a_1 : ... : 1/a_d]).$$

On a alors que :

$$[1 : 1/a_1 : ... : 1/a_d] = [a_1 : 1 : a_1 : ... : a_1][a_2 : a_2 : 1 : a_2 : ... : a_2]...[a_d : ... : a_d : 1].$$

En exprimant chacun de ces éléments sous la forme : $[a_i : ... : a_i : 1 : a_i : ... : a_i]$, où la valeur 1 apparaît à la position $i+1$ pour tout $i = 1, ..., d$, ils se décomposent de suivante manière :

$$[a_i : ... : a_i : 1 : a_i : ... : a_i] = [a_i : 1 : ... : 1]...[1 : 1 : ... : 1 : a_i].$$

Nous avons alors, pour chaque $i = 1, ..., d$ exactement un vecteur où a_i apparaît au fur et à mesure en chaque position sauf la $(i+1)-$ème. Il est donc possible de multiplier à nouveau tous les termes dans un ordre opportun, de manière à obtenir un produit de d vecteurs ayant des a_i différents en chaque position, sauf une, occupée par 1. Comme la hauteur de chacun de ces termes est toujours $h([1 : a_1 : ... : a_d])$, la propriété (1.2) nous donne finalement la minoration annoncée.

Un tout premier résultat important pour l'effectivité de la théorie est le **théorème de Northcott**, valable à la fois dans le cas des corps de fonctions et de corps de nombres :

Théorème 1.2.8. *On considère le corps k (respectivement, le corps $\mathbb{Q}$ dans le cas de corps de nombres) ; il est plongé dans $\mathcal{C}$ (respectivement, $\mathbb{Q} \subset \mathbb{C}$), qui est un corps algébriquement clos et complet. Soient $A, B > 0$ deux constantes fixées. Alors, l'ensemble des points $\overline{x} \in \overline{k}^n$, quelque soit $n \in \mathbb{N} \setminus \{0\}$ (respectivement, $\overline{x} \in \overline{\mathbb{Q}}^n$, où $\overline{\mathbb{Q}}$ est une clôture algébrique fixée de $\mathbb{Q}$ dans $\mathbb{C}$) tels qu'on ait $[k(\overline{x}) : k] \leq A$ (respectivement, $[\mathbb{Q}(\overline{x}) : \mathbb{Q}] \leq A$) et $h(\overline{x}) \leq B$ (respectivement, $h_{\mathbb{Q}}(\overline{x}) \leq B$, où $h_{\mathbb{Q}}$ est la hauteur logarithmique définie sur $\mathbb{Q}$, voir par exemple [BG] pour la définition) est fini.*

Démonstration. Voir [Se1], page 16, pour le cas relatif aux corps de nombres. Faute de référence, le cas du corps k vient assez directement du lemme qui suit (cas $n = 1$). □

Plusieurs travaux ont étés produits dans le but de trouver une borne supérieure effective la plus précise possible en fonction de ceux du degré algébrique et de la hauteur. Dans le cas d'un module de Drinfeld une estimation suffisante à nos objectifs est la suivante :

Lemme 1.2.9. *Pour tout $\chi \geq 1$, étant donné $D \geq 1$, on a que :*

$$|\{x \in \overline{k}, [k(x) : k] \leq D, h(x) \leq \chi\}| \leq q^{5D^2\chi}.$$

Démonstration. A tout $x \in \overline{k}$ de degré D sur k on associe l'un des ses polynômes minimaux entiers $P(X)$ de degré D à coefficients dans A, premiers entre eux (pas forcément unitaire). Soit $P_1(X)$ le polynôme unitaire qu'on obtient en divisant $P(X)$ par le coefficient dominant de ce dernier. Comme, d'après la Proposition 1.2.5, $Dh(x) = h(P_1(X))$, nous essayons de compter combien de polynômes à coefficients dans A premiers entre eux sont des polynômes minimaux des x dans l'ensemble qu'on étudie, avec un degré majoré par D et valeur en $\deg_T$ de leurs coefficients majorés par $D\chi$. On notera :

$$P_1(X) = \sum_{i=0}^{D-1} \frac{a_i}{a_D} X^i + X^D = \frac{1}{a_D} P(X).$$

Nous remarquons que :

$$h(P_1(X)) = h([1 : a_0/a_D : ... : a_{D-1}/a_D : 1]) = h([a_0 : ... : a_D]) =$$

$$= \sum_{v \texttt{ sur } k} \max_{i=0,\ldots,D} \{-v(a_i)\} = \max_{i=0,\ldots,D} \{-v_{1/T}(a_i)\} = \max_{i=0,\ldots,D} \{\deg_T(a_i)\}.$$

On a, donc :

$$|\{P(X) \in A[X] \setminus A, \deg_X(P(X)) \leq D, h(P_1(X)) \leq D\chi\}| \leq q^{(D\chi+1)(D+1)}.$$

Or, comme tout polynôme irréductible de degré D admet au plus D racines distinctes, le nombre de ces polynômes, respectant les conditions sur leur degré et leur hauteur, doit être multiplié par D. En définitif :

$$|\{x \in \overline{k}, [k(x) : k] \leq D, h(x) \leq \chi\}| \leq Dq^{(D\chi+1)(D+1)} \leq Dq^{\kappa D^2\chi} \leq q^{\widetilde{c}D^2\chi},$$

pour $\widetilde{c} > \kappa > 1$ opportunes. On remarque que les constantes κ et $\widetilde{c}$ ne sont pas universelles, mais dépendent de la valeur minimale de χ. Plus précisément, ils augmentent pour tout choix de χ de plus en plus petit. Pour $\chi \geq 1$, un choix acceptable immédiat est : $\kappa = 4$ et $\widetilde{c} = 5$. $\square$

Théorème 1.2.10. *Soit $\mathbb{D} = (\mathbb{G}_a, \Phi)$ un module de Drinfeld quelconque de rang d. Il existe alors une constante positive $c_2 = q^{5d(2(d+1)h(\Phi)+1)c(\Phi)^2}$ telle que, si $x \in \mathbb{D}(\overline{k})_{NT}$ et $D = [k(x) : k]$, on a l'estimation suivante :*

$$\widehat{h}(x) \geq \frac{1}{c_2^{D^2}}.$$

Démonstration. Si $\widehat{h}(x) \leq 1$, par la Proposition 1.2.6 et le Théorème 1.2.7, $h(x) \leq 1 + \gamma \leq 1 + 2(d+1)h(\Phi)$. Un majorant du nombre d'éléments de cet ensemble est alors, par le Lemme 1.2.9 : $q^{5D^2(1+\gamma)}$. S'il existe $c_3 > 0$ tel que $x \in \mathbb{D}(\overline{k})_{NT}$ de degré D sur k et de hauteur canonique telle que $\widehat{h}(x) < \frac{1}{q^{c_3D^2c(\Phi)^2}}$, tout élément $a \in A$ de degré $\deg_T(a)$ en T serait tel que :

$$\widehat{h}(\Phi(a)(x)) = q^{d\deg_T(a)}\widehat{h}(x) < \frac{q^{d\deg_T(a)}}{q^{c_3D^2c(\Phi)^2}}.$$

On choisit c_3 assez grande pour que cette dernière valeur soit ≤ 1. On obtient que :

$$q^{d\deg_T(a)-c_3D^2c(\Phi)^2} \leq 1.$$

Ce qui signifie :

$$\deg_T(a) \leq \frac{c_3D^2c(\Phi)^2}{d}.$$

L'estimation qu'on a tirée du Lemme 1.2.9 et de la Proposition 1.2.6 nous permet de dire que le nombre d'éléments y algébriques de degré au plus $Dc(\Phi)$ sur k et dont la hauteur h est telle que $h(y) \leq 1 + 2(d+1)h(\Phi)$, est au plus $q^{5(1+2(d+1)h(\Phi))D^2c(\Phi)^2}$. Nous remarquons que pour tout $a \in A \setminus \{0\}$ de degré $\deg_T(a) \leq M$ où M est un entier fixé, l'élément $y = \Phi(a)(x)$ est algébrique de degré $[k(\Phi, x) : k] \leq Dc(\Phi)$. Or, le nombre des $\Phi(a)(x)$ est, si x n'est pas de torsion (donc, $a \neq b \Longrightarrow \Phi(a)(x) \neq \Phi(b)(x)$), exactement q^{M+1}. En imposant, alors, $M = [\frac{1}{d}(c_3D^2c(\Phi)^2)]$, on aura nécessairement au moins q^{M+1} éléments distincts avec degré sur k au plus $Dc(\Phi)$ et hauteur canonique au plus 1. On sait également que cet ensemble contient au plus $q^{5(1+2(d+1)h(\Phi))D^2c(\Phi)^2}$ éléments. Donc, pour $c_3 = 5d(1 + 2(d+1)h(\Phi))$:

$$[\frac{c_3D^2c(\Phi)^2}{d}] + 1 > 5(1 + 2(d+1)h(\Phi))D^2c(\Phi)^2,$$

achevant la preuve pour $c_2 := q^{c_3 c(\Phi)^2}$. On remarque, ensuite, qu'il est possible d'exprimer c_2 en fonction uniquement de $h(\Phi)$, de d et de $c(\Phi)$, comme c'est le cas pour c_3. On peut alors poser :

$$c_2 = q^{5d(2(d+1)h(\Phi)+1)c(\Phi)^2}.$$

$\square$

Corollaire 1.2.11. *Pour tout $N \in \mathbb{N} \setminus \{0\}$ et pour tout $1 \leq D \leq N$:*

$$\widehat{h}(x) \geq c_2^{-N^2};$$

pour tout $x \in \mathbb{D}(\overline{k})_{NT}$ de degré algébrique sur k au plus N.

Démonstration. Comme conséquence du Lemme 1.2.9 on sait que :

$$\widehat{h}(x) \geq c_2^{-D^2};$$

pour tout $D \geq 1$. Si, alors, x algébrique de degré D sur k, pour $D \leq N$:

$$\widehat{h}(x) \geq c_2^{-N^2}.$$

$\square$

Proposition 1.2.12. *Le nombre X des polynômes unitaires et irréductibles dans A de degré N, pour $N \in \mathbb{N} \setminus \{0\}$, vérifie l'estimation :*

$$\frac{1}{2}\frac{q^N}{N} \leq X \leq \frac{q^N}{N}.$$

Démonstration. La valeur exacte de X en fonction de N est :

$$X = 1/N \sum_{d|N} \mu(N/d) q^d;$$

où μ est la fonction de Moebius, comme montré dans le livre de K. Ireland et M. Rosen [IR], page 84. Alors, pour tout $d|N$, $\mu(N/d) \leq 1$, ce qui donne l'inégalité, pour [4] $N \geq 2$:

$$X - \frac{q^N}{N} \leq \sum_{i=2}^{N} \frac{q^{[N/i]}}{N} \leq \frac{1}{N} \sum_{i=1}^{[N/2]} q^i \leq \frac{1}{N} \frac{q^{(N/2)+1} - q}{q-1} =$$

$$= \frac{1}{N} \frac{q}{q-1} (q^{N/2} - 1) \leq \frac{1}{2} \frac{q^N}{N},$$

comme $q^{N/2} - 1 \leq \frac{q-1}{2q} q^N$ pour tout q et N comme dans les hypothèses. Ce qui nous donne une première inégalité :

$$X \leq \frac{3}{2} \frac{q^N}{N}.$$

D'un autre coté,

$$X = |\frac{q^N}{N} + \frac{1}{N} \sum_{d|N, d \neq N} \mu(\frac{N}{d}) q^d| =$$

4. Pour $N = 1$ il suffit de se rappeler que $X = q$, ce qui respecte l'énoncé.

$$= |\frac{q^N}{N} - (-\frac{1}{N}\sum_{d|N, d\neq N}\mu(\frac{N}{d})q^d)| \geq \frac{q^N}{N} - \frac{q}{q-1}(q^{N/2}-1) \geq \frac{1}{2}\frac{q^N}{N},$$

grâce à la majoration précédente de la différence entre la valeur totale et le terme principal.

Finalement, se souvenant d'un important analogue en $\mathbb{F}_q[T]$ de la décomposition du polynôme $T^m - 1$ dans $\mathbb{Q}[T]$ en polynômes cyclotomiques de degré divisant m, pour lequel on a :

$$T^{q^N} - T = \prod_{d|N}\phi_d(T);$$

$\phi_d(T) \in \mathbb{F}_q[T]$ produit des polynômes irréductibles et unitaires de degré d, en appelant X_d le nombre de ces derniers, on a :

$$\deg_T(\prod_{d|N}\phi_d(T)) = NX + \sum_{d|N, d\neq N} dX_d = \deg_T(T^{q^N} - T).$$

En particulier, on a :

$$X \leq \frac{q^N}{N}.$$

□

Une conséquence de la Proposition 1.2.12 est, comme déjà remarqué après la définition 1.1.6, la possibilité de se réduire effectivement à considérer la situation $c_1 = 1/2$ dans le cas où $r = 1$. En effet, si le nombre des polynômes irréductibles et unitaires de degré N est au moins $q^N/2N$, ce sera le même à plus forte raison pour le nombre des polynômes irréductibles et unitaires de degré $\leq N$.

On remarque, d'ailleurs, comment une deuxième conséquence de cette Proposition est l'impossibilité de l'existence d'une hypothétique formulation de la condition RV(r) pour un module de Drinfeld, dans le cas où $r > 1$. Une telle condition entrerait immédiatement en conflit avec le fait que le nombre total des polynômes irréductibles et unitaires de degré $\leq N$ soit de l'ordre $q^N/N + q^{N-1}/(N-1) + ... + q \leq q^N$, alors qu'un sous-ensemble à priori strict de celui ci aurait cardinalité d'ordre $q^{rN}/2N$, pour $r > 1$, ce qui est impossible pour N très grand.

On énonce, finalement, le véritable résultat clé dont on se servira pour prouver les Théorèmes 1.1.7 et 1.1.8 ; il s'agit du **Lemme de Siegel**, dont la preuve est à repérer dans [Den1] :

Lemme 1.2.13. *Soient $a_{j,i}$ ($1 \leq i \leq N$, $1 \leq j \leq M$) des éléments de $\overline{k}$ engendrant une extension $\widetilde{k}/k$ finie de degré D. Supposons $N > MD$. Alors il existe des éléments $x_1, ..., x_N \in A$, pas tous 0, vérifiant :*

$$\sum_{1\leq i\leq N} x_i a_{j,i} = 0$$

pour tout $1 \leq j \leq M$, tels que

$$\deg_T(x_i) \leq \frac{D}{N - MD}\sum_{1\leq j\leq M} h(a_{j,1}, ..., a_{j,N})$$

pour tout $1 \leq i \leq N$.

Dorénavant on supposera que le module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ est RV(r).

La démarche de la preuve du Théorème 1.1.7 (et du Théorème 1.1.8) consiste à montrer que l'Hypothèse suivante, qu'on supposera satisfaite jusqu'à parvenir à une contradiction, est fausse :

Hypothèse 1. *Pour toute* $C > 0$ *il existe* $x \in \mathbb{D}(\overline{k})_{NT}$, *de degré algébrique* D *sur* k, $D \in \mathbb{N}$, $D \geq q^{q+d+1}$, *tel que*

$$\widehat{h}(x) < C\frac{(\log\log D)^{\mu}}{D(\log D)^{\kappa}};$$

où :

$$\kappa := 2 + \frac{d}{r}h(\Phi)c(\Phi); \tag{1.5}$$

et :

$$\mu := 1 + \frac{2d}{r}h(\Phi)c(\Phi). \tag{1.6}$$

1.3 Polynôme auxiliaire

1.3.1 Cas séparable

Supposons x séparable sur k. On remplacera dorénavant $\overline{k}$ par k^{sep} clôture séparable de k dans $\overline{k}$ et D sera le degré séparable de x sur k. La notation $\mathbb{D}(k^{sep})_{NT}$ indiquera aussi les points pas de torsion du module ed Drinfeld $\mathbb{D}$ algébriques séparables sur k.

Lemme 1.3.1. *1. Soit* $x \in \mathbb{D}(k^{sep})_{NT}$, *soient* $\sigma_1, ..., \sigma_{D'}$ *les différents plongements fixant* $k(\Phi)$ *(où* $D' := [k(\Phi, x) : k(\Phi)]$*) du corps* $k(\Phi, x)$ *dans* $\overline{k}$. *Pour des raisons pratiques on fixera un prolongement de chacun de ces* $k(\Phi)-$*isomorphismes de* $k(\Phi, x)$ *en un automorphisme de* $\overline{k}$ *sans changer leur appellation. Pour tout couple* $(a, b) \in A^2$ *telle que* $a/b \in k \setminus \mathbb{F}_q$, *on a :*

$$\sigma_i(\Phi(a)(x)) \neq \sigma_j(\Phi(b)(x));$$

pour tout couple $(i, j) \in \{1, ..., D'\}^2$.

2. Soit $\boldsymbol{M}$ *un sous ensemble de* A *formé d'éléments premiers entre eux deux à deux tel que pour tout* $a \in \boldsymbol{M}$, *il existe* $i \neq j$, i *et* j *entre* 1 *et* D', *tels que* $\sigma_i(\Phi(a)(x)) = \sigma_j(\Phi(a)(x))$. *Alors, la cardinalité de* $\boldsymbol{M}$ *est majorée par* $\log D'/\log 2$.

Démonstration. 1. Si $\sigma_i(\Phi(a)(x)) = \sigma_j(\Phi(b)(x))$ pour un couple $(i, j) \in \{1, ..., D'\}^2$ et a et b tels que $a/b \notin \mathbb{F}_q$, $\Phi(a)(x)$ et $\Phi(b)(x)$ sont conjugués, donc il existe $\sigma \in G(k_x/k(\Phi))$ (où k_x est la clôture de Galois de $k(\Phi, x)/k(\Phi)$), tel que $\sigma(\Phi(a)(x)) = \Phi(b)(x)$. Comme le groupe de Galois de $k_x/k(\Phi)$ est fini, il existe un ordre μ de σ, tel que $\sigma^{\mu} = id_{k_x}$. On a alors,

$$\Phi(a^{\mu})(x) = \sigma^{\mu}(\Phi(a^{\mu})(x)) = \Phi(a^{\mu-1})(\sigma^{\mu}(\Phi(a)(x))) = \Phi(a^{\mu-1})(\sigma^{\mu-1}(\Phi(b)(x))) =$$

$$= \Phi(a^{\mu-2})(\sigma^{\mu-1}\Phi(a)(\Phi(b)(x))) = \Phi(a^{\mu-2})(\sigma^{\mu-2}\Phi(b^2)(x)) = ... = \Phi(b^{\mu})(x);$$

ce qui veut dire que x est de torsion (comme $a/b \in k \setminus \mathbb{F}_q$ nous avons qu'il existe un élément $a^\mu - b^\mu \in A \setminus \{0\}$ tel que $\Phi(a^\mu - b^\mu)(x) = 0$. Si en effet $a^\mu = b^\mu$ alors a/b est une racine de l'unité dans $\mathbb{F}_q(T)$, ce qui impliquerait que $a/b \in \mathbb{F}_q$), en contradiction avec l'hypothèse.

2. Pour $a \in A$ et j entre 1 et D', soit :

$$I(a,j) = \{i \in \{1, ..., D'\} / \sigma_i(\Phi(a)(x)) = \sigma_j(\Phi(a)(x))\}.$$

On a alors les propriétés suivantes le concernant :

(a) $|I(a,j)| = |I(a,i)|$ pour tout couple $(i,j) \in \{1, ..., D'\}^2$ et deux ensembles différents de cette forme sont disjoints.

(b) Si a et b sont premiers entre eux, $|I(a,i) \cap I(b,j)| \leq 1$.

(c) Si a et b sont premiers entre eux, $|I(ab,j)| \geq |I(a,j)||I(b,j)|$.

Le premier point est conséquence de la Théorie des Corps. Si $i \neq j$ dans $\{1, ..., D'\}$, $r \in I(a,j)$ veut dire que $\Phi(a)(x) \in k(\Phi, x)^{\sigma_j \sigma_r^{-1}}$ et que $k(\Phi)(\Phi(a)(x)) = \cap_{r \in I(a,j)} k(\Phi, x)^{\sigma_j \sigma_r^{-1}}$; $[k(\Phi, x) : k(\Phi)(\Phi(a)(x))] = |I(a,j)|$, ce qui ne dépend pas du j choisi. Par ailleurs, si $I(a,i) \cap I(a,j) \neq \emptyset$, $i \in I(a,j)$ et vice-versa, ce qui fournit une relation d'équivalence entre les éléments de $\{1, ..., D'\}$, d'où le premier point. Pour le deuxième point : si $l, m \in I(a,i) \cap I(b,j)$, $\sigma_m(\Phi(b)(x)) = \sigma_l(\Phi(b)(x))$ et $\sigma_m(\Phi(a)(x)) = \sigma_l(\Phi(a)(x))$, donc grâce au Théorème de Bachet-Bézout, $\sigma_m(\Phi((a,b))(x)) = \sigma_l(\Phi((a,b))(x))$ (où on indique avec la notation (a,b) le plus grand diviseur commun de a et b dans A), et par conséquent, comme l et m sont premiers entre eux, $\sigma_m(x) = \sigma_l(x)$, donc $m = l$. Pour le troisième point, considérons l'inégalité suivante :

$$|I(ab,j)| \geq |\cup_{i \in I(a,j)} I(b,i)|.$$

En effet, comme $l \in I(b,i)$ est tel que $\sigma_l(\Phi(b)(x)) = \sigma_i(\Phi(b)(x))$, à plus forte raison $\sigma_l(\Phi(ab)(x)) = \sigma_i(\Phi(ab)(x)) = \sigma_j(\Phi(ab)(x))$, d'où :

$$\cup_{i \in I(a,j)} I(b,i) \subset I(ab,j).$$

Les deux points précédents montrent alors le troisième.

Finalement, pour n'importe quel i fixé, comme $\mathbf{M}$ est justement l'ensemble des $a \in A$ respectant la condition du point 2 et tels qu'il existe au moins un autre indice $j \neq i$ pour le quel $\sigma_i(\Phi(a)(x)) = \sigma_j(\Phi(a)(x))$, on a facilement que $|I(a,i)| \geq 2$. En conclusion, on peut dire que :

$$2^{|\mathbf{M}|} \leq \prod_{a \in \mathbf{M}} |I(a,i)| \leq |I(\prod_{a \in \mathbf{M}} a, i)| \leq D';$$

ce qui donne :

$$|\mathbf{M}| \leq \frac{\log D'}{\log 2}.$$

□

Corollaire 1.3.2. *La cardinalité de* $\mathbf{M}$ *est donc majorée par* $\log D / \log 2$*, puisque* $D' = [k(\Phi, x) : k(\Phi)] \leq [k(x) : k] \leq D$*. De la même manière, il faut se souvenir du fait que les conjugués distincts de chaque* $\Phi(a)(x)$*, pour* a *qui varie dans* $A \setminus \{0\}$*, sont* D'*.*

Définition 1.3.3. *Soit K un corps de valuation non-archimédienne complet par rapport à celle-ci. Soit $U \subset K$ un ouvert dans K par rapport à la topologie induite sur ce dernier par la valeur absolue $1/T-$adique. Une application :*

$$f : U \to K;$$

est ***analytique sur*** *K si et seulement si elle est sous la forme suivante :*

$$f(z) = \sum_{i \geq 0} a_i z^i, \ \ \forall z \in U;$$

et une telle expression formelle en série de puissances converge à $f(z)$ pour tout $z \in U$. Si $U = K$ on dit que f est ***entière*** *et en particulier que $\lim_{i \to +\infty} a_i R^i = 0$ pour tout $R \in \mathbb{R}_+$.*

La ***dérivée divisée*** *à l'ordre h d'une fonction analytique $f : K \to K$, définie sur un corps K muni d'une métrique et à caractéristique $p > 0$, est la fonction analytique $d^{(h)} : K \to K$ correspondant au coefficient du terme H^h, où $H \in K^*$ est un paramètre quelconque, dans le développement en série de puissances de H de l'expression formelle $f(z + H)$.*

Cette définition peut s'étendre de manière intuitive au *Jacobien divisé* d'une fonction analytique plus générale, du type :

$$f : K^m \to K^n.$$

Remarque 1.3.4. *Etant donné un polynôme $A(X) \in \overline{k}[X] \setminus \{0\}$, un élément $x \in \overline{k}$ est racine de $A(X)$ de multiplicité au moins $h \geq 1$ si et seulement si $d^{(h')}A(x) = 0$ pour tout $h' = 0, ..., h-1$.*

Démonstration. On va procéder par récurrence sur h. Le cas où $h = 1$ est immédiat. Supposons donc $h \geq 2$. Soit $A(X)$ et soit x une racine de $A(X)$. On va montrer d'abord que si elle est de multiplicité h alors les dérivées divisées de $A(X)$ jusqu'à l'ordre $h-1$ s'annulent en x. Si x est racine de $A(X)$ de multiplicité h elle est en particulier racine de $A(X)$ avec multiplicité $h-1$, ce qui veut dire que $A(X)$ admet une décomposition unique dans le domaine factoriel $\overline{k}[X]$ de la forme :

$$A(X) = (X - x)^{h-1} R(X);$$

et, par l'hypothèse de récurrence, ceci revient à dire que :

$$d^{(h')}A(x) = 0;$$

pour chaque $0 \leq h' \leq h-2$. Il nous reste alors à montrer que dans une telle situation, x est racine de $A(X)$ de multiplicité h si et seulement si $d^{(h-1)}A(x) = 0$. En choisissant un paramètre H on développe :

$$A(X + H) = ((X - x) + H)^{h-1} R(X + H);$$

en obtenant :

$$d^{(h-1)}A(X) = \sum_{h'=0}^{h-2} \binom{h-1}{h'} (X - x)^{h-1-h'} d^{(h')} R(X) + R(X).$$

On a donc :

$$d^{(h-1)}A(x) = R(x).$$

Par conséquent, $d^{(h-1)}A(x) = 0$ si et seulement si $R(x) = 0$ ou de façon équivalente, si et seulement si $(X - x)|R(X)$ dans $\overline{k}[X]$. Donc, si et seulement si :

$$A(X) = (X - x)^h \widetilde{R(X)};$$

où $\widetilde{R(X)} = R(X)/(X - x) \in \overline{k}[X]$. Si on suppose par contre que $d^{(h')}A(x) = 0$ pour chaque $h' = 0, ..., h-1$ et donc, en particulier, pour chaque $h' = 0, ..., h-2$, l'hypothèse de récurrence implique que x est racine de $A(X)$ de multiplicité $h - 1$. Comme on est donc à nouveau dans le cas de la même décomposition de $A(X)$ qu'on a déjà étudié avant, si on répète les mêmes passages précédents on retrouve encore une fois que $d^{(h-1)}A(x) = 0$ si et seulement si $R(x) = 0$, ce qui prouve donc que x est racine de $A(X)$ de multiplicité h. □

On se propose premièrement de montrer le Théorème suivant :

Théorème 1.3.5. *Soient $L, t, D \in \mathbb{N}$ tels qu'on ait que :*

$$L^2 > tDc(\Phi).$$

Soit $N \in A$ polynôme en T de degré :

$$\deg_T(N) = \left[\frac{1}{d}\log L\right] + 1.$$

Il existe alors un polynôme :

$$G(X, Y) = \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} p_{ij}X^iY^j \in A[X, Y] \setminus \{0\};$$

de degré au plus $L - 1$ tant en X qu'en Y tel que :

$$G_N(X) := G(X, \Phi(N)(X)) \in A[\Phi][X] \setminus \{0\};$$

s'annule en x avec multiplicité t et les coefficients $p_{ij} \in A$ de $G(X, Y)$ sont tels que :

$$\deg_T(p_{ij}) \leq \frac{Dc(\Phi)}{L^2 - tDc(\Phi)}\Sigma;$$

pour chaque $0 \leq i, j \leq L - 1$, où Σ est la somme des hauteurs des vecteurs constitués par les lignes de la matrice des coefficients du système linéaire

$$d^{(h)}G_N(x) = 0,$$

pour $h = 0, ..., t - 1$, dont les inconnues sont justement les coefficients (à déterminer) de $G(X, Y)$, ceux de N étant fixés.

Démonstration. Construisons le polynôme G de façon directe. Il est nécessairement de la forme :

$$G(X, Y) = \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} p_{ij}X^iY^j.$$

Si on impose sur un élément $N \in A \setminus \{0\}$ d'être tel que $G_N \neq 0$ dans $A[\Phi][X]$, cela équivaut à dire que la variété algébrique d'équation $Y = \Phi(N)(X)$ dans $\mathcal{C}^2$ n'est pas contenue dans celle associée au polynôme $G(X,Y)$. Autrement dit, dans le domaine factoriel $A[\Phi][X,Y]$ on a la condition suivante :

$$Y - \Phi(N)(X) \nmid G(X,Y).$$

En imposant $q^{d \deg_T(N)} > L-1$ cela est évidemment satisfait. On pose, alors :

$$\deg_T(N) := [\frac{1}{d}\log L] + 1. \tag{1.7}$$

On aura, donc :

$$L - 1 < q^{d \deg_T(N)} \leq q^d L. \tag{1.8}$$

Imposer maintenant l'annulation de G_N sur x à l'ordre t revient à dire que la dérivée divisée de G_N à l'ordre h, pour tout $0 \leq h \leq t-1$, s'annule en x. Ce qui donne un système linéaire à t conditions, dont les inconnues sont les L^2 coefficients de G. Si on impose donc $L^2 > Dc(\Phi)t$, où $Dc(\Phi) \geq [k(\Phi, x) : k]$, les conditions du Lemme 1.2.13 sont satisfaites. En posant Σ comme expliqué dans l'énoncé on a le Théorème. □

La stratégie qu'on se propose de suivre pour arriver à une contradiction consiste à montrer que le polynôme $G_N(X)$, pas nul par hypothèse, a pourtant plus de zéros qu'il pourrait en avoir.

Nous examinons donc ce polynôme, qu'on appellera dorénavant *polynôme auxiliaire* :

$$G_N(X) = \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} p_{ij} X^i (\Phi(N)(X))^j.$$

Les propriétés des dérivées divisées permettent de dire non seulement que x est un zéro d'ordre t de $G_N(X)$, mais que, pour $h = 0, ..., t-1$, la dérivée divisée $G_N^{(h)}(X)$ de $G_N(X)$ à l'ordre h admet également x comme zéro d'ordre $t-h$. En laissant $h \leq t-1$ générique, on a alors la décomposition suivante :

$$G_N^{(h)}(X) = \Delta(X)^{t-h} R_h(X)$$

où $\Delta(X) \in k(\Phi)[X]$ est le polynôme minimal de x sur $k(\Phi)$ et $G_N(X) = \Delta(X)^t R_h(X)$ pour un certain $R_h(X) \in k(\Phi)[X]$.

Proposition 1.3.6. *Il existe $h \in \mathbb{N} \setminus \{0\}$ assez grand, qu'on déterminera plus tard, respectant les conditions du Théorème 1.3.5 tel que, quelque soit $l \in A \setminus \{0\}$ qui respecte la propriété RV, on ait que :*

$$G_N^{(h')}(\Phi(l)(x)) = 0;$$

pour tout $0 \leq h' \leq h-1$.

On va montrer cette Proposition par l'absurde en supposant l'hypothèse suivante et en tirant une contradiction :

Hypothèse 2. *Supposons que pour un opportun $l \in A$ comme dans la Proposition 1.3.6, on ait que :*

$$G_N^{(h')}(\Phi(l)(x)) \neq 0;$$

pour au moins un h' tel que $0 \leq h' \leq h-1$, où h est celui de la Proposition 1.3.6.

Majoration de la hauteur du polynôme auxiliaire

On commence par majorer la hauteur de $G_N^{(h')}(\Phi(l)(x))$. Pour cela, il faut d'abord comprendre l'expression précise de la dérivée divisée à l'ordre h générique du polynôme $G_N(X) \in A[\Phi][X] \setminus \{0\}$, dans le but de pouvoir bénéficier de l'estimation de ses coefficients, dont on dispose suite au Lemme de Siegel.

On avait vu que $\Sigma = \sum_{j=1}^{M} h(a_{j1}, ..., a_{jN})$ où les $a_{j,i} \in \overline{k}$ sont les coefficients du système de Siegel qui, dans notre cas, a la forme :

$$d^{(h)}G_N(x) = 0$$

pour toute dérivée divisée $d^{(h)}$ à l'ordre $h = 0, ..., t-1$ de $G_N(X) = G(X, \Phi(N)(X))$ dans x. On rappelle que :

$$G(X,Y) = \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} p_{ij}X^iY^j.$$

Par définition, la dérivée divisée de $G_N(X)$ en x à l'ordre h est le coefficient de H^h, où H est un paramètre, dans l'expression en série de puissances de H de la translatée formelle :

$$G_N(X+H) =$$

$$= \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} p_{ij}(\sum_{a=0}^{i}\binom{i}{a}X^{i-a}H^a)(\sum_{b=0}^{j}\binom{j}{b}(\Phi(N)(X))^{j-b}(\Phi(N)(H))^b);$$

où :

$$\Phi(N)(H) = \sum_{s=0}^{d\deg_T(N)} \widetilde{a}_s(T)H^{q^s},$$

où les $\widetilde{a}_s(T)$ sont des éléments dans $k(\Phi)$, venant d'une écriture explicite du polynôme additif $\Phi(N(T)) = N(\Phi(T)) \in \overline{k}\{\tau\}$, de degré $d\deg_T(N)$ en τ. L'expression finale de cette dérivée divisée à l'ordre h est alors fonction de la valeur de h et est une somme d'autant de termes que le nombre de toutes les possibilités de former la puissance H^h dans l'expression précédente de la translatée formelle $G_N(X+H)$, en rappelant l'expression de $\Phi(N)(H)$ que nous venons d'écrire. Chacun de ces termes est de la forme suivante :

$$\sum_{i=a}^{L-1}\sum_{j=b}^{L-1} p_{ij}\binom{i}{a}\binom{j}{b}\binom{b}{n_0, ..., n_{d\deg_T(N)}}X^{i-a}(\Phi(N)(X))^{j-b}\prod_{i=0}^{d\deg_T(N)}\widetilde{a}_i(T)^{n_i} =$$

$$= \sum_{i=a}^{L-1}\sum_{j=b}^{L-1} p_{ij}\binom{i}{a}\binom{j}{j-b, n_0, ..., n_{d\deg_T(N)}}X^{i-a}(\Phi(N)(X))^{j-b}\prod_{i=0}^{d\deg_T(N)}\widetilde{a}_i(T)^{n_i},$$

pour tout couple (a,b) et toute $(d\deg_T(N)+1)-$uplet $\overline{n} = (n_0, ..., n_{d\deg_T(N)}) \in \mathbb{N}^{d\deg_T(N)+1}$ telle que :

$$b = \sum_{i=0}^{d\deg_T(N)} n_i$$

et

$$h = a + \sum_{i=0}^{d \deg_T(N)} n_i q^i.$$

On a, donc, que $0 \leq a \leq h$ et $0 \leq \sum_{i=0}^{d \deg_T(N)} n_i q^i \leq h - a$.

Pour tout couple $(i,j) \in \{0, ..., L-1\}^2$, le coefficient associé à l'inconnue p_{ij} dans le système de Siegel

$$d^{(h)} G_N(x) = 0$$

est alors :

$$\sum_{(a,b,\overline{n}) \in \mathcal{I}(i,j,h)} \binom{i}{a} \binom{j}{j-b, n_0, ..., n_{d \deg_T(N)}} x^{i-a} (\Phi(N)(x))^{j-b} \prod_{i=0}^{d \deg_T(N)} \widetilde{a}_i^{n_i},$$

avec l'ensemble :

$$\mathcal{I}(i,j,h) := \{(a, b, n_0, ..., n_{d \deg_T(N)}) \in \mathbb{N}^{d \deg_T(N)+3}, 0 \leq a \leq \min\{i, h\},$$

$$, a + \sum_{i=0}^{d \deg_T(N)} n_i q^i = h, \sum_{i=0}^{d \deg_T(N)} n_i = b\}.$$

La hauteur L_h de la ligne $h-$ième

$$d^{(h)} G_N(x) = 0$$

du système de Siegel sera alors :

$$h(L_h) := h(\{\sum_{(a,b,\overline{n}) \in \mathcal{I}(i,j,h)} x^{i-a} (\Phi(N)(x))^{j-b} \prod_{i=0}^{d \deg_T(N)} \widetilde{a}_i^{n_i}\}_{(i,j)}) =$$

$$= \frac{1}{[k(\Phi, x) : k]} \sum_{v \texttt{ sur } k(\Phi,x)/k} n_v \max_{(i,j)} \{0, -v(\sum_{(a,b,\overline{n}) \in \mathcal{I}(i,j,h)} x^{i-a} (\Phi(N)(x))^{j-b} \prod_{i=0}^{d \deg_T(N)} \widetilde{a}_i^{n_i})\}.$$

La propriété (1.3) nous amène à majorer la hauteur $h(L_h)$ de cette façon :

$$h(L_h) \leq \frac{1}{[k(\Phi, x) : k]} \sum_{v \texttt{ sur } k(\Phi,x)/k} n_v \max_{(i,j,a,b,\overline{n})} \{0, -v(x^{i-a} (\Phi(N)(x))^{j-b} \prod_{i=0}^{d \deg_T(N)} \widetilde{a}_i^{n_i})\} =$$

$$= h(\{x^{i-a} (\Phi(N)(x))^{j-b} \prod_{i=0}^{d \deg_T(N)} \widetilde{a}_i^{n_i}\}_{(i,j,a,b,\overline{n})}).$$

Pour tout choix $i, j = 0, ..., L-1$, $a = 0, ..., \min\{i, h\}$, b tel que $h = a + \sum_{i=0}^{d \deg_T(N)} n_i q^i$, à l'élément $x^{i-a} (\Phi(N)(x))^{j-b}$ de l'équation h est de façon univoque associé un élément $\prod_{i=0}^{d \deg_T(N)} \widetilde{a}_i^{n_i}$ tel que $h = a + \sum_{i=0}^{d \deg_T(N)} n_i q^i$, créant alors un nouveau vecteur d'égale longueur à celle de $\{x^{i-a} (\Phi(N)(x))^{j-b}\}$ (avec i, j, a, b dans les bornes indiquées avant), son produit avec ce dernier, composante par composante, donnant celui dont on vient d'indiquer la hauteur. La propriété du produit (1.2) nous permet donc encore de majorer $h(L_h)$ de la manière suivante :

$$h(L_h) \leq h(\{x^{i-a}(\Phi(N)(x))^{j-b}\}) + h(\{\prod_{i=0}^{d\deg_T(N)} \widetilde{a}_i^{n_i}\}).$$

Suite aux propriétés des hauteurs, le premier terme est majoré par la valeur :

$$L[h(x) + h(\Phi(N)(x))].$$

Cherchons une majoration du deuxième. Si $N(T) = \alpha_0+\alpha_1 T+...+\alpha_{\deg_T(N)}T^{\deg_T(N)} \in A$, avec :

$$\Phi(N(T)) = N(\Phi(T)) = \alpha_0 + \alpha_1\Phi(T) + ... + \alpha_{\deg_T(N)}\Phi(T)^{\deg_T(N)};$$

examinons la hauteur de chacun de ces termes dans la somme. Pour $0 \leq \delta \leq \deg_T(N)$:

$$(\Phi(T)(\tau))^{\delta} = \sum_{i=0}^{d\delta}(\sum_{\overline{j}\in\Delta_\delta(i)}\prod_{s=1}^{\delta} a_{j(s)}^{q^{\sum_{\nu=0}^{s-1}j(\nu)}})\tau^i;$$

où :

$$\Delta_\delta(i) := \{(j(1),...,j(\delta)) \in \mathbb{N}^\delta; \sum_{s=1}^{\delta} j(s) = i\};$$

avec $j(s) \in \{0,...,d\}$, $j(0) := 0$. En effet, si on considère la puissance :

$$\Phi(T)(\tau)^\delta = (T + a_1\tau + ... + a_d\tau^d)(T + a_1\tau + ... + a_d\tau^d)...(T + a_1\tau + ... + a_d\tau^d);$$

en développant les produits selon les règles arithmétiques de l'algèbre de Ore $\overline{k}\{\tau\}$ on obtient le coefficient de τ^i, quelque soit $i = 0,...,d\delta$, en multipliant entre eux les coefficients $a_{j(s)}$ de chaque $s-$ième terme du produit de toutes les façons possibles afin que $\sum_{s=1}^{\delta} j(s) = i$, soumis à l'action des puissances $j(0),...,j(s-1)$ de τ, où on impose $j(0) := 0$. Comme, en effet, $a_{j(s)}$ n'est, dans son propre $s-$ième terme, soumis qu'à l'action de l'identité τ^0, cette action le fait apparaître dans le produit avec exposant 1, qu'on représente par le cas $s = 0$ pour rendre la formule compatible avec toute situation possible. En effet, $a_{j(1)}$ n'est soumis qu'à l'action de τ^0 dans le produit, ce qui donne ce dernier sous la forme $a_{j(1)}^{q^{j(0)}} = a_{j(1)}$. Si on appelle $\widetilde{a}_i$ le coefficient de τ^i dans l'expression de $\Phi(N)$, de façon que :

$$\Phi(N)(\tau) = \sum_{i=0}^{d\delta}\widetilde{a}_i\tau^i;$$

on en a que :

$$-w(\widetilde{a}_i) \leq \max\{\sum_{s=1}^{\delta} -q^{\sum_{\nu=0}^{s-1}j(\nu)}w(a_{j(s)})\} \leq \delta q^i \max_{j=0,...,d}\{-w(a_j)\}.$$

Alors :

$$h(\{\prod_{i=0}^{d\deg_T(N)}\widetilde{a}_i^{n_i}\}_{(i,j,a,b,\overline{n})}) = \frac{1}{c(\Phi)}\sum_{w \texttt{ sur } k(\Phi)/k} n_w \max\{0,-\sum_{i=0}^{d\deg_T(N)} n_i w(\widetilde{a}_i)\} \leq$$

$$\leq \frac{1}{c(\Phi)} \sum_{w \texttt{ sur } k(\Phi)/k} n_w \sum_{i=0}^{d\deg_T(N)} \max\{0, -n_i w(\widetilde{a}_i)\} \leq$$

$$\leq \frac{1}{c(\Phi)} \sum_{w \texttt{ sur } k(\Phi)/k} n_w \sum_{i=0}^{d\deg_T(N)} n_i \deg_T(N) q^i \max_{j=0,\dots,d}\{0, -w(a_j)\} \leq \deg_T(N) h(\Phi) h.$$

En conclusion, pour chaque $h = 0, ..., t-1$:

$$h(L_h) \leq L[h(x) + h(\Phi(N)(x))] + \deg_T(N) h(\Phi) h. \tag{1.9}$$

Or :

$$G_N^{(h')}(\Phi(l)(x)) = \sum_{i=0}^{L-1} \sum_{j=0}^{L-1} p_{ij} \sum_{(a,b,\overline{n}) \in \mathcal{I}(i,j,h')} (\Phi(l)(x))^{i-a} (\Phi(Nl)(x))^{j-b} \prod_{i=0}^{d\deg_T(N)} \widetilde{a}_i^{n_i};$$

pour tout $0 \leq h' \leq h-1$ (où on considère $h \geq 1$ parmi ceux inférieurs à t qu'on vient d'examiner), comme conséquence des calculs précédents. Donc :

$$h(G_N^{(h')}(\Phi(l)(x))) = h(\sum_{i=0}^{L-1} \sum_{j=0}^{L-1} p_{ij} \sum_{(a,b,\overline{n}) \in \mathcal{I}(i,j,h')} (\Phi(l)(x))^{i-a} (\Phi(Nl)(x))^{j-b} \prod_{i=0}^{d\deg_T(N)} \widetilde{a}_i^{n_i}).$$

On obtient donc la majoration :

$$h(G_N^{(h')}(\Phi(l)(x))) \leq h(p_{ij}) + L[h(\Phi(l)(x)) + h(\Phi(Nl)(x))] + \deg_T(N) h(\Phi) h'.$$

On est maintenant face à deux situations possibles :

1. $w(x) \geq 0$ pour chaque w extension de la place v_l, où v_l est la place $l-$adique sur A, à $k(\Phi, x)$ (on indique le fait que w étende v_l à $k(\Phi, x)$ avec la notation $w|v_l$) ;
2. Il existe au moins une place $w|v_l$ sur $k(\Phi, x)$ telle que $w(x) < 0$.

Minoration de la hauteur de $G_N^{(h')}(x)$

Dans le cas où $w(x) \geq 0$ pour chaque $w|v_l$ sur A, on pose $\zeta := N_{k(\Phi,x)/k}(G_N^{(h')}(\Phi(l)(x)))$, en supposant d'après l'hypothèse 2 que pour un opportun nombre naturel $h' < h$ on ait que $G_N^{(h')}(\Phi(l)(x)) \neq 0$, et on a, en indiquant $\mathcal{I}(k(\Phi, x)/k)$ l'ensemble des $k-$isomorphismes de l'extension $k(\Phi, x)/k$:

$$h(\zeta) = h(\prod_{\sigma \in \mathcal{I}(k(\Phi,x)/k)} \sigma(G_N^{(h')}(\Phi(l)(x)))) \leq [k(\Phi, x) : k] h(G_N^{(h')}(\Phi(l)(x)))$$

comme la hauteur de Weil est stable sous la conjugaison et respecte la propriété (1.2). En supposant $w(x) \geq 0$ pour chaque $w|v_l$, le polynôme minimal unitaire $\Delta(X)$ de x est à coefficients dans $\mathcal{O}_l$, anneau de v_l-valuation dans $k(\Phi)$. On sait que :

$$G_N^{(h')}(\Phi(l)(x)) = \Delta(\Phi(l)(x))^{t-h'} R_{h'}(\Phi(l)(x))$$

où $\Delta(X)$ et $R_{h'}(X)$ sont dans $\mathcal{O}_l[X]\backslash\{0\}$ [5] (notons que puisque $\Delta(X), \Phi(l)(X) \in \mathcal{O}_l[X]$ alors $R_{h'}(X) \in \mathcal{O}_l[X]$ aussi). Alors, en utilisant l'hypothèse RV(r) sur l,

$$\Delta(\Phi(l)(x)) \equiv \Delta(x^{q^{d\deg_T(l)}}) \ \mathtt{mod}\ (w).$$

Nous remarquons maintenant que $\Delta(X) \in \mathcal{O}_l[X]$ et que le degré d'inertie $f_{l,\Phi}$ de l'extension $v_{l,\Phi}$ de la place v_l à $\mathcal{O}_l$ est tel que :

$$f_{l,\Phi} = [\mathcal{O}_{v_{l,\Phi}}/v_{l,\Phi} : A_l/l];$$

où $\mathcal{O}_{v_{l,\Phi}}$ et A_l sont, respectivement, les completés de $\mathcal{O}_l$ par rapport à $v_{l,\Phi}$ et de A par rapport à v_l. Par conséquent, on a que :

$$|\mathcal{O}_{v_{l,\Phi}}/v_{l,\Phi}| = q^{f_{l,\Phi}\deg_T(l)}.$$

Comme dans la condition RV, respectée par l, on demande que $f_{l,\Phi} = 1$, il s'ensuit que les coefficients de $\Delta(X)$ sont congrus à leurs puissances d'exposant $q^{d\deg_T(l)}$ mod $(v_{l,\Phi})$ et donc mod (w). Par conséquent, on a que :

$$\Delta(x^{q^{d\deg_T(l)}}) \equiv \Delta(x)^{q^{d\deg_T(l)}} \equiv 0 \ \mathtt{mod}\ (w).$$

On peut donc conclure que :

$$w(G_N^{(h')}(\Phi(l)(x))) \geq t - h';$$

pour toute $w|v_l$. Nous appliquons l'hypothèse 2 : en supposant $G^{(h')}(\Phi(l)(x)) \neq 0$, il s'ensuit que $\zeta \neq 0$ et, par conséquent, que ζ^{-1} existe. Comme $v_l(\zeta) = \sum_{w|v_l} w(G_N^{(h')}(\Phi(l)(x)))$:

$$h(\zeta) = h(\zeta^{-1}) \geq \max\{0, -\deg_T(l)v_l(\zeta^{-1})\} = \max\{0, \deg_T(l)v_l(\zeta)\} \geq$$
$$\geq [k(\Phi, x) : k]\deg_T(l)(t - h').$$

Dans le deuxième cas, où il existe au moins une extension $w|v_l$ telle que $w(x) < 0$, choisissons en une de valuation minimale en x (il y en n'a qu'un nombre fini à ne pas être 0 sur x en tout cas). Remarquons qu'il est alors possible d'obtenir directement un très bon résultat de minoration de la hauteur canonique de x. Plus précisément :

$$\widehat{h}(x) = \lim_{n\to\infty} q^{-d\deg_T(l)n} h(\Phi(l^n)(x)),$$

d'où on se ramène à étudier la valeur

$$h(\Phi(l)(x)) \geq \frac{1}{[k(\Phi, x) : k]} \sum_{w|v_l} n_w \max\{0, -w(\Phi(l)(x))\}.$$

Nous exprimons :

$$\Phi(l)(x) = lx + \alpha_1 x^q + ... + \alpha_{d\deg_T(l)} x^{q^{d\deg_T(l)}}.$$

5. C'est parce-que x est séparable sur $k(\Phi)$ que sa multiplicité dans son polynôme minimal est $t - h'$. Dans le cas pas séparable, il faut utiliser un exposant plus petit : $\frac{t-h'}{D_{p.i.}}$, avec $D_{p.i.}$ degré d'inséparabilité de x sur $k(\Phi)$

L'hypothèse RV sur l implique alors que $w(\alpha_i) > 0$ pour chaque $i = 0, ..., d\deg_T(l)-1$, alors que $w(\alpha_{d\deg_T(l)}) = 0$. Par conséquent, comme $w(x) < 0$, on a que :

$$w(\alpha_{d\deg_T(l)} x^{q^{d\deg_T(l)}}) = q^{d\deg_T(l)} w(x) < q^i w(x) < w(\alpha_i) + w(x^{q^i}) = w(\alpha_i x^{q^i});$$

pour tout $i = 0, ..., d\deg_T(l)-1$. Les propriétés des valuations non archimédiennes impliquent alors que :

$$w(\Phi(l)(x)) = q^{d\deg_T(l)} w(x).$$

Par récurrence, en changeant x et $\Phi(l^{n-1})(x)$, on a que :

$$h(\Phi(l^n)(x)) \geq q^{d\deg_T(l)n} \frac{1}{[k(\Phi, x) : k]} \sum_{w|v_l} n_w \max\{0, -w(x)\};$$

la dernière somme étant minorée par 1, ce deuxième cas sur x implique, comme prévu, une solution au problème initial sous la forme suivante :

$$\widehat{h}(x) \geq \frac{1}{Dc(\Phi)};$$

puisque :

$$D \leq [k(\Phi, x) : k] \leq Dc(\Phi);$$

(on rappelle que $D = [k(x) : k]$ et que $D \geq q^{q+d+1}$).

Ces passages peuvent être également répétés dans une situations d'inséparabilité de x sur k, nous permettant de même y garder l'hypothèse de $l-$intégralité sur x là où ce serait nécessaire.

On en conclut finalement qu'on peut poursuivre en supposant le premier cas sans aucune perte de géneralité. On obtient donc que :

$$\deg_T(l)(t-h') \leq h(p_{ij}) + L[h(\Phi(l)(x)) + h(\Phi(Nl)(x))] + \deg_T(N)h(\Phi)h'. \quad (1.10)$$

Contradiction finale

Rappelons que l satisfaisant l'hypothèse RV(r) est supposé tel que :

$$G_N^{(h')}(\Phi(l)(x)) \neq 0.$$

Grâce à la majoration de la hauteur qu'on a obtenu par le Lemme de Siegel, on est maintenant en condition de pouvoir majorer le terme $h(p_{ij})$, apparaissant dans l'inégalité (1.10). Le Lemme de Siegel donne l'estimation :

$$h(p_{ij}) \leq \frac{Dc(\Phi)}{L^2 - tDc(\Phi)} \sum_{h=0}^{t-1} h(L_h).$$

Nous imposons pour l'instant la condition :

$$L^2 > tDc(\Phi). \quad (1.11)$$

L'inégalité (1.9) nous donne alors :

$$h(p_{ij}) \leq \frac{Dc(\Phi)}{L^2 - tDc(\Phi)} \sum_{0 \leq h \leq t-1} (L[h(x)+h(\Phi(N)(x))]+\deg_T(N)h(\Phi)h). \quad (1.12)$$

Nous faisons les choix suivants [6] :

$$L := \left[c_0^2 \frac{D \log D}{(\log\log D)^2}\right] + 1; \quad (1.13)$$

$$t := \left[c_0^3 \frac{D \log D}{(\log\log D)^3}\right]; \quad (1.14)$$

$$h := \left[c_0 \frac{D}{(\log\log D)^2}\right]; \quad (1.15)$$

avec $c_0 > 0$ une constante opportune, dépendant du choix de Φ. Le choix :

$$c_0 \geq c(\Phi); \quad (1.16)$$

implique alors la suivante condition :

$$L^2 - tDc(\Phi) \geq \frac{1}{2}L^2;$$

pour chaque $D \geq q^{q+d+1}$. En effet, une telle inégalité peut s'exprimer de façon équivalente sous la forme $\frac{1}{2}L^2 - tDc(\Phi) \geq 0$. Comme :

$$L^2 \geq c_0^4 \frac{D^2(\log D)^2}{(\log\log D)^4};$$

et :

$$tDc(\Phi) \leq c_0^4 \frac{D^2 \log D}{(\log\log D)^3};$$

on en a que :

$$\frac{1}{2}L^2 - tDc(\Phi) \geq c_0^4 D^2 \log D \left(\frac{\frac{1}{2}\log D - \log\log D}{(\log\log D)^4}\right).$$

Cette dernière expression n'est pas négative, si $D \geq q^{q+d+1}$, si et seulement si :

$$\frac{1}{2}\log D \geq \log\log D;$$

condition qui est vraie comme le montre un étude opportun de fonctions pour $D \geq q^{q+d+1}$. Suite aux inégalités (1.11) et (1.12) on a alors que :

$$h(p_{ij}) \leq \frac{Dc(\Phi)}{L^2 - tDc(\Phi)} \sum_{0 \leq h \leq t-1} (L[h(x) + h(\Phi(N)(x))] + \deg_T(N)h(\Phi)h) \leq$$

$$\leq 2\frac{Dc(\Phi)}{L^2} \sum_{0 \leq h \leq t-1} (L[\widehat{h}(x) + 2\gamma + \widehat{h}(\Phi(N)(x))] + \deg_T(N)h(\Phi)h) \leq$$

6. Ces choix des paramètres sont du même ordre de grandeur que dans le travail de H. Bauchère [B] et nous nous en sommes inspirés.

$$\leq 2\frac{Dtc(\Phi)}{L^2}(2Lq^{d\deg_T(N)}\widehat{h}(x)+4(d+1)Lh(\Phi)+\deg_T(N)h(\Phi)t/2).$$

Les conditions (1.7) et (1.8) nous donnent alors[7] l'inégalité :

$$h(p_{i,j})\leq 2\frac{Dtc(\Phi)}{L^2}(2q^dL^2\widehat{h}(x)+4(d+1)Lh(\Phi)+\frac{1}{d}\log Lh(\Phi)t)=$$

$$=4q^dc(\Phi)Dt\widehat{h}(x)+\frac{8(d+1)h(\Phi)c(\Phi)}{L}Dt+\frac{2h(\Phi)c(\Phi)}{d}\frac{Dt^2\log L}{L^2}. \qquad (1.17)$$

La condition (1.10) implique alors que :

$$\deg_T(l)(t-h)<\deg_T(l)(t-h')\leq 4q^dc(\Phi)Dt\widehat{h}(x)+\frac{8(d+1)h(\Phi)c(\Phi)}{L}Dt+\frac{2h(\Phi)c(\Phi)}{d}\frac{Dt^2\log L}{L^2}+$$

$$+L[2q^{d(\deg_T(N)+\deg_T(l))}\widehat{h}(x)+4(d+1)h(\Phi)]+\deg_T(N)h(\Phi)h'\leq$$

$$\leq 4q^dc(\Phi)Dt\widehat{h}(x)+\frac{8(d+1)h(\Phi)c(\Phi)}{L}Dt+\frac{2h(\Phi)c(\Phi)}{d}\frac{Dt^2\log L}{L^2}+$$

$$+2q^{d\deg_T(l)}q^dL^2\widehat{h}(x)+4(d+1)h(\Phi)L+\frac{2}{d}\log Lh(\Phi)h'<$$

$$<4q^dc(\Phi)Dt\widehat{h}(x)+\frac{8(d+1)h(\Phi)c(\Phi)}{L}Dt+\frac{2h(\Phi)c(\Phi)}{d}\frac{Dt^2\log L}{L^2}+$$

$$+2q^{d\deg_T(l)}q^dL^2\widehat{h}(x)+4(d+1)h(\Phi)L+\frac{2}{d}\log Lh(\Phi)h.$$

Les choix (1.14), (1.15) et (1.16) impliquent que $h\leq t/2$. Donc :

$$\deg_T(l)t\leq 8q^dc(\Phi)Dt\widehat{h}(x)+\frac{16(d+1)h(\Phi)c(\Phi)}{L}Dt+\frac{4h(\Phi)c(\Phi)}{d}\frac{Dt^2\log L}{L^2}+$$

$$+4q^{d\deg_T(l)}q^dL^2\widehat{h}(x)+8(d+1)h(\Phi)L+\frac{4}{d}\log Lh(\Phi)h.$$

Sachant que $tDc(\Phi)<L^2$, nous obtenons que :

$$\deg_T(l)t<c_4(L^2q^{d\deg_T(l)}\widehat{h}(x)+h(\Phi)L+\frac{h(\Phi)c(\Phi)}{d}\frac{Dt^2}{L^2}\log L+\frac{h(\Phi)}{d}h\log L); \qquad (1.18)$$

avec :

$$c_4:=24q^d.$$

Nous choisissons alors :

$$\deg_T(l):=h(\Phi)c(\Phi)\left[\frac{1}{r}\log\left(c_0^4\frac{(\log D)^2}{\log\log D}\right)\right]. \qquad (1.19)$$

Tout d'abord nous remarquons qu'étant donnés $a,b\in\mathbb{R}^+$ tels que $a,b\geq 4$, on a que $[a][b]\geq\frac{1}{2}ab$. Nous avons donc, en imposant :

$$\alpha:=h(\Phi)c(\Phi); \qquad (1.20)$$

et :

$$c_0\geq q^d; \qquad (1.21)$$

7. Comme $\log L\geq d$ (conséquence du fait que $D\geq q^{q+d+1}$) on a que $\deg_T(N)\leq\frac{2}{d}\log L$.

(condition qui, avec l'hypothèse que $D \geq q^{q+d+1}$, implique que $t, \deg_T(l) >= 4$) que :

$$\deg_T(l)t \geq \frac{1}{2}\frac{\alpha}{r}(4\log c_0 + 2\log\log D - \log\log\log D)c_0^3 \frac{D\log D}{(\log\log D)^3} \geq$$

$$\geq \frac{1}{2}\frac{\alpha}{r}(4\log c_0 + \log\log D)c_0^3 \frac{D\log D}{(\log\log D)^3} \geq$$

$$\geq \frac{1}{2}\frac{\alpha}{r}c_0^3 \frac{D\log D}{(\log\log D)^2}. \tag{1.22}$$

Avec un tel choix nous calculons maintenant la meilleure minoration possible de c_0 afin que les trois suivantes conditions soient respectées :

$$\deg_T(l)t \geq 4c_4 h(\Phi)L; \tag{1.23}$$

$$\deg_T(l)t \geq 4c_4 \frac{h(\Phi)c(\Phi)}{d}\frac{Dt^2}{L^2}\log L; \tag{1.24}$$

$$\deg_T(l)t \geq 4c_4 \frac{h(\Phi)}{d} h \log L. \tag{1.25}$$

En appliquant, suite aux conditions (1.13) et (1.16), et à l'hypothèse pour laquelle $D \geq q^{q+d+1}$ (ce qui implique que $c_0^2 \frac{D\log D}{(\log\log D)^2} \geq 1$)le fait que :

$$c_0^2 \frac{D\log D}{(\log\log D)^2} \leq L \leq 2c_0^2 \frac{D\log D}{(\log\log D)^2}; \tag{1.26}$$

l'inégalité (1.23) est alors conséquence de celle-ci :

$$\frac{1}{2}\frac{\alpha}{r}c_0^3 \frac{D\log D}{(\log\log D)^2} \geq 8c_4\alpha c_0^2 \frac{D\log D}{(\log\log D)^2};$$

ce qui nous amène à la condition :

$$c_0 \geq 16rc_4 = 384rq^d. \tag{1.27}$$

L'inégalité (1.24) est par contre conséquence de celle-ci :

$$\frac{1}{2}\frac{\alpha}{r}c_0^3 \frac{D\log D}{(\log\log D)^2} \geq 4c_4 \frac{\alpha}{d} c_0^6 \frac{D^3(\log D)^2}{(\log\log D)^6} \frac{(\log\log D)^4}{c_0^4 D^2 (\log D)^2} \log L;$$

(conséquence du fait que $L \geq c_0^2 \frac{D\log D}{(\log\log D)^2}$, voir la condition (1.26)) qui vient de la suivante :

$$c_0 \log D \geq \frac{8rc_4}{d}(2\log c_0 + \log D + \log\log D - 2\log\log\log D + \log 2);$$

(conséquence du fait que $L \leq 2c_0^2 \frac{D\log D}{(\log\log D)^2}$, voir la condition (1.26)) impliquée par celle qui suit :

$$c_0 \log D \geq \frac{8rc_4}{d}(2\log c_0 + 3\log D). \tag{1.28}$$

Pour montrer une telle inégalité il nous suffira donc d'avoir à la fois que :

$$c_0 \geq \frac{48rc_4}{d} = \frac{1152rq^d}{d}; \tag{1.29}$$

et que :

$$c_0 \log D \geq \frac{32rc_4}{d} \log c_0.$$

Nous cherchons alors c_0 tel que :

$$\frac{c_0}{\log c_0} \geq \frac{32rc_4}{d} = \frac{768rq^d}{d}.$$

Suite à la condition (1.21) et au fait que la fonction $\frac{\log X}{X}$ est croissante pour $X \geq q$, une telle inégalité est conséquence de celle-ci :

$$\frac{q^d}{d} \geq \frac{768rq^d}{d}. \tag{1.30}$$

Si on admet que :

$$r \leq \frac{1}{768}; \tag{1.31}$$

cette dernière condition est respectée. Si on admet en revanche que :

$$r > \frac{1}{768}; \tag{1.32}$$

nous cherchons X sous la forme :

$$X := X_0 768rq^d; \tag{1.33}$$

telle que :

$$\frac{X}{\log X} \geq \frac{768rq^d}{d};$$

donc telle que :

$$\frac{X_0}{\log 768 + \log r + \log X_0 + d} \geq \frac{1}{d}.$$

L'hypothèse sur r nous garantit que le premier terme de cette inégalité est bien un nombre positif, ce qui rend suffisant de vérifier que :

$$\frac{X_0}{\log X_0 + d} \geq \frac{1}{d}.$$

Donc, que :

$$d(X_0 - 1) \geq \log X_0. \tag{1.34}$$

Condition vérifiée pour tout $X_0 \geq 2$. Donc pour tout choix de c_0 tel que :

$$c_0 \geq 2(768rq^d) = 1536rq^d. \tag{1.35}$$

Comme on suppose que $r \leq \frac{1}{768}$ on a que dans tous les cas une telle condition implique aussi la (1.21) et la (1.29). La condition (1.25) est finalement, d'après l'inégalité (1.22) et en répétant les mêmes majorations du terme $\log L$ qui nous avaient amènés à la condition (1.28), conséquence de celle-ci :

$$\frac{1}{2}\frac{\alpha}{r}c_0^3\frac{D\log D}{(\log\log D)^2} \geq 4c_4\frac{\alpha}{d}c_0\frac{D}{(\log\log D)^2}(2\log c_0 + 3\log D);$$

et, donc, de celle-ci :

$$c_0^2\log D \geq \frac{8rc_4}{d}(2\log c_0 + 3\log D). \tag{1.36}$$

Comme cette dernière est conséquence de (1.28), nous concluons que les conditions (1.23), (1.24) et (1.25) sont vérifiées pour tout choix de c_0 respectant la condition (1.35).

On aura donc une contradition avec (1.18) en imposant :

$$\widehat{h}(x) < \frac{\deg_T(l)t}{4c_4L^2q^{d\deg_T(l)}}. \tag{1.37}$$

On a donc que, pour $\widehat{h}(x)$ assez petit, $G_N(\Phi(l)(x)) = 0$ pour chaque l respectant la propriété RV de degré $\deg_T(l)$ choisi comme avant. Grâce au Lemme 1.3.1 nous pouvons par conséquent compter le nombre de zéros de $G_N(X)$ avec leur multiplicité. Comme on suppose le module de Drinfeld de type RV(r) on aura en effet au moins :

$$(\frac{q^{r\deg_T(l)}}{2r\deg_T(l)} - \frac{\log D}{\log 2})D';$$

zéros de $G_N(X)$, de multiplicité au moins h, où $\deg_T(l)$ est défini comme avant. Comme $D = [k(x) : k] \leq [k(\Phi, x) : k(\Phi)][k(\Phi) : k] = D'c(\Phi)$, il s'ensuit qu'on aura finalement au moins :

$$(\frac{q^{r\deg_T(l)}}{2r\deg_T(l)} - \frac{\log D}{\log 2})\frac{D}{c(\Phi)};$$

zéros de $G_N(X)$. Nous cherchons alors une condition sur c_0 telle que :

$$\frac{q^{r\deg_T(l)}}{2r\deg_T(l)} \geq 2\frac{\log D}{\log 2}. \tag{1.38}$$

Comme la condition (1.19) implique que :

$$\alpha\log\left(c_0^4\frac{(\log D)^2}{\log\log D}\right) \geq r\deg_T(l) \geq r\alpha\left(\frac{1}{r}\log\left(c_0^4\frac{(\log D)^2}{\log\log D}\right) - 1\right);$$

il s'ensuit que :

$$q^{r\deg_T(l)} \geq \frac{\left(c_0^4\frac{(\log D)^2}{\log\log D}\right)^\alpha}{q^{r\alpha}}.$$

Donc :

$$\frac{q^{r\deg_T(l)}}{2r\deg_T(l)} \geq \frac{\left(c_0^4\frac{(\log D)^2}{\log\log D}\right)^\alpha}{q^{r\alpha}2\alpha(4\log c_0 + 2\log\log D - \log\log\log D)}. \tag{1.39}$$

La condition (1.38) sera donc conséquence de celle-ci :

$$\frac{\left(c_0^4 \frac{(\log D)^2}{\log\log D}\right)^\alpha}{q^{r\alpha} 2\alpha(4\log c_0 + 2\log\log D)} \geq 2\frac{\log D}{\log 2}.$$

Il nous reste alors à montrer que :

$$c_0^{4\alpha}(\log D)^{2\alpha-1} \geq \frac{4q^{r\alpha}\alpha}{\log 2}(4\log c_0 + 2\log\log D)(\log\log D)^\alpha.$$

Les conditions à imposer sont alors :

$$c_0^{4\alpha}(\log D)^{2\alpha-1} \geq \frac{32q^{r\alpha}\alpha}{\log 2}\log c_0(\log\log D)^\alpha;$$

et :

$$c_0^{4\alpha}(\log D)^{2\alpha-1} \geq \frac{16q^{r\alpha}\alpha}{\log 2}(\log\log D)^{\alpha+1}.$$

Pour la première condition, nous remarquons que pour $\alpha \geq 1$ et $D \geq q^{q+d+1}$ on a que :

$$(\log D)^{2\alpha-1} \geq (\log\log D)^\alpha;$$

il suffit donc que :

$$\frac{c_0^{4\alpha}}{\log c_0} \geq \frac{32q^{r\alpha}\alpha}{\log 2}.$$

Nous supposons alors que :

$$c_0 \geq 2q. \tag{1.40}$$

Comme la fonction $\frac{X}{\log X}$ est croissante pour $X \geq q$, une telle condition est donc conséquence de celle-ci :

$$\frac{(2q)^{4\alpha}}{\log 2 + 1} \geq \frac{32q^{r\alpha}\alpha}{\log 2};$$

qui est encore conséquence des inégalités suivantes :

$$q^2\frac{2^{4\alpha}}{\log 2 + 1} \geq \frac{32}{\log 2}\alpha;$$

et :

$$q^{4\alpha-2} \geq q^{r\alpha};$$

qui sont des conditions toujours respectées par toutes les valeurs possibles de α, r et q parmi celles admises par les hypothèses.

Pour la deuxième condition, nous remarquons que l'inégalité que nous voulons montrer est conséquence des suivantes :

$$c_0(\log D)^{2\alpha-1} \geq (\log\log D)^{\alpha+1};$$

et :

$$c_0^{4\alpha-1} \geq \frac{16q^{r\alpha}\alpha}{\log 2}.$$

Les choix précedemment faits de c_0 et de D impliquent ces deux dernières inégalités. En effet, comme $c_0 \geq 2q$ la première inégalité est toujours respectée pour tout $D \geq q^{q+d+1}$ et tout $\alpha \geq 1$, puisque sous de telles conditions $2\log D \geq (\log\log D)^2$ et donc l'inégalité est impliquée par celle-ci :

$$q(\log D)^{2\alpha-2} \geq (\log\log D)^{\alpha-1};$$

qui est toujours respectée. La deuxième inégalité est conséquence de celle-ci :

$$2^{4\alpha-1}q^{4\alpha-1} \geq \frac{16q^{r\alpha}\alpha}{\log 2}.$$

Qui est encore conséquence des inégalités suivantes :

$$2^{4\alpha-1}q \geq 16;$$

et :

$$q^{4\alpha-2} \geq \frac{q^\alpha\alpha}{\log 2};$$

dont la première est immédiate et la deuxième conséquence du fait que :

$$q \geq \frac{1}{\log 2} = \log_2 q;$$

et que :

$$q^{4\alpha-3} \geq q^\alpha\alpha;$$

pour tout q puissance d'un nombre premier et $\alpha \geq 1$.

Sachant que $\deg_X(G_N(X)) \leq 2(L-1)q^{d\deg_T(N)} < 2q^dL^2$, un choix de paramètres tel que :

$$\frac{q^{r\deg_T(l)}}{4r\deg_T(l)}\frac{D}{c(\Phi)}h \geq 2q^dL^2;$$

nous donnerait la contradition cherchée, montrant comment l'Hypothèse 1 aussi est fausse. Une telle condition est conséquence, suite à la condition (1.39) et aux faits (toujours conséquences des hypothèses $D \geq q^{q+d+1}$ et $c_0 \geq 1$) que :

$$h \geq \frac{1}{2}c_0\frac{D}{(\log\log D)^2}; \tag{1.41}$$

et que :

$$L \leq 2c_0^2\frac{D\log D}{(\log\log D)^2}; \tag{1.42}$$

de celle-ci :

$$\frac{\left(c_0^4\frac{(\log D)^2}{\log\log D}\right)^\alpha}{q^{r\alpha}4c(\Phi)\alpha(4\log c_0 + 2\log\log D - \log\log\log D)}\frac{c_0D^2}{2(\log\log D)^2} \geq$$

$$\geq 2q^d4c_0^4\frac{D^2(\log D)^2}{(\log\log D)^4}.$$

Qui se réduit, comme $\alpha \geq 1$, à l'estimation suivante :

$$\frac{\left(c_0^4 \frac{(\log D)^2}{\log\log D}\right)^{\alpha}}{q^{r\alpha} 4\alpha^2 (4\log c_0 + 2\log\log D)} \geq 16 q^d c_0^3 \frac{(\log D)^2}{(\log\log D)^2}.$$

En posant :

$$X := \log D;$$

on a à étudier la condition :

$$\frac{c_0^{4\alpha-3} X^{2\alpha-2}}{128 q^{d+r\alpha}\alpha^2 (2\log c_0 (\log X)^{\alpha-2} + (\log X)^{\alpha-1})} \geq 1;$$

où $\alpha \geq 1$ et $\log X \geq 1$. Avec la majoration :

$$(\log X)^{\alpha-2} \leq (\log X)^{\alpha-1};$$

nous nous réconduisons alors à étudier l'inégalité :

$$\frac{c_0^{4\alpha-3} X^{2(\alpha-1)}}{128 q^{d+r\alpha}\alpha^2 (\log X)^{\alpha-1}(2\log c_0 + 1)} \geq 1.$$

Puisque $X^{2(\alpha-1)} \geq (\log X)^{\alpha-1}$ pour tout $X \geq 1$, il nous reste à montrer la suivante inégalité :

$$\frac{c_0^{4\alpha-3}}{128 q^{d+r\alpha}\alpha^2 (2\log c_0 + 1)} \geq 1;$$

qui est conséquence de la suivante :

$$\frac{c_0}{2\log c_0 + 1} \geq 128 q^{d+r\alpha}\alpha^2.$$

Nous choisissons donc c_0 sous la suivante forme :

$$c_0 \geq A d \alpha^3 q^{d+r\alpha}; \tag{1.43}$$

où A est un nombre réel positif suffisament grand qu'on déterminera tout de suite. La condition à imposer sur A est en effet la suivante :

$$\frac{A d\alpha^3 q^{d+r\alpha}}{2(\log A + \log d + 3\log\alpha + d + \alpha) + 1} \geq 128 q^{d+r\alpha}\alpha^2.$$

Ce qui peut aussi s'exprimer comme il suit :

$$\frac{2\log A + 2\log d + 6\log\alpha + 2d + 2\alpha + 1}{A d\alpha} \leq \frac{1}{128}.$$

Le choix :

$$A := 6500;$$

nous donne alors les trois suivantes conditions :

$$2\frac{2\log A}{A} \leq \frac{1}{128};$$

$$4\frac{2\log d + 2d}{Ad} \leq \frac{1}{128};$$

$$4\frac{6\log\alpha+2\alpha+1}{A\alpha}\le\frac{1}{128};$$

pour tout $\alpha, d\in\mathbb{N}\setminus\{0\}$. La première de ces inégalités se revèle être respectée en choisissant $A=6500$. Un tel choix implique d'ailleurs facilement les deux autres suite aux majorations suivantes :

$$2\log d+2d\le 4d;$$

et :

$$3\log\alpha\le\alpha+2;$$

valables quelque soit le choix de α et d dans $\mathbb{N}\setminus\{0\}$. La condition que nous imposons à c_0 est donc finalement la suivante :

$$c_0\ge 6500d\alpha^3q^{d+r\alpha}. \tag{1.44}$$

En rassemblant toutes les conditions qu'on a obtenu sur c_0 ((1.16), (1.21), (1.27), (1.35), (1.40), (1.44)) on peut donc finalement donner l'estimation générale que cette constante doit respecter afin de rendre fausses les hypothèses 1 et 2 :

$$\begin{aligned} c_0 &\ge \max\{c(\Phi), q^d, 384rq^d, 1536rq^d, 2q, 6500d\alpha^3q^{d+r\alpha}\} = \\ &= 6500d\alpha^3q^{d+r\alpha}. \end{aligned} \tag{1.45}$$

Nous imposons donc :

$$c_0\ge 6500d\alpha^3q^{d+r\alpha}. \tag{1.46}$$

En conclusion, si $\widehat{h}(x)$ est trop petite, on a la Proposition 1.3.6, qui implique que $G_N(X)$ admet un nombre de zéros, comptés avec leur multiplicité, supérieur à $\deg_X(G_N(X))$, ce qui est en contradiction avec le Lemme de Siegel, pour lequel un tel $G_N(X)$ existe et n'est pas le polynôme 0. En définitif, suite à l'impossibilité de la condition (1.37), et grâce aux conditions (1.19), (1.22) et (1.26), on obtient que :

$$\widehat{h}(x)\ge\frac{\deg_T(l)t}{4c_4L^2q^{d\deg_T(l)}}\ge\frac{\frac{1}{2}\frac{h(\Phi)c(\Phi)}{r}c_0^3\frac{D\log D}{(\log\log D)^2}}{16c_4c_0^4\frac{D^2(\log D)^2}{(\log\log D)^4}\left(c_0^4\frac{(\log D)^2}{\log\log D}\right)^{\frac{d}{r}h(\Phi)c(\Phi)}}\ge$$

$$\ge\frac{h(\Phi)c(\Phi)}{768rq^dc_0^{1+\frac{4d}{r}h(\Phi)c(\Phi)}}\frac{(\log\log D)^{2+\frac{d}{r}h(\Phi)c(\Phi)}}{D(\log D)^{1+\frac{2d}{r}h(\Phi)c(\Phi)}}.$$

Finalement, grâce au Corollaire 1.2.11, on peut étendre ce résultat de la situation où $D\ge q^{q+d+1}$ au cas de D quelconque avec la minoration énoncée dans le Théorème 1.1.7 :

$$\widehat{h}(x)\ge C_0\frac{(\log\log_+ D)^{2+\frac{d}{r}h(\Phi)c(\Phi)}}{D(\log_+ D)^{1+\frac{2d}{r}h(\Phi)c(\Phi)}}.$$

Nous remarquons qu'avec la notation $\log_+(.)$ et $\log\log_+(.)$ introduite au début, on a que :

$$\frac{(\log\log_+ D)^{2+\frac{d}{r}h(\Phi)c(\Phi)}}{D(\log_+ D)^{1+\frac{2d}{r}h(\Phi)c(\Phi)}}\le 1;$$

quelque soit $D\in\mathbb{N}\setminus\{0\}$, ce qui nous permet de formuler un résultat valable pour toute valeur de $D\in\mathbb{N}\setminus\{0\}$.

Nous remarquons maintenant que la même méthode marche également sous l'hypothèse plus faible $\mathrm{RV}(r)^*$. En effet, on a le Lemme suivant :

Lemme 1.3.7. *On suppose que l'Hypothèse 1 soit vraie pour tout $C \in]0, C_0]$. Alors on peut définir une application $D = D(C)$ de $]0, C_0]$ dans $[q^{q+d+1}, +\infty[$ en choisissant, pour tout $C > 0$, un élément x de degré $D(C) = D$ minimal sur k tel que :*

$$\widehat{h}(x) < C\frac{(\log\log D)^{\mu}}{D(\log D)^{\kappa}};$$

où κ et μ sont définis en (1.5) et (1.6). Cette fonction croît vers l'infini quand C décroît vers 0^+.

Démonstration. Nous allons montrer d'abord que la fonction $D = D(C)$ qu'on a défini n'est pas bornée (tout en restant minorée par la valeur q^{q+d+1}). Si, par l'absurde, une telle borne $D \leq M$ existait, où $D = [k(x) : k]$, avec $x \in \mathbb{D}(\overline{k})_{NT}$ choisi en fonction de C comme expliqué dans l'énoncé, suite au Théorème 1.2.10 on aurait que $\widehat{h}(x) \geq c_2^{-M^2}$. D'où $c_2^{-M^2} \leq \widetilde{C}$, suite à l'hypothèse 1, en choisissant $\widetilde{C} := \max_{D=1,\ldots,M}\{C\frac{(\log\log_+ D)^{\mu}}{D(\log_+ D)^{\kappa}}\}$. On choisit donc C assez petit afin que $\widetilde{C} < c_2^{-M^2}$. Ce qui implique $\widehat{h}(x) = 0$ ou, de façon équivalente, que x est un point de torsion, ce qui contredit les hypothèses. Il ne nous reste plus qu'à montrer que D croît toujours quand C décroît vers 0^+. Cette propriété est équivalente à dire que la fonction $D = D(C)$ est décroissante pour C croissant vers C_0. Etant donné C et C' tels que $0 < C < C'$, on montrera donc que $D = D(C) \geq D' = D(C')$. En effet, au choix de C on associe $x \in \mathbb{D}(\overline{k})_{NT}$ de degré D sur k minimal tel que $\widehat{h}(x) < C\frac{(\log\log_+ D)^{\mu}}{D(\log_+ D)^{\kappa}}$, et on choisit de la même manière $x' \in \mathbb{D}(\overline{k})_{NT}$ et D' associés à C'. Comme $C' > C$, on a alors que :

$$\widehat{h}(x) < C'\frac{(\log\log_+ D)^{\mu}}{D(\log_+ D)^{\kappa}}.$$

La minimalité du choix de $D' = D(C')$ implique alors que $D' \leq D$, ce qui achève la preuve. $\square$

On supposera, donc, la condition $\mathrm{RV}(r)^*$ pour le module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$. Il s'agit d'une condition plus faible que $\mathrm{RV}(r)$: dans les passages précédents, où on était sous la condition $\mathrm{RV}(r)$, nous avons montré comment les hypothèses 1 et 2 sont fausses avec le choix précis :

$$C = C_0 := \min\{q^{-5d(2(d+1)h(\Phi)+1)(q^{q+d+1}-1)^2c(\Phi)^2}, \frac{h(\Phi)c(\Phi)}{768rq^dc_0^{1+\frac{4d}{r}h(\Phi)c(\Phi)}}\};$$

en effet, ce choix impliquait, suite à la condition $\mathrm{RV}(r)$, l'existence d'au moins $q^{r\deg_T(l)}/2r\deg_T(l)$ éléments $l \in P_{\deg_T(l)}$, où $\deg_T(l)$ est fixé comme en (1.19).

Dans la nouvelle situation, la condition $\mathrm{RV}(r)^*$ n'est plus suffisante à nous garantir l'existence d'autant d'éléments dans $P_{\deg_T(l)}(k)$, avec un tel $\deg_T(l)$. Cette nouvelle condition nous garantit l'existence d'assez d'éléments dans $P_{\deg_T(l)}(k)$, seulement pour une valeur $\deg_T(l)$ suffisamment grande, mais pas explicitée. Le seul moyen de pouvoir, donc, répéter les mêmes passages qu'avant, en gardant les mêmes choix des paramètres $L, t, h, \deg_T(l)$ en fonction de $r, h(\Phi), c(\Phi), d, D$, est d'augmenter jusqu'à ce qu'il le faut la valeur de D, de façon que :

$$\deg_T(l) := h(\Phi)c(\Phi)\left[\frac{1}{r}\log\left(c_0^4\frac{(\log D)^2}{\log\log D}\right)\right];$$

soit assez grand pour pouvoir lui appliquer la condition $\mathrm{RV}(r)^*$.

Le Lemme 1.3.7 nous garantit, alors, de pouvoir choisir D assez grand pour cela, quitte à choisir C assez petit. Plus précisement, nous choisissons un nombre $N_\Phi \in \mathbb{N}$ étant le plus petit parmi ceux tels que pour $D \geq N_\Phi$ la valeur du degré $\deg_T(l)$ des éléments de $P_{\deg_T(l)}(k)$, exprimée en tant que fonction en D comme on vient de le faire avant, soit, en accord avec la notation choisie dans la Définition 1.1.4, supérieure à $\widetilde{N}(\Phi)$, où :

$$\widetilde{N}(\Phi) := h(\Phi)c(\Phi)\left[\frac{1}{r}\log\left(c_0^4\frac{(\log N_\Phi)^2}{\log\log N_\Phi}\right)\right];$$

et $\widetilde{N}(\Phi) \geq N(\Phi)$, où $N(\Phi)$ est justement la valeur indiquée dans la Définition 1.1.4 telle que la condition RV soit respectée par tout élément $l \in S(A)$ dont le degré $\deg_T(l)$ soit supérieur à $N(\Phi)$. Afin de pouvoir répéter les mêmes passages qu'avant et grâce au fait que la fonction en D dans laquelle $\deg_T(l)$ est exprimée, est croissante nous supposons sans perdre en généralité que :

$$N_\Phi > q^{q+d+1};$$

ce qui nous permet de supposer $D \geq q^{q+d+1}$ comme précédemment. Nous remarquons en effet que dans le cas où $N_\Phi \leq q^{q+d+1}$ il nous suffit de choisir $N_\Phi = q^{q+d+1}$ et le même résultat qu'avant, avec les mêmes estimations, restera valable ici. En sacrifiant, donc, la précision de la valeur C, qui ne sera plus C_0 mais seulement en général $\leq C_0$, on peut appliquer la même méthode sous la condition $\mathrm{RV}(r)^*$, en obtenant finalement une minoration de la forme :

$$\widehat{h}(x) \geq C\frac{(\log\log D)^\mu}{D(\log D)^\kappa};$$

avec μ et κ donnés en (1.5) et (1.6) et $C \leq C_0$, valable pour $D \geq N_\Phi$. Pour $D < N_\Phi$ on complète ce résultat encore une fois avec le Théorème 1.2.10. Ce qui nous amène finalement à l'énoncé complet du Théorème 1.1.7.

Voyons maintenant comment on pourrait donner une valeur explicite de la constante C. Nous donnons ici un énoncé général.

Remarque 1.3.8. *A tout choix d'un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ de type RV(r)* correspond, d'après la Définition 1.1.6, l'existence théorique d'un nombre $N_\Phi \in \mathbb{N}\setminus\{0\}$ avec la propriété suivante. En appelant :*

$$\widetilde{N}(\Phi) := h(\Phi)c(\Phi)\left[\frac{1}{r}\log\left(c_0^4\frac{(\log N_\Phi)^2}{\log\log N_\Phi}\right)\right];$$

on a que :

$$\widetilde{N}(\Phi) \geq N(\Phi);$$

où $N(\Phi)$ est celui qui est défini dans la Définition 1.1.6, et que pour tout $D > N_\Phi$, en conséquence du choix qu'on a fait de $\deg_T(l)$ en tant que fonction en D, $\deg_T(l) \geq \widetilde{N}(\Phi) \geq N(\Phi)$. Suite à la Définition 1.1.6 on a alors que :

$$|P_{\deg_T(l)}(k)| \geq \frac{q^{r\deg_T(l)}}{2r\deg_T(l)}.$$

Nous répétons alors exactement la même méthode déjà utilisée sous l'hypothèse que le module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ était de type $RV(r)^*$, mais en supposant $D > N_\Phi$ au lieu de $D \geq q^{q+d+1}$. Pour $D > N_\Phi > q^{q+d+1}$ nous obtiendrons donc à nouveau :

$$\widehat{h}(x) \geq \frac{h(\Phi)c(\Phi)}{768rq^d c_0^{1+\frac{4d}{r}h(\Phi)c(\Phi)}} \frac{(\log\log D)^{2+\frac{d}{r}h(\Phi)c(\Phi)}}{D(\log D)^{1+\frac{2d}{r}h(\Phi)c(\Phi)}};$$

où c_0 est défini en (1.46). Appliquant à nouveau le Théorème 1.2.10 au cas où $D \leq N_\Phi$, on pourra donc expliciter la constante $C \leq C_0$ de la deuxième partie du Théorème 1.1.7 comme il suit :

$$C = \min\{q^{-5d(2(d+1)h(\Phi)+1)(N_\Phi-1)^2c(\Phi)^2}, \frac{h(\Phi)c(\Phi)}{768rq^d c_0^{1+\frac{4d}{r}h(\Phi)c(\Phi)}}\}.$$

1.3.2 Cas pas séparable

Si x n'est pas forcément séparable sur k, soient $D_{p.i.}$ son degré d'inséparabilité et $D_{sep.}$ son degré de séparabilité sur k. On est donc dans la suivante situation :

$$D = [k(x):k] = D_{sep.}D_{p.i.};$$

où :

$$D_{sep.} = [k(x):k]_{sep.} \texttt{ et } D_{p.i.} = [k(x):k]_{p.i.} = p^e;$$

pour un nombre entier $e \in \mathbb{N}$ opportun. On se propose d'étudier comment les résultats obtenus sous l'hypothèse de séparabilité se modifient avec l'introduction de l'hypothèse d'inséparabilité. Ce que nous obtenons est le Théorème 1.1.8.

Tout d'abord, on notera :

$$k_x^{p.i.} := k^{p.i.} \cap k(x);$$

où $k^{p.i.}$ est la clôture purement inséparable de k dans $\overline{k}$. Soient $a_1, ..., a_d \in \overline{k}$ les coefficients de Φ, engendrant, comme dans le Lemme 1.3.1, une extension finie $k(\Phi) := k(a_1, ..., a_d)$ de k, telle que :

$$D' := [k(\Phi, x) : k(\Phi)];$$

$$D' = D'_{sep.}D'_{p.i.};$$

où :

$$D'_{sep.} := [k(\Phi, x) : k(\Phi)]_{sep.} \texttt{ et } D'_{p.i.} := [k(\Phi, x) : k(\Phi)]_{p.i.} =: p^{e'};$$

où $e' \in \mathbb{N}$ est tel que $e' \leq e$. Etant donné $c(\Phi) := [k(\Phi) : k]$ comme précedemment, on définit :

$$c_1(\Phi) := [k(\Phi) : k]_{sep.} \textit{ et } c_2(\Phi) := [k(\Phi) : k]_{p.i.}.$$

La preuve du Théorème 1.1.8 se déroule de façon analogue au cas séparable. En général la plupart des raisonnements ne sont pas concernés par les changements, sauf un nombre limité de passages clés qu'on va reprendre. Le premier d'entre eux est celui qui est résumé dans le Lemme 1.3.1, dont la nouvelle reformulation est celle qui suit :

Lemme 1.3.9. *1. Soit $x \in \mathbb{D}(\overline{k})_{NT}$ ayant degré d'inséparabilité sur k égal à $D_{p.i.}$, et $\sigma_1, ..., \sigma_{D'_{sep.}}$ les différents plongements de $k(\Phi, x)$ fixant $k(\Phi)$, où on note :*

$$D' = D'_{sep.} D'_{p.i.} = [k(\Phi, x) : k(\Phi)].$$

Pour tout couple $(a, b) \in A^2$ telle que $a/b \notin \mathbb{F}_q$, on a :

$$\sigma_i(\Phi(a)(x)) \neq \sigma_j(\Phi(b)(x))$$

pour tout couple $(i, j) \in \{1, ..., D'_{sep.}\}^2$.

2. Soit $\boldsymbol{M}$, un sous ensemble de A formé d'éléments premiers entre eux à deux à deux. Alors le nombre d'éléments $a \in \boldsymbol{M}$ pour lesquels il existe $i \neq j$ dans $\{1, ..., D'_{sep.}\}$ tels que $\sigma_i(\Phi(a)(x)) = \sigma_j(\Phi(a)(x))$ est majoré par $\log D_{sep.} / \log 2$.

Démonstration. 1. En ce qui est du premier point, on répéte les mêmes passages dont on s'était servi pour montrer l'analogue dans le cas séparable, sauf pour le fait que le nombre de conjugués d'un élément de la forme $\Phi(a)(x)$, qui sont tous différents des conjugués d'un différent $\Phi(b)(x)$, est au plus $D'_{sep.}$.

2. Même ce point est prouvé avec les mêmes raisonnements qui montrent son analogue dans le cas séparable, sauf que sans l'hypothèse de séparabilité de x sur k, les ensembles $I(a, i)$ ont une cardinalité au plus $D'_{sep.}$, ce qui nous amène à une inégalité de la forme :

$$2^{|\mathbf{M}|} < D'_{sep.};$$

donc :

$$|\mathbf{M}| < \log D'_{sep.} / \log 2.$$

□

Le Corollaire 1.2.11 reste par contre valable sans aucune hypothèse de séparabilité sur $k(x)/k$, ce qui nous permet encore une fois de choisir une minoration de D, que nous fixons encore à $D \geq q^{q+d+1}$, en minorant éventuellement $\widehat{h}(x) \geq c_2^{-(q^{q+d+1}-1)^2 c(\Phi)^2}$ dans le cas où $D \leq q^{q+d+1} - 1$, en répétant exactement les mêmes passages déjà faits dans le cas séparable.

Nous allons re-construire la fonction polynomiale auxiliaire dans cette nouvelle situation.

Comme on a déjà fait, on se propose de construire un polynôme

$$G(X, Y) = \sum_{i=0}^{L-1} \sum_{j=0}^{L-1} p_{ij} X^i Y^j$$

à coefficients dans A et un élément $N \in A \setminus \{0\}$ tels que le polynôme $G_N(X) = G(X, \Phi(N)(X)) \in A[\Phi][X] \setminus \{0\}$ s'annule au moins à l'ordre $t' := tp^{e'}$ en x. Comme précédemment, $\deg_T(N) = \deg_T(N)$ est tel que $q^{d \deg_T(N)} > L - 1$ en imposant :

$$\deg_T(N) := [\frac{1}{d} \log L] + 1;$$

ce qui donne :

$$L - 1 < q^{d \deg_T(N)} \leq q^d L.$$

La condition d'annulation de $G_N(X)$ en x à l'ordre t' prévoit à nouveau qu'on cherche les coefficients de $G_N(X)$ dans l'espace des solutions d'un système linéaire à L^2 inconnues et t' conditions données par l'annulation des dérivées divisées de $G_N(X)$ en x jusqu'à l'ordre t'. Nous montrons maintenant que le nombre de ces conditions peut se ramener à t seulement. En effet, si x est zéro de $G_N(X)$ on a comme première condition que :

$$G_N(x) = 0.$$

Il s'agit d'une équation linéaire à L^2 inconnues dont l'espace des solutions contient évidemment celui auquel nous sommes intéressés. Par conséquent, les coefficients de $G_N(X)$ qui nous intéressent seront tels que, dans l'anneau factoriel $k(\Phi)[X]$:

$$\Delta(X)|G_N(X);$$

avec $\Delta(X) \in k(\Phi)[X]$ polynôme minimal de x sur $k(\Phi)$. Comme le degré de pure inséparabilité de x sur $k(\Phi)$ est $D'_{p.i.} = p^{e'}$, x est racine de $\Delta(X)$ à l'ordre $p^{e'}$. Elle est donc racine au moins au même ordre de $G_N(X)$ également. La condition de simple annulation de $G_N(X)$ en x implique alors déjà implicitement les $p^{e'} - 1$ autres conditions :

$$d^{(h)} G_N(x) = 0;$$

avec $h \leq p^{e'} - 1$. De la même manière, intersecter cet espace de solutions avec celui de l'équation linéaire :

$$d^{(p^{e'})} G_N(x) = 0;$$

impose que :

$$\Delta(X)|\frac{G_N(X)}{\Delta(X)};$$

en tant qu'éléments de $k(\Phi)[X]$ comme, par la Remarque 1.3.4, une telle intersection implique que x est racine de $G_N(X)$ à l'ordre au moins $p^{e'} + 1$, alors que les racines de $\Delta(X)$ ne sont qu'à l'ordre $p^{e'}$ seulement. Puisque on a qu'en effet :

$$\Delta(X)^2 | G_N(X);$$

on aura aussi que les $p^{e'} - 1$ conditions :

$$d^{(h)} G_N(x) = 0;$$

avec $h = p^{e'} + 1, ..., 2p^{e'} - 1$ sont conséquences de la condition précédente $d^{(p^{e'})} G_N(x) = 0$. En conclusion, en répétant les mêmes passages à chaque condition $G_N(x) = 0$, $d^{(p^{e'})} G_N(x) = 0$, ..., $d^{((t-1)p^{e'})} G_N(x) = 0$, le système linéaire qu'on a effectivement à résoudre est finalement de la forme :

$$d^{(hp^{e'})} G_N(x) = 0;$$

avec $h = 0, ..., t-1$ et il est équivalent (et non pas simplement contenu) à celui de la forme $d^{(h)}G_N(x) = 0$ pour chaque $h = 0, ..., t'-1$.

L'estimation des coefficients de G_N qui suit du Lemme de Siegel est alors :

$$\deg_T(p_{ij}) \leq \frac{Dc(\Phi)}{L^2 - tDc(\Phi)} \sum_{h=0}^{t-1} h(\{\sum_{(a,b,\overline{n})\in\mathcal{I}(i,j,h)} x^{i-a}(\Phi(N)(x))^{j-b} \prod_{i=0}^{d\deg_T(N)} \widetilde{a}_i^{n_i}\});$$

où :

$$\mathcal{I}(i,j,h) := \{(a,b), 0 \leq a \leq \min\{i,h\}, 0 \leq b \leq \min\{j,h\},$$
$$, a + \sum_{i=0}^{d\deg_T(N)} n_i q^i = hp^{e'}, \sum_{i=0}^{d\deg_T(N)} n_i = b\}.$$

On remarque que la formulation du Lemme de Siegel est indépendante de l'hypothèse de séparabilité ou d'inséparabilité, indiquant avec D le degré total de x sur k. En reprenant les mêmes passages relatifs au cas séparable, on parvient à la majoration suivante des coefficients du polynôme $G_N(X)$:

$$h(p_{ij}) \leq \frac{Dc(\Phi)}{L^2 - tDc(\Phi)} \sum_{0\leq h\leq t-1} (L[h(x) + h(\Phi(N)(x))] + \deg_T(N)h(\Phi)hp^{e'}).$$

Nous choisissons ici :

$$L := \left[c_0^2 \frac{D\log D}{(\log\log D)^2} p^{e'}\right] + 1; \tag{1.47}$$

$$t := \left[c_0^3 \frac{D\log D}{(\log\log D)^3} p^{e'}\right]; \tag{1.48}$$

$$h := \left[c_0 \frac{D}{(\log\log D)^2}\right]; \tag{1.49}$$

où c_0 est un nombre entier positif qu'on choisira de manière opportune plus tard. En supposant :

$$c_0 \geq c(\Phi); \tag{1.50}$$

nous avons encore une fois que :

$$L^2 - tDc(\Phi) \geq \frac{1}{2}L^2;$$

suite à la condition $D \geq q^{q+d+1}$. En dévéloppant les calculs comme dans le précédent cas nous obtenons alors que :

$$h(p_{ij}) \leq \frac{Dc(\Phi)}{L^2 - tDc(\Phi)} \sum_{0\leq h\leq t-1} (L[h(x) + h(\Phi(N)(x))] + \deg_T(N)h(\Phi)hp^{e'}) \leq$$

$$\leq 2\frac{Dc(\Phi)}{L^2} \sum_{0\leq h\leq t-1} (2Lq^{d\deg_T(N)}\widehat{h}(x) + 4(d+1)h(\Phi)L + \deg_T(N)h(\Phi)hp^{e'}) \leq$$

$$\leq 2\frac{Dtc(\Phi)}{L^2}(2q^d L^2 \widehat{h}(x) + 4(d+1)h(\Phi)L + \frac{1}{d}h(\Phi)(\log L)tp^{e'}) \leq$$

$$\leq 4q^d Dtc(\Phi)\widehat{h}(x) + 8(d+1)h(\Phi)c(\Phi)\frac{Dt}{L} + h(\Phi)c(\Phi)\frac{2}{d}\frac{Dt^2}{L^2}\log Lp^{e'};$$

où on a choisi :

$$\deg_T(N) := \left[\frac{1}{d}\log L\right] + 1.$$

Le polynôme auxiliaire :

$$G_N(X) = \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} p_{ij}X^i(\Phi(N)(X))^j;$$

est tel que :

$$G_N^{(h'p^{e'})}(X) = \Delta(X)^{t-h'}R_{h'}(X);$$

pour tout $h' = 0, ..., h-1$. Si $l \in A$ est un polynôme unitaire et irréductible de degré $\deg_T(l)$, respectant l'hypothèse RV, supposons que :

$$G_N^{(h'p^{e'})}(\Phi(l)(x)) \neq 0.$$

Comme précédemment, nous allons estimer la hauteur de cet élément avec une majoration et une minoration, pour tout $h' = 0, ..., h-1$. Si :

$$\zeta := N_{k(\Phi,x)/k}(G_N^{(h'p^{e'})}(\Phi(l)(x))) = N_{k(\Phi,x)/k^{p.i.}_{\Phi,x}}(G_N^{(h'p^{e'})}(\Phi(l)(x)))^{[k(\Phi,x):k]_{p.i.}};$$

alors :

$$h(\zeta) \leq [k(\Phi,x):k]h(G_N^{(h'p^{e'})}(\Phi(l)(x))) \leq [k(\Phi,x):k](h(p_{ij})+L[h(\Phi(l)(x))+h(\Phi(Nl)(x))]+$$
$$+\deg_T(N)h(\Phi)h'p^{e'}).$$

D'un autre coté :

$$h(\zeta) = h(\zeta^{-1}) \geq \max\{0, \deg_T(l)v_l(\zeta)\} \geq [k(\Phi,x):k]\deg_T(l)(t-h');$$

si $w(x) \geq 0$ pour toute $w|v_l$. En effet, en sachant que la restriction de w à $k(\Phi)$ a degré d'inertie 1 sur v_l, on peut montrer avec les mêmes passages qu'on avait fait dans le cas séparable que :

$$\Delta(\Phi(l)(x)) \equiv 0 \mod w;$$

ce qui nous donne la dernière inégalité.

S'il existe par contre, comme l'on a déjà remarqué, une extension $w|v_l$ telle que $w(x) < 0$, la même minoration directe de la hauteur canonique de x qu'on avait trouvé dans le cas séparable vaut également dans la situation générale.

L'inégalité finale se présente donc sous la suivante forme :

$$\deg_T(l)(t-h) \leq \deg_T(l)(t-h') \leq h(p_{ij})+L[h(\Phi(l)(x))+h(\Phi(Nl)(x))]+\deg_T(N)h(\Phi)h'p^{e'} \leq$$
$$\leq h(p_{ij}) + 2q^{d\deg_T(l)}L^2\widehat{h}(x) + 4(d+1)Lh(\Phi) + \deg_T(N)h(\Phi)hp^{e'}.$$

Encore une fois on remarque que $h \leq t/2$ et donc que :

$$\deg_T(l)t \leq c_4((Dtc(\Phi)\widehat{h}(x) + h(\Phi)c(\Phi)\frac{Dt}{L} + h(\Phi)c(\Phi)\frac{1}{d}\frac{Dt^2}{L^2}(\log L)p^{e'})+$$

$$+q^{d\deg_T(l)}L^2\widehat{h}(x) + Lh(\Phi) + \frac{1}{d}(\log L)h(\Phi)hp^{e'}) \leq$$

$$\leq c_4(q^{d\deg_T(l)}L^2\widehat{h}(x)+h(\Phi)c(\Phi)L+h(\Phi)c(\Phi)\frac{1}{d}\frac{Dt^2}{L^2}\log Lp^{e'}+\frac{1}{d}h(\Phi)c(\Phi)\log Lhp^{e'}); \tag{1.51}$$

où $c_4 := 24q^d$ et en utilisant le fait que $L^2 > tDc(\Phi)$. En imposant :

$$\deg_T(l) := h(\Phi)c(\Phi)\left[\frac{1}{r}\log\left(c_0^4\frac{(\log D)^3 p^{2e'}}{\log\log D}\right)\right];$$

nous devons montrer les inégalités suivantes :

$$\deg_T(l)t \geq 4c_4h(\Phi)c(\Phi)L; \tag{1.52}$$

$$\deg_T(l)t \geq 4c_4h(\Phi)c(\Phi)\frac{1}{d}\frac{Dt^2}{L^2}\log Lp^{e'}; \tag{1.53}$$

$$\deg_T(l)t \geq 4c_4\frac{1}{d}h(\Phi)c(\Phi)\log Lhp^{e'}. \tag{1.54}$$

Nous remarquons encore une fois que pour $D \geq q^{q+d+1}$ nous avons que :

$$\deg_T(l)t \geq \frac{1}{2}\frac{\alpha}{r}(4\log c_0+3\log\log D+2\log p^{e'}-\log\log\log D)c_0^3\frac{D\log D}{(\log\log D)^3}p^{e'} \geq$$

$$\geq \frac{\alpha}{r}c_0^3\frac{D\log D}{(\log\log D)^2}p^{e'}. \tag{1.55}$$

La première inégalité est de cette forme :

$$\frac{\alpha}{r}c_0^3\frac{D\log D}{(\log\log D)^2}p^{e'} \geq 4c_4\alpha 2c_0^2\frac{D\log D}{(\log\log D)^2}p^{e'};$$

donc :

$$c_0 \geq 8c_4r. \tag{1.56}$$

La deuxième inégalité est sous la suivante forme :

$$\frac{\alpha}{r}c_0^3\frac{D\log D}{(\log\log D)^2}p^{e'} \geq 4c_4\frac{\alpha}{d}\frac{c_0^6D^3(\log D)^2p^{2e'}}{(\log\log D)^6}\frac{(\log\log D)^4}{c_0^4D^2(\log D)^2p^{2e'}}(2\log c_0+\log D+$$

$$+\log\log D - 2\log\log\log D + \log p^{e'} + \log 2)p^{e'};$$

elle est donc impliquée par la suivante :

$$\frac{\alpha}{r}c_0^3\frac{D\log D}{(\log\log D)^2}p^{e'} \geq 4c_4\frac{\alpha}{d}\frac{c_0^2D}{(\log\log D)^2}(2\log c_0+2\log D+\log\log D+\log 2)p^{e'};$$

Celle-ci est elle même impliquée par la suivante :

$$c_0\log D \geq \frac{4rc_4}{d}(2\log c_0 + 4\log D).$$

Pour montrer cette inégalité nous demandons alors que :

$$c_0 \geq \frac{32rc_4}{d} = \frac{768rq^d}{d};$$

et que :

$$c_0 \log D \geq \frac{16rc_4}{d} \log c_0 = \frac{384rq^d}{d} \log c_0.$$

Comme déjà montré dans le cas séparable une telle condition est impliquée par la (1.35) :

$$c_0 \geq 768rq^d.$$

La troisième inégalité est finalement impliquée par celle-ci :

$$\frac{\alpha}{r} c_0^3 \frac{D \log D}{(\log \log D)^2} p^{e'} \geq \frac{4c_4\alpha}{d} (2 \log c_0 + \log D +$$

$$+ \log \log D - 2 \log \log \log D + \log p^{e'} + \log 2) c_0 \frac{D}{(\log \log D)^2} p^{e'}.$$

Celle-ci est alors conséquence de la suivante :

$$c_0^2 \log D \geq \frac{4rc_4}{d} (2 \log c_0 + 4 \log D);$$

et une telle condition est conséquence immédiate de la (1.35) à plus forte raison.

La condition :

$$\widehat{h}(x) < \frac{\deg_T(l) t}{4c_4 q^{d \deg_T(l)} L^2}; \tag{1.57}$$

implique donc que l'inégalité (1.51) est fausse pour tout $h' = 0, ..., h-1$, ce qui implique que le polynôme $G_N(X)$ s'annule avec multiplicité $hp^{e'}$ en $\Phi(l)(x)$. Nous allons montrer alors, comme on l'avait déjà fait dans le cas séparable, qu'il a un nombre de zéros, comptés avec leur multiplicité, supérieur à son degré, ce qui nous donnerait la contradiction cherchée.

Comme on a montré qu'une telle condition implique que $G_N(X)$ s'annule en $\Phi(l)(x)$ quelque soit l irréductible et unitaire dans A de degré $\deg_T(l)$, la condition RV supposée être satisfaite par l nous avons alors, suite au Lemme 1.3.9, que $G_N(X)$ a au moins :

$$\left(\frac{q^{r \deg_T(l)}}{2r \deg_T(l)} - \frac{\log D_{sep.}}{\log 2} \right) D'_{sep.} hp^{e'};$$

zéros comptés avec leur multiplicité. D'un autre côté nous savons aussi que :

$$\deg_X(G_N(X)) \leq 2(L-1) q^{d \deg_T(N)} \leq 2q^d L^2.$$

Ce qui nous amène alors à devoir prouver l'inégalité suivante :

$$\left(\frac{q^{r \deg_T(l)}}{2r \deg_T(l)} - \frac{\log D_{sep.}}{\log 2} \right) \frac{D}{c(\Phi)} h \geq 2q^d L^2.$$

Nous demandons, suite au Lemme 1.3.9, que la condition suivante :

$$\frac{q^{r\deg_T(l)}}{2r\deg_T(l)} \geq 2\frac{\log D_{sep.}}{\log 2};$$

soit satisfaite. Avec les encadrements usuels des parties entières (voir la preuve de l'inégalité (1.39)) on a alors que :

$$\frac{q^{r\deg_T(l)}}{2r\deg_T(l)} \geq \frac{\left(c_0^4\frac{(\log D)^3p^{2e'}}{\log\log D}\right)^\alpha}{q^{r\alpha}2\alpha(4\log c_0+3\log\log D+2\log p^{e'}-\log\log\log D)}.$$

La condition cherchée est alors conséquence de celle-ci :

$$\frac{\left(c_0^4\frac{(\log D)^3p^{2e'}}{\log\log D}\right)^\alpha}{q^{r\alpha}2\alpha(4\log c_0+3\log\log D+2\log p^{e'})} \geq 2\frac{\log D_{sep.}}{\log 2}.$$

Cette dernière est d'ailleurs conséquence de celle-ci :

$$c_0^{4\alpha}(\log D)^{3\alpha-1}p^{2\alpha e'} \geq \frac{q^{r\alpha}4\alpha}{\log 2}(\log\log D)^\alpha(4\log c_0+3\log\log D+2\log p^{e'}).$$

Une telle inégalité est impliquée par les trois conditions suivantes :

$$c_0^{4\alpha}(\log D)^{3\alpha-1}p^{2\alpha e'} \geq \frac{48q^{r\alpha}\alpha}{\log 2}(\log\log D)^\alpha\log c_0;$$

$$c_0^{4\alpha}(\log D)^{3\alpha-1}p^{2\alpha e'} \geq \frac{36q^{r\alpha}\alpha}{\log 2}(\log\log D)^{\alpha+1};$$

$$c_0^{4\alpha}(\log D)^{3\alpha-1}p^{2\alpha e'} \geq \frac{24q^{r\alpha}\alpha}{\log 2}(\log\log D)^\alpha\log p^{e'}.$$

La première de ces trois inégalités est satisfaite par la condition suivante :

$$\frac{c_0^{4\alpha}}{\log c_0} \geq \frac{48q^{r\alpha}\alpha}{\log 2}. \tag{1.58}$$

En supposant :

$$c_0 \geq 2q; \tag{1.59}$$

la condition (1.58) est conséquence de son côté des deux conditions suivantes :

$$\frac{2^{4\alpha}q^3}{\log 2+1} \geq \frac{48\alpha}{\log 2};$$

et :

$$q^{4\alpha-3} \geq q^{r\alpha};$$

qui sont toujours respectées pour tout q puissance d'un nombre premier, $\alpha \geq 1$, $r \leq 1$, $D \geq q^{q+d+1}$.

La deuxième condition est d'ailleurs conséquence de l'inégalité suivante :

$$c_0^{4\alpha}p^{\alpha e'} \geq \frac{36q^{r\alpha}\alpha}{\log 2}.$$

Une telle condition est vérifiée suite à (1.59). La troisième condition est finalement conséquence directe de la (1.58).

Nous nous sommes donc reconduits à devoir prouver l'inégalité suivante :

$$\frac{q^{r\deg_T(l)}}{4r\deg_T(l)}\frac{D}{c(\Phi)}h \geq 2q^d L^2. \tag{1.60}$$

L'inégalité qui précède la condition (1.39) nous amène donc finalement à la condition suivante :

$$\frac{\left(c_0^4\frac{(\log D)^3 p^{2e'}}{\log\log D}\right)^{\alpha}}{q^{r\alpha}4\alpha(4\log c_0+3\log\log D+2\log p^{e'}-\log\log\log D)}\frac{D}{c(\Phi)}\frac{1}{2}c_0\frac{D}{(\log\log D)^2}\geq$$

$$\geq 2q^d 4c_0^4\frac{D^2(\log D)^2}{(\log\log D)^4}p^{2e'}.$$

Ce qui est impliqué par l'inégalité qui suit :

$$\frac{c_0^{4\alpha-3}(\log D)^{3\alpha-2}p^{2(\alpha-1)e'}}{64q^{r\alpha+d}\alpha(4\log c_0+3\log\log D+2\log p^{e'})c(\Phi)(\log\log D)^{\alpha-2}}\geq 1.$$

En appellant :

$$X:=\log D;$$

et se souvenant du fait que $c(\Phi)\leq\alpha$, il nous suffira de montrer l'inégalité suivante :

$$\frac{c_0^{4\alpha-3}X^{3\alpha-2}p^{2(\alpha-1)e'}}{64q^{d+r\alpha}\alpha^2(4\log c_0+3\log X+2\log p^{e'})(\log X)^{\alpha-2}}\geq 1.$$

Une telle inégalité est conséquence de celle-ci :

$$\frac{64q^{d+r\alpha}\alpha^2((4\log c_0+2\log p^{e'})(\log X)^{\alpha-2}+3(\log X)^{\alpha-1})}{c_0^{4\alpha-3}X^{3\alpha-2}p^{2(\alpha-1)e'}}\leq 1.$$

Elle est conséquence des conditions qui suivent :

$$\frac{768q^{d+r\alpha}\alpha^2(\log X)^{\alpha-2}\log c_0}{c_0^{4\alpha-3}X^{3\alpha-2}}\leq 1;$$

$$\frac{384q^{d+r\alpha}\alpha^2(\log X)^{\alpha-2}}{c_0^{4\alpha-3}X^{3(\alpha-1)}}\leq 1;$$

$$\frac{576q^{d+r\alpha}\alpha^2(\log X)^{\alpha-1}}{c_0^{4\alpha-3}X^{3\alpha-2}}\leq 1.$$

La première des trois dernières inégalités est impliquée par la condition suivante :

$$\frac{c_0}{\log c_0}\geq 768q^{d+r\alpha}\alpha^2.$$

En imposant :

$$c_0\geq Ad\alpha^3q^{d+r\alpha}; \tag{1.61}$$

où $A \in \mathbb{N}\backslash\{0\}$, une telle condition est conséquence des trois inégalités suivantes :

$$\frac{A}{\log A} \geq 2304;$$

$$\frac{Ad}{d+\log d} \geq 2304;$$

$$\frac{A\alpha}{3\log\alpha+\alpha} \geq 2304.$$

Le choix :

$$A := 35000;$$

nous donne alors la condition cherchée. Nous demandons alors que :

$$c_0 \geq 35000 d\alpha^3 q^{d+r\alpha}. \tag{1.62}$$

Les deux dernières inégalités sont par contre une conséquence directe de la première.

Nous obtenons donc la minoration suivante de la hauteur canonique de x :

$$\widehat{h}(x) \geq \frac{\deg_T(l)t}{96q^{d(\deg_T(l)+1)}L^2} \geq \frac{\frac{\alpha}{r}c_0^3\frac{D\log D}{(\log\log D)^2}p^{e'}}{96q^d\left(c_0^4\frac{(\log D)^3p^{2e'}}{\log\log D}\right)^{\frac{\alpha d}{r}}4c_0^4\frac{D^2(\log D)^2}{(\log\log D)^4}p^{2e'}} \geq$$

$$\geq \frac{\frac{\alpha}{r}(\log\log D)^{2+\frac{\alpha d}{r}}}{384q^dc_0^{\frac{4\alpha d}{r}+1}(\log D)^{\frac{3\alpha d}{r}+1}p^{(\frac{2\alpha d}{r}+1)e'}D}.$$

La majoration :

$$p^{e'} = D'_{p.i.} \leq D_{p.i.} = p^e;$$

nous donne finalement l'énoncé du Théorème 1.1.8.

1.4 Modules de Drinfeld et premiers à réduction supersingulière

Nous examinons ici les situations où un module de Drinfeld respecte effectivement la propriété RV$(r)^*$ pour $0 < r \leq 1$. Grâce au travail de C. David [Dav] Theorem 1.2, nous sommes déjà en condition de pouvoir dire que, "'en moyenne"', les modules de Drinfeld de rang 2 (supposés à coefficients dans k) satisfont la condition RV$(r, c_q)^*$, avec $r = 1/d = 1/2$ et $c_q > 0$ une constante ne dépendant que de q. Nous souhaitons ici étendre à un rang quelconque la possibilité d'exhiber une classe qui contient suffisamment de modules de Drinfeld qui respectent la propriété RV$(r)^*$ pour un certain r. Au cours de notre raisonnement nous utiliserons dans un passage clé le **Théorème de Chebotarev effectif** (voir Théorème 1.4.13), dont la formulation nous amène à considérer la classe suivante de modules de Drinfeld.

Définition 1.4.1. *Soit $r \in]0,1]$ un nombre réel et $c_1 > 0$ une constante positive. Soit $\mathbb{D} = (\mathbb{G}_a, \Phi)$ un module de Drinfeld auquel on associe un nombre naturel η. Nous disons que ce module de Drinfeld est $\boldsymbol{RV}_\eta\boldsymbol{(}r, c_1\boldsymbol{)}^*$ s'il existe un nombre naturel $N(\Phi)$ dépendant du choix de $\mathbb{D}$ tel que pour tout $N \in \mathbb{N}$ tel que $N \geq N(\Phi)$ et que $N \equiv 1$ mod (η), on ait :*

$$|\{l \in P_N(k), l \texttt{ est } RV\}| \geq c_1 \frac{q^{rN}}{N}.$$

Comme il est possible de le remarquer immédiatement, cette classe contient, r et c_1 étant fixés, la classe $\mathrm{RV}(r, c_1)^*$, avec laquelle elle coïncide dans le cas où $\eta = 1$. Nous proposons donc une preuve du fait qu'un module de Drinfeld de type CM (ou à **multiplication complexe**) de rang d premier respecte toujours la propriété $\mathrm{RV}_\eta(1, 1/2d)^*$, où η est un nombre entier qu'on définira plus tard, ne dépendant que du choix du module de Drinfeld.

Il est facile de voir qu'on peut donc obtenir pour ces modules des minorations de la hauteur des points pas de torsion similaires à nos Théorèmes 1.1.7 et 1.1.8. En effet il suffit de choisir dans la preuve de transcendance $\deg_T(l) \equiv 1$ mod (η) (voir Remarque 1.3.8), ce qui ne demande qu'à modifier des constantes dans nos preuves et permettrait d'obtenir une minoration de la hauteur canonique de même ordre de grandeur en D que celle contenu dans les Théorèmes 1.1.7 et 1.1.8. Etant donné la lourdeur des constantes à expliciter nous ne détaillerons pas la nouvelle constante C qu'on obtiendrait.

Avant de commencer et pour se conformer à une notation universelle (voir par exemple [Brown] ou [Pn]) on appelle un élément $p(T) \in S(A)$ unitaire respectant la propriété RV par rapport à un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ assigné, un premier à **réduction supersingulière** de Φ.

Jusqu'à présent on a considéré toujours le cas des modules de Drinfeld définis sur un corps extension finie de k. En général, ce n'est pas forcément le cas et, plus précisément, on a la notion de **caractéristique** d'un module de Drinfeld défini sur un corps $\mathcal{F}$. On donne un morphisme :

$$i : A \to \mathcal{F};$$

qui fait de $\mathcal{F}$ un $A-$module et dont un générateur $p(T) \in S(A)$ du noyau (on suppose ce polynôme unitaire à une multiplication par un élément de $\mathbb{F}_q^*$ près sans rien perdre en généralité) est appelé caractéristique du module de Drinfeld défini sur $\mathcal{F}$. On dira que $\mathcal{F}$ est un $A-$corps s'il existe un tel morphisme i. Par abus de notation, i et $\mathcal{F}$ étant fixé, on continuera de noter $\mathbb{D} = (\mathbb{G}_a, \Phi)$ le module de Drinfeld. Jusqu'à présent les modules de Drinfeld qu'on a considérés étaient de caractéristique 0.

Soit $\mathbb{D} = (\mathbb{G}_a, \Phi)$ un module de Drinfeld de caractéristique quelconque, défini sur un corps $\mathcal{F}$ qui est aussi un $A-$module. On définit, alors :

$$End_{\mathcal{F}}(\Phi) := \{P(\tau) \in \mathcal{F}\{\tau\}, \forall a \in A, \Phi(a)P = P\Phi(a)\}.$$

Il s'agit d'un $A-$module via l'action de Φ et il est aussi un sous-anneau de

$\mathcal{F}\{\tau\}$. Comme on peut le constater, il n'a pas d'éléments de $A-$torsion [8] et par conséquent c'est un module projectif. Comme A est un anneau principal, $End_{\mathcal{F}}(\Phi)$ est en particulier un $A-$module libre. Mieux encore, on a le Théorème suivant :

Théorème 1.4.2. *$End_{\mathcal{F}}(\Phi)$, quelque soit la caractéristique de Φ, est de rang fini et $\leq d^2$ sur A, d étant le rang de Φ.*

Démonstration. Soit a un élément dans A, premier avec la caractéristique de Φ. On a, alors, (voir [Goss], Theorem 4.7.8) l'inclusion naturelle :

$$End_{\mathcal{F}}(\Phi)\otimes_A A/(a) \hookrightarrow End_A(\Phi[a]) \simeq End_{A/(a)}(\Phi[a]) \simeq (A/(a))^{d\times d}.$$

En effet, si $P(\tau)$ est 0 sur $\Phi[a]$, cela veut dire que $\Phi(a)(\tau)$ en est diviseur droit dans l'algèbre de Ore $\mathcal{F}\{\tau\}$. Les propriétés de cette dernière impliquent donc que $P = P_0\Phi(a)$, avec $P_0 \in End_{\mathcal{F}}(\Phi)$. Ce qui correspond à l'élément 0 dans $End_{\mathcal{F}}(\Phi)/aEnd_{\mathcal{F}}(\Phi)$. Or, si $M := End_{\mathcal{F}}(\Phi)$ n'était pas un $A-$module de type fini, on aurait, pour tout $i \in \mathbb{N}\setminus\{0\}$:

$$m_1, ..., m_i \in V := End_{\mathcal{F}}(\Phi)\otimes_A k_\infty;$$

éléments $k_\infty-$linéairement indépendants, engendrants l'espace vectoriel :

$$V_i := \bigoplus_{j=1}^{i} m_j k_\infty \subset V.$$

Le $A-$sous-module $M_i := V_i \cap M$ est alors de type fini, libre et de rang i. Les deux premières conclusions sont évidentes. Pour la troisième : on remarque que M_i est un sous-$A-$module discret [9] de V_i, comme A est sous-module discret de k_∞ (il suffit de choisir le voisinage ouvert $N := \{x \in k_\infty, v_{1/T}(x) > 0\}$ de 0), et que k_∞ est un corps local, tel que k_∞/A est compacte par rapport à la topologie $1/T-$adique. Un résultat général (voir [Goss], Proposition 4.6.2) nous dit alors que dans une telle situation le sous-$A-$module est de type fini et de rang sur A au plus $i = \dim_k(V_i)$. Comme un sous-$A-$module d'un module libre est encore libre, $M_i = A^j$, avec $j \leq i$. Mais M est $A-$module libre et $V_i \simeq k_\infty^i$, ce qui implique forcément $j \geq i$, puisque $M_i = V_i \cap M$. En effet, pour tout $m_j \in k_\infty \setminus \{0\}$ il existe toujours $\alpha_j \in \frac{1}{m_i}A$ tel que $\widetilde{m_j} := m_j\alpha_j \in A$. Une $A-$relation entre les i éléments $\widetilde{m_1}, ..., \widetilde{m_i}$ est de la forme $\sum_{j=1}^{i}\beta_j\widetilde{m_j} = 0$, où $(\beta_1, ..., \beta_i) \in A^i \setminus \{0\}$. Elle ne peut donc pas exister sans entrer en contradition avec l'hypothèse de $k_\infty-$indépendance linéaire de $m_1, ..., m_i$, ce qui prouve l'existence d'au moins i éléments de M $A-$libres dans V_i. Par conséquent, $\rho_A(M_i) \geq i$. Soit, donc, $0 \neq a \in A$. On a que $a^{-1}M_i/M_i \subset a^{-1}M/M$. En effet, si $m \in M$ est aussi dans $a^{-1}M_i$, alors $m \in M \cap V_i = M_i$. On remarquera aussi que $a^{-1}M_i/M_i \simeq (A/(a))^i$. On a donc une suite de sous-$A-$modules de la forme $(A/(a))^i$ contenus dans $M/aM \simeq a^{-1}M/M$, pour tout $i \in \mathbb{N}\setminus\{0\}$. Comme, d'ailleurs, on vient de prouver aussi que $M/aM \subset End_{A/(a)}(\Phi[a])$, dont le rang en A est $\leq d^2$, on

8. On remarque que $\Phi : A \to \mathcal{F}\{\tau\}$ est injectif dans tous les cas en tant que morphisme d'algèbres.

9. Soit V un espace vectoriel de type fini sur un corps de valuation K. Il est donc muni de la norme du sup $||.||_\infty$. Un sous-groupe additif H de V est dit **discret** si et seulement s'il existe un voisinage ouvert N de 0 dans V tel que $N \cap H = \{0\}$.

a la contradition à l'hypothèse que le $A-$rang de M soit infini. On aura donc $M = M_i$, et $i \leq d^2$. Par conséquent, $End_{\mathcal{F}}(\Phi)$ a un rang $\leq d^2$, en tant que $A-$module. $\square$

On met en évidence comment ces passages ne nécessitent aucune hypothèse sur la caractéristique de Φ.

On a déjà remarqué, en caractéristique 0, comment la fonction exponentielle est non seulement un revêtement topologique de Φ, mais aussi un morphisme algébrique entre le $A-$module $\mathcal{C}$ trivialement défini par la multiplication usuelle, et le module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$. On sait que le noyau Λ de cette fonction est un $A-$réseau de rang d, où d est le rang de Φ, et par conséquent on peut identifier, étant donné n'importe quel $a \in A$, les points de $a-$torsion de Φ aux éléments de $a^{-1}\Lambda/\Lambda$ à travers l'exponentielle. En particulier, on a l'isomorphisme de $A/(a)-$modules :

$$\Phi[a] \simeq a^{-1}\Lambda/\Lambda \simeq (A/(a))^d.$$

Plus précisément, on a une immersion naturelle :

$$End_{\mathcal{F}}(\Phi) \hookrightarrow End_{\mathcal{C}}(\Lambda);$$

où l'anneau $End(\Lambda)$ des endomorphismes du réseau Λ est défini comme il suit :

$$End(\Lambda) := \{c \in \mathcal{C}, c\Lambda \subset \Lambda\}.$$

Mieux encore (voir [Goss], Théorème 4.6.9) on a une équivalence entre la catégorie des modules de Drinfeld à caractéristique 0 et la catégorie des $A-$réseaux, où la définition de morphisme dans les deux cas est analogue à celle d'endomorphisme.

Tout ça n'est cependant plus vrai en caractéristique $p(T) \in S(A)$. Dans ce cas il n'y a plus d'isomorphisme $\Phi[a] \simeq (A/(a))^d$ que dans la situation où a est premier avec la caractéristique p de Φ. Si ce n'est pas le cas, en effet, le polynôme additif associé $\Phi(a)(X)$ n'est plus séparable et par conséquent $|\Phi[a]| \neq q^{d \deg_T(a)}$. Ce qui montre aussi comment la catégorie des $A-$réseaux dans $\mathcal{C}$ est équivalente à celle des modules de Drinfeld à travers l'exponentielle, seulement dans le cas à caractéristique 0, seule situation dans laquelle la construction de ce revêtement est possible.

La conséquence immédiate de tout ça est que l'anneau $End_{\mathcal{F}}(\Phi)$ est commutatif si Φ est à caractéristique 0 (puisque $End_{\mathcal{C}}(\Lambda)$ l'est clairement), mais pas forcément en caractéristique $p(T) \neq 0$.

Lemme 1.4.3. *Soit Φ un module de Drinfeld de caractéristique 0 défini sur le corps $\mathcal{F}$, de rang d. Le rang $\rho(\Phi)$ du $A-$module $End_{\mathcal{F}}(\Phi)$ est un nombre qui divise d.*

Démonstration. On a déjà remarqué pourquoi ce $A-$module a un rang fini, et $\leq d^2$. En tant qu'anneau il est donc entier de degré n sur A. Ainsi on peut étendre de façon naturelle l'homomorphisme :

$$\Phi : A \to \mathcal{F}\{\tau\};$$

de la façon suivante :

$$\widetilde{\Phi} : End_{\mathcal{F}}(\Phi) \to \mathcal{F}\{\tau\}$$

$$P(\tau) \mapsto P(\tau).$$

grâce à la relation algébrique induite par l'intégralité, on peut voir comment cette application est compatible avec l'originelle sur A [10]. L'extension $\widetilde{\Phi}$ de Φ à $End_{\mathcal{F}}$ donne lieu à un nouveau module de Drinfeld, défini cette fois sur une extension entière de A, et de rang $\widetilde{d}|d$. Etant toujours de caractéristique 0, il est aussi associé à un $End_{\mathcal{F}}(\Phi)-$réseau de rang $\widetilde{d}$ dans $\mathcal{C}$, qui doit forcément être aussi un $A-$réseau de rang d restreignant $\widetilde{\Phi}$ à Φ. Comme tout $End_{\mathcal{F}}(\Phi)-$période de Λ est un entier de degré ρ sur A, on obtient par conséquent que :

$$\rho\widetilde{d} = d.$$

Ce qui prouve l'assertion. □

Définition 1.4.4. *Soit Φ module de Drinfeld de caractéristique quelconque, défini sur un corps L. Soit K/k une extension finie de k =Frac(A). Soit $\mathcal{O}_K$ un $A-$ordre de K. On dit, alors, que Φ est* ***de type CM par rapport à*** *$\mathcal{O}_K$ s'il existe un plongement algébrique $\mathcal{O}_K \hookrightarrow End_L(\Phi)$.*

Lemme 1.4.5. *Soit Φ un module de Drinfeld défini comme dans la définition 1.4.4. On suppose qu'il est de type CM par rapport à $\mathcal{O}_K$. Il est alors isogène sur L à un module de Drinfeld Ψ de type CM par rapport à l'ordre maximal des $A-$entiers $\widetilde{\mathcal{O}}_K$.*

Démonstration. Voir [Goss], Proposition 4.7.19. □

Définition 1.4.6. *Un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ défini sur $\mathcal{F}$ extension finie de k, est dit de* ***type CM*** *ou bien à* ***multiplication complexe*** *si le rang de $End_{\mathcal{F}}(\Phi)$ en tant que $A-$module est d.*

Remarque 1.4.7. *Tout module de Drinfeld de rang* 1 *est à multiplication complexe.*

Définition 1.4.8. *Soit Φ un module de Drinfeld de caractéristique* 0 *et de rang d, et soit $\mathcal{F}$ le corps de ses coefficients. Soit :*

$$\Phi(T)(\tau) = T + a_1\tau + ... + a_d\tau^d \in \mathcal{F}\{\tau\}.$$

Soit $p(T) \in S(A)$. Soit $\mathcal{A}_{p(T)}$ l'anneau des $p(T)-$entiers de $\mathcal{F}$. Soient, respectivement, A_∞ et $\mathcal{A}_{p(T)_\infty}$ les complétés de A et $\mathcal{A}_{p(T)}$ par rapport à la valuation $1/T-$adique. Il existe alors un unique $P_{p,\infty} \in$ Spec $\mathcal{A}_{p_\infty}$ qui étend $p(T) \in$ Spec A_∞. Nous convenons d'appeler $p(T)$ premier de ***bonne réduction*** *de Φ si les coefficients de Φ sont tous contenus dans $\mathcal{O}_{P_{p,\infty}}$, anneau de $P_{p,\infty}-$valuation de $\mathcal{F}$, et $a_d \in \mathcal{O}^*_{P_{p,\infty}}$.*

Soit Φ un module de Drinfeld de rang d et de caractéristique 0. Tout $p(T) \in S(A)$, sauf un nombre fini, est premier de bonne réduction de Φ. Les coefficients

10. On remarquera aussi qu'en général ce n'est pas toujours possible d'étendre Φ à n'importe quelle extension entière de A.

de ce dernier sont donc dans $\mathcal{O}_{P_{p,\infty}}$. Cette réduction donne lieu alors à un module de Drinfeld réduit :

$$\Phi^{v_p} : A \to \mathbb{F}_{q^s}\{\tau\};$$

de même degré d et de caractéristique $p(T)$. Les coefficients de Φ^{v_p} sont en effet contenus dans le corps résiduel $\mathbb{F}_{q^s} := \mathcal{O}_{P_{p,\infty}}/P_{p,\infty}$, où :

$$s = [\mathcal{O}_{P_{p,\infty}}/P_{p,\infty} : \mathbb{F}_q] = [\mathcal{O}_{P_{p,\infty}}/P_{p,\infty} : A/p(T)] \deg_T(p(T)) = f(P_{p,\infty}|p) \deg_T(p(T)).$$

Nous convénons d'appeler dorénavant avec un abus de notation **réduction de Φ, ou de ses coefficients, modulo $p(T)$, ou modulo v_p** la réduction de ces objets modulo $P_{p,\infty}$. On appelle :

$$F := \tau^s.$$

On a, alors, que $F \in End_{\mathbb{F}_{q^s}}(\Phi^{v_p})$. Comme on a déjà remarqué, il s'agit d'une $A-$algèbre de rang $\leq d^2$, centrale sur A (ce qui veut dire que A est bien son centre), pas forcément commutative. On a donc toujours l'action de A sur cette dernière par l'homomorphisme d'algèbres :

$$\Phi^{v_p} : A \hookrightarrow End_{\mathbb{F}_{q^s}}(\Phi^{v_p});$$

qui est encore injectif. On considère $End_{\mathcal{F}}(\Phi)/A$ comme une extension entière finie d'anneaux. En général on ne peut pas étendre l'homomorphisme Φ^{v_p} (tout comme Φ) à une extension entière de A, mais la nature même des éléments de $End_{\mathcal{F}}(\Phi)$ rend une telle extension naturelle dans ce cas particulier. Plus précisément, on étend Φ^{v_p} à :

$$\widetilde{\Phi^{v_p}} : End_{\mathcal{F}}(\Phi) \hookrightarrow End_{\mathbb{F}_{q^s}}(\Phi^{v_p})$$

$$P(\tau) \mapsto P(\tau)^{v_p};$$

où $P(\tau)^{v_p}$ est obtenu en réduisant modulo $p(T)$ les coefficients de $P(\tau)$. On remarque, en effet, qu'une telle application a son image dans $End_{\mathbb{F}_{q^s}}(\Phi^{v_p})$ (pour tout $a \in A$, $P(\tau)^{v_p}\Phi_a^{v_p} = (P(\tau)\Phi_a)^{v_p} = (\Phi_a P(\tau))^{v_p} = \Phi_a^{v_p} P(\tau)^{v_p})$ [11], et qu'elle est injective (si $P(\tau)^{v_p} = 0$, $P(\tau) \in End_{\mathcal{F}}(\Phi) \setminus \{0\}$ est élément entier sur A, satisfaisant un polynôme minimal $f(X) \in A[X]$ dont le coefficient constant α est forcément différent de 0. Comme $(\cdot)^{v_p}$ est un homomorphisme d'algèbres, $f(P(\tau)) = 0$ implique $f(0) = f(P(\tau)^{v_p}) = f(P(\tau))^{v_p} = 0$, implique $\Phi^{v_p}(\alpha) = 0$, qui, suite à l'injectivité de Φ^{v_p}, implique $\alpha = 0$). Comme conséquence de cela on a que le $A-$rang de $End_{\mathbb{F}_{q^s}}(\Phi^{v_p})$ est en théorie supérieur à celui de $End_{\mathcal{F}}(\Phi)$.

Nous étendons également Φ et Φ^{v_p} à k de façon naturelle. En effet, l'algèbre de Ore $\mathcal{F}\{\tau\}$ admet l'algorithme de division à droite et il est donc possible de la plonger dans son algèbre de division des fractions droites, qui contiendra de façon naturelle Frac($End_{\mathcal{F}}(\Phi)$), où $End_{\mathcal{F}}(\Phi)$ contient l'image de Φ dans $\mathcal{F}\{\tau\}$.

11. L'application de réduction modulo v_p des coefficients est en effet un homomorphisme d'algèbres :

$$(\cdot)^{v_p} : End_{\mathcal{F}}(\Phi) \to End_{\mathbb{F}_{q^s}}(\Phi^{v_p});$$

mais pas forcément surjectif, en accord avec le fait que, à la différence de $End_{\mathcal{F}}(\Phi)$, $End_{\mathbb{F}_{q^s}}(\Phi^{v_p})$ n'est pas nécessairement commutative.

On répète les mêmes passages encore plus facilement pour Φ^{v_p}, $\mathbb{F}_{q^s}$ étant un corps parfait et donc tel que $\mathbb{F}_{q^s}\{\tau\}$ admet l'algorithme de division à gauche aussi, constituant un $\mathbb{F}_q[F]-$ordre maximal dans $\mathbb{F}_{q^s}(\tau)$, voir [Goss], Lemma 4.12.6.

On sait (voir [Goss], Proposition 4.7.13) que chaque isogénie entre deux modules de Drinfeld divise un élément de $A \setminus \{0\}$. On va donc tensoriser sur A par k la catégorie des modules de Drinfeld et des isogénies. On étend donc de façon naturelle les homomorphismes d'algèbres Φ et Φ^{v_p} à k. Si w est une place sur k on appelle :

$$V_w(\Phi^{v_p}) := T_w(\Phi^{v_p}) \otimes_A k;$$

où $T_w(\Phi^{v_p})$ est le A_w-module de Tate (voir [Goss], paragraphe 4.10, pour la définition). On rappelle que dans le cas où $w \neq p(T)$:

$$T_w(\Phi^{v_p}) \simeq A_w^d.$$

On sait que F est entier, en tant qu'élément de $End_{\mathbb{F}_{q^s}}(\Phi^{v_p})$, sur A. On appelle n son $A-$degré. On appelle d'ailleurs :

$$D := End_{\mathbb{F}_{q^s}}(\Phi^{v_p}) \otimes_A k.$$

Soit :

$$E := k(F) \subset D.$$

On appelle :

$$n := [E : k];$$

$$t := [K : E];$$

où K est un corps maximal dans D contenant E (voir [Goss], Corollaire 4.11.15 pour voir que leur dimension sur E est toujours la même et qu'ils sont égaux à leurs centralisateurs dans D, en sachant, voir [Goss] Lemma 4.12.7, que l'algèbre de division D est centrale sur E). On a alors le Théorème suivant :

Théorème 1.4.9. *1. Il n'y a qu'une seule place P_E sur E qui est zéro de F, et une seule place ∞_E sur E qui divise ∞.*

2. $V_w(\widetilde{\Phi^{v_p}})$ est E_w-espace vectoriel de dimension t pour toute place $w \neq P_E, \infty_E$ dans E, alors que $V_{P_E}(\widetilde{\Phi^{v_p}}) = 0$.

3. $d = tn$.

4. $w_{\infty_E}(F) = -n$.

Démonstration. Voir [Goss], Théorème 4.12.8, points 1, 3, 4 et 5. □

Lemme 1.4.10. *En considérant E/k comme une extension de corps dans D construite à partir du plongement de k dans D par Φ^{v_p}, où $p(T) \in S(A)$ est premier de bonne réduction de Φ, P_E est une place dans E étendant p dans l'extension entière $\mathcal{O}_E/A$, où $\mathcal{O}_E$ est l'anneau des $A-$entiers de E. Par conséquent :*

$$p(T)|N_{E/k}(F).$$

Démonstration. On sait que (voir [Goss], paragraphe 4.11) toute algèbre $L\{\tau\}$ avec L corps, est une algèbre de Ore, ce qui veut dire qu'on peut la plonger de façon naturelle dans son algèbre (gauche) de division des quotients. Si L (comme $\mathbb{F}_{q^s}$) est un corps parfait, elle peut être plongée dans son algèbre de division droite des quotients aussi, et les deux structures à éléments inversibles sont isomorphes de façon canonique. On peut donc utiliser sans ambiguité la notation $\mathbb{F}_{q^s}(\tau)$. On est donc dans la situation suivante dans D :

$$\Phi^{v_p}(k) \subset \Phi^{v_p}(k)(F) \subset \mathbb{F}_{q^s}(\tau).$$

On remarque, alors, comment τ est une place divisant F dans cette extension. Comme P_E est la seule place zéro de F dans E, il s'ensuit que $\tau|P_E$. D'un autre coté, $\Phi(p(T)) \equiv 0(\tau)$, ce qui veut dire que $\tau|p(T)$ dans l'extension totale. Par restriction on a finalement que :

$$P_E|p(T).$$

Se souvenant du fait que F est entier sur A, on peut établir une relation de la forme suivante :

$$F^n + \Phi^{v_p}_{a_{n-1}} F^{n-1} + ... + \Phi^{v_p}_{a_0} = 0;$$

$a_0, ..., a_{n-1} \in A$. On a donc que $a_0 = N_{E/k}(F)$. Le point 1 du Théorème 1.4.9 nous dit d'ailleurs que l'idéal principal (F) dans $\mathcal{O}_E$ est de la forme :

$$(F) = P_E^n.$$

L'indice n vient du point 4 du Théorème 1.4.9, sachant que :

$$\sum_{w|(F)} w(F) + w_{\infty_E}(F) = 0.$$

Comme :

$$(F) \cap A = P_E^n \cap A \supset (P_E \cap A)^n = (p(T))^n;$$

et :

$$(F) \cap A = P_E^n \cap A \subset P_E \cap A = (p(T));$$

il s'ensuit que :

$$(p(T))^n \subset (F) \cap A \subset (p(T));$$

ce qui veut dire qu'il existe un nombre naturel $\beta \leq n$ tel que :

$$(F) \cap A = (p(T))^\beta.$$

La relation polynomiale en F montre comment $(F) \supset a_0\mathcal{O}_E$, ce qui implique que $p(T)^\beta|a_0$ dans A. □

Si L est un corps et Φ et Ψ sont deux modules de Drinfeld à caractéristique quelconque, définis sur L, de même degré, et $w \neq \mathrm{char}(L)$ une place de A, on a (voir [Goss], Proposition 4.12.11) un plongement naturel :

$$Hom_L(\Phi, \Psi) \otimes_A A_w \hookrightarrow Hom_{A_w}(T_w(\Phi), T_w(\Psi)).$$

Si $L = \mathbb{F}_{q^s}$ et $G := G(\overline{\mathbb{F}_{q^s}}/\mathbb{F}_{q^s})$, les deux modules de Tate deviennent des $A_w[G]-$modules, et on a le résultat suivant ([Goss], Théorème 4.12.12) :

Théorème 1.4.11. *1. Sous les hypothèses précédentes, où $p := char(\Phi^{v_p}) = char(\Psi^{v_p})$:*

$$Hom_{\mathbb{F}_{q^s}}(\Phi^{v_p}, \Psi^{v_p}) \otimes_A A_w \simeq Hom_{A_w[G]}(T_w(\Phi^{v_p}), T_w(\Psi^{v_p})).$$

2. Si $m(X) \in A[X]$ est le polynôme minimal de F sur $\Phi^{v_p}(A)$ et $f(X) \in A_w[X]$ son polynôme caractéristique en tant qu'endomorphisme agissant sur $T_w(\Phi^{v_p})$:

$$f(X) = m(X)^t.$$

3. Deux modules de Drinfeld Φ et Ψ sur $\mathbb{F}_{q^s}$ sont isogènes si et seulement si $m_\Phi = m_\Psi$

Pour la preuve, voir la référence. On remarque juste qu'étant donné le premier point, les deux autres suivent facilement. En effet, si λ est valeur propre de F agissant sur $T_w(\Phi^{v_p})$, elle doit forcément annuler le même polynôme minimal $m(X)$ à coefficients dans une algèbre d'operateurs sur $T_w(\Phi^{v_p})$ par le premier point [12]. Sachant que $w \neq p(T)$ implique $V_w(\Phi^{v_p}) \simeq k_w^d$ et que $d = nt$, on a le deuxième point. De la même façon, on notera que :

$$V_w(\Phi^{v_p}) \simeq (k_w[X]/m(X))^t.$$

Si donc, Φ et Ψ modules de Drinfeld sur $\mathbb{F}_{q^s}$ sont isogènes, l'isomorphisme :

$$Hom_{\mathbb{F}_{q^s}}(\Phi, \Psi) \otimes_A k_w \simeq Hom_{k_w[G]}(V_w(\Phi), V_w(\Psi));$$

rend l'isogénie $P(\tau)$ entre les deux modules de Drinfeld un isomorphisme d'espace vectoriels :

$$P_* : (k_w[X]/m_\Phi(X))^{t_\Phi} \simeq (k_w[X]/m_\Psi(X))^{t_\Psi};$$

ce qui donne $t_\Phi = t_\Psi$ et $m_\Phi(X) = m_\Psi(X)$.

En particulier, on a un plongement naturel des classes d'isogénie de modules de Drinfeld de degré d définis sur $\mathbb{F}_{q^s}$ et les classes de $G(\overline{k}/k)-$conjugaison des nombres de Weil de rang d pour l'$A-$corps $\mathbb{F}_{q^s}$ ou, de façon équivalente, les polynômes minimaux $m(X)$ associés à char$(\mathbb{F}_{q^s})$ [13] (voir [Goss], définition 4.12.14). Ce plongement est en effet (voir [Goss], Theorem 4.12.15) une bijection.

On énonce, finalement, le critère dont on va se servir pour repérer les premiers à réduction supersingulière de Φ, parmi ceux de bonne réduction. Voir [Goss], Proposition 4.12.17 pour l'énoncé complet.

Théorème 1.4.12. *Soit Φ^{v_p} module de Drinfeld de rang d et de caractéristique $p(T)$ réduction modulo $p(T)$ du module de Drinfeld Φ à caractéristique 0 défini sur $\mathcal{F}$. Les situations suivantes sont alors équivalentes :*

12. Si λ est valeur propre de $F \in End_{A_w[G]}(T_w(\Phi^{v_p}))$, il existe $x \in T_w(\Phi^{v_p}) \setminus \{0\}$ tel que $Fx = \lambda x$. Alors, $F^2x = F(Fx) = F\lambda x$. Comme, par le premier point, $\lambda \in End_{\mathbb{F}_{q^s}}(\Phi^{v_p})$, on a que $F\lambda = \lambda F$, ce qui implique que $F^h x = \lambda^h x$ pour tout $h \geq 0$. On a donc que $m(\lambda)x = m(F)x = 0$ et, puisque $T_w(\Phi^{v_p})$ est un anneau intègre, que $m(\lambda) = 0$.

13. On remarque qu'étant donné un premier $p(T)$ dans A, l'automorphisme F dans $End_{\mathbb{F}_{q^s}}(\Phi^{v_p})$ est un élément tout à fait différent de son interprétation dans $End_{\mathbb{F}_{q^s}}(\Psi^{v_p})$, pouvant même avoir un degré différent sur A dans chaque situation.

1. *Il existe une extension finie $\mathbb{F}_{q^{\alpha s}}$ de $\mathbb{F}_{q^s}$ telle que :*

$$\dim_k(End_{\mathbb{F}_{q^{\alpha s}}}(\Phi^{v_p}) \otimes_A k) = d^2.$$

2. *Il existe une puissance F^α de F telle que $F^\alpha \in A$.*
3. *$p(T)$ est un premier à réduction supersingulière de Φ.*
4. *P_E est la seule place dans $\mathcal{O}_E$ divisant $(p(T))$.*

Démonstration. L'équivalence entre les points 1 et 2 suit du fait que si F est le nombre de Weil de rang d associé à $\mathbb{F}_{q^s}$, alors F^α est le nombre de Weil associé à $\mathbb{F}_{q^{\alpha s}}$. On se place donc dans la classe d'isogénie associé au nouveau nombre de Weil. Le point 2 du Théorème 1.4.11 implique en effet que $f_{F^\alpha} = m^t_{F^\alpha}$. Sachant (voir [Goss], Lemma 4.12.7) que $\dim_{k(F^\alpha)}(End_{\mathbb{F}_{q^{\alpha s}}}(\Phi^{v_p}) \otimes_A k) = t^2$ et donc que $\dim_k(End_{\mathbb{F}_{q^{\alpha s}}}(\Phi^{v_p}) \otimes_A k) = t^2 n = dt$ ($d = nt$ pour le point 3 du Théorème 1.4.9), il s'ensuit que le point 1 équivaut à dire que $d = t$, donc que $k(F^\alpha) = k$.

Supposons le point 2 vérifié. On a donc $F^\alpha = a \in A$ pour $\alpha \in \mathbb{N} \setminus \{0\}$ opportun. Mais $(F^\alpha) \cap A = ((F) \cap A)^\alpha$ comme $F^\alpha \in A$. Donc, $F^\alpha = p(T)^{\alpha\beta}$. Par conséquent :

$$\Phi^{v_p}[p(T)] \subset \Phi^{v_p}[p(T)^{\alpha\beta}] = 0;$$

ce qui veut dire que $p(T)$ est premier à réduction supersingulière de Φ. Si, par contre, on suppose le point 3 vérifié, $\Phi^{v_p}(p(T)) = cF^\alpha$ pour $c \in \mathbb{F}^*_{q^s}$ et $\alpha \in \mathbb{N}\setminus\{0\}$ opportun. Donc :

$$\Phi^{v_p}(p(T)^{q-1}) = F^{(q-1)\alpha};$$

ce qui implique le point 2.

L'équivalence entre les points 3 et 4 peut être montrée de cette façon : $p(T)$ est premier à réduction supersingulière de Φ si et seulement si $T_p(\Phi^{v_p}) = 0$; mais :

$$T_p(\Phi^{v_p}) = 0 \Longleftrightarrow T_{w_E}(\widetilde{\Phi^{v_p}}) = 0 \ \ \forall w_E | p(T) \ \texttt{dans} \ E/k.$$

Mais la seule place dans $\mathcal{O}_E$ divisant F est P_E, et on a que :

$$V_{P_E}(\widetilde{\Phi^{v_p}}) = 0;$$

alors que :

$$V_w(\widetilde{\Phi^{v_p}}) \simeq E^t_w \ \ \forall w \neq P_E, \infty_E \ \texttt{dans} \ E/k;$$

pour le point 2 du Théorème 1.4.9. S'il y avait donc une place $w_E \neq P_E$ dans E/k telle que $w_E|p(T)$ (qui sera donc $\neq \infty_E$ parce-que $p \neq \infty$), $V_{w_E}(\widetilde{\Phi^{v_p}}) \neq 0$, ce qui implique alors que $T_{w_E}(\Phi^{v_p}) \neq 0$, en contradiction avec l'hypothèse de réduction supersingulière en $p(T)$ de Φ. □

La méthode par laquelle on va estimer la cardinalité de l'ensemble des premiers de A à réduction supersingulière de Φ en fonction de leur degré en T est le **Théorème effectif de la Densité de Chebotarev**, relatif aux corps de fonctions (voir [FJ], Proposition 6.4.8) :

Théorème 1.4.13. *Soit L/K une extension finie et de Galois d'un corps de fonctions K sur $\mathbb{F}_q$. Soit $\mathbb{F}_{q^\eta}$ la clôture algébrique de $\mathbb{F}_q$ dans L. Soit $\mu := [L : K\mathbb{F}_{q^\eta}]$, avec $\eta = [K\mathbb{F}_{q^\eta} : K]$. Soit $P_N(K) := \{p(T) \in Spec\ \mathcal{O}_K, \deg_T(p(T)) =$*

$N\}$, où $\mathcal{O}_K$ est l'anneau des $k-$entiers de K. De façon analogue on définit $\mathcal{O}_L$ dans L. Soit donc $P \in Spec\, \mathcal{O}_L$ tel que $P|p(T)$. A un nombre fini d'éléments près on peut supposer que tout $l \in P_N(K)$ soit non ramifié dans $\mathcal{O}_L$. La réduction modulo $p(T)$ induit alors l'isomorphisme :

$$D(P|p(T)) \simeq G(L_P/K_p) \simeq \mathbb{Z}/f_p\mathbb{Z} \simeq < \sigma_p >;$$

où f_p indique le degré d'inertie de $p(T)$ dans $\mathcal{O}_L$. On indique par :

$$\left(\frac{L/K}{p}\right);$$

la classe de conjugaison du générateur σ_p de $D(P|p(T))$ dans $G(L/K)$. Soit $\mathscr{C}$ une classe de conjugaison dans $G(L/K)$. On définit, alors :

$$C_N(L/K, \mathscr{C}) := \{p(T) \in P_N(K), \left(\frac{L/K}{p}\right) = \mathscr{C}\}.$$

Soit, donc, $a \in \mathbb{N}$ tel que :

$$\sigma|_{\mathbb{F}_{q^\eta}} = \tau^a|_{\mathbb{F}_{q^\eta}};$$

pour tout $\sigma \in \mathscr{C}$.

1. *Si $N \neq a \ \ (\eta)$, alors $C_N(L/K, \mathscr{C}) = \emptyset$.*
2. *Si $N \equiv a \ \ (\eta)$, alors $|C_N(L/K, \mathscr{C})| \sim_{N \to +\infty} \frac{|\mathscr{C}|q^N}{N\mu}$.*

On voudrait utiliser ce Théorème pour calculer le nombre de premiers $p(T) \in S(A)$ de degré $\deg_T(p(T))$ en T fixé, à réduction supersingulière de Φ, en les voyant, par le critère qu'on a donné avec le Théorème 1.4.12, comme ceux qui, dans une extension finie et de Galois de k contenant E, se décomposent dans une seule place. Donc, tels que leur σ_p correspondant induit une classe de conjugaison triviale dans cette extension.

Tout ça n'est cependant pas utilisable d'une façon directe. En effet, à chaque $p(T) \in S(A)$ correspond non seulement un nombre de Weil $F = F_p$ (et, donc, une extension $E = E_p/k$ dans D), mais en effet toute l'algèbre ambiante $D = D_p$ dans laquelle on voudrait faire les calculs. Mais, comme on l'a déjà remarqué, fixé Φ, pour chaque $p(T) \in S(A)$, l'algèbre D_p associée est complètement différente des autres (par exemple, comme on disait avant, l'extension E_p/k dans D_p peut même avoir un degré différent en fonction de $p(T)$). On ne dispose donc pas d'un L "'global"' contenant k ainsi que tous les premiers $p(T) \in S(A)$.

On notera à partir d'ici, étant choisi un premier $p(T) \in S(A)$ de bonne réduction de Φ, $F = F_p$ le nombre de Weil associé à Φ^{v_p}, $E = E_p = k(F_p)$ et $D = D_p = End_{\mathbb{F}_{q^s}}(\Phi^{v_p}) \otimes_A k$ pour bien souligner que chacun de ces objets est dépendant du choix de $p(T)$.

Avant de commencer nous rappelons une propriété d'Algèbre Commutative.

Proposition 1.4.14. *Soit B/A extension entière finie avec B domaine d'intégrité. Alors :*

$$K = B \otimes_A k \Longleftrightarrow K = Frac(B).$$

Démonstration. Dans les deux cas B est un $A-$ordre dans K, puisque B/A est une extension entière finie. Elle contient donc une $k-$base de K. L'homomorphisme (injectif comme B est domaine d'intégrité) d'algèbres :

$$B \otimes_A k \hookrightarrow Frac(B)$$

$$b \otimes_A x \mapsto bx;$$

induit le plongement $B \otimes_A k \subset \mathrm{Frac}(B)$. L'égalité des $k-$dimensions des deux $k-$espaces vectoriels induit l'égalité $B \otimes_A k = \mathrm{Frac}(B)$. □

Cette propriété nous montre comment $End_{\mathcal{F}}(\Phi) \otimes_A k$ est en effet un corps. L'hypothèse d'être un domaine d'intégrité est essentielle : par exemple A^2, bien qu'extension entière de A, ne respecte pas la propriété : $A^2 \otimes_A k = k^2$ n'est pas un corps. $End_{\mathcal{F}}(\Phi)$ est au contraire un domaine d'intégrité de façon évidente, étant contenu dans l'algèbre de division $\mathcal{F}\{\tau\}$. Le Lemme 1.4.3 nous montrait seulement un isomorphisme de $A-$modules entre $End_{\mathcal{F}}(\Phi)$ et $A^{\rho(\Phi)}$, mais pas du tout un isomorphisme d'anneaux, raison pour laquelle $End_{\mathcal{F}}(\Phi)$ est domaine d'intégrité et $A^{\rho(\Phi)}$ ne l'est pas.

On remarquera également que l'extension finie $L := End_{\mathcal{F}}(\Phi) \otimes_A k/k$ est normale : si $\sigma \in \mathcal{I}(L/k)$ (ensemble des $k-$isomorphismes de L dans $\overline{L}$), le plongement naturel de k dans L induit par Φ est tel que si $P(\tau) \in End_{\mathcal{F}}(\Phi)$, pour tout $a \in A$ on aura que $\sigma(\Phi_a P(\tau)) = \sigma(P(\tau)\Phi_a) = \sigma(P(\tau))\Phi_a = \Phi_a \sigma(P(\tau))$, ce qui montre la propriété voulue. L'extension L/k n'est toutefois a priori pas toujours séparable. On notera cependant qu'elle peut se décomposer sous la forme $L/k'/k$, où L/k' est séparable et k'/k purement inséparable. L'extension k'/k est normale et a la propriété que $k' = \mathrm{Frac}(A')$, avec $A' = \mathbb{F}_q[T^{1/e}]$, e indice de ramification de l'extension, degré de k' sur k et puissance de $p(T)$, ce qui induit une bijection :

$$S(A) \longleftrightarrow S(A)'$$

$$p(T) \longleftrightarrow p(T)^{1/e}.$$

Au nombre fini près des premiers de A qui se ramifient dans L, le critère du Théorème 1.4.12 nous permet alors d'identifier les premiers à réduction supersingulière de Φ (ceux qui gardent toujours un seul premier les divisant dans l'extension $L/E_p/k$) avec les premiers totalement inertes dans l'extension L/k'. Sans perte de généralité on supposera donc l'extension L/k séparable et donc de Galois. Dans la formule finale qu'on obtient avec le Théorème 1.4.13 on aura $[L : k']$ au lieu de d. S'agissant toutefois d'une différence qui ne fait qu'améliorer les estimations cherchées on peut également oublier ce passage sans rien perdre.

Nous remarquons que dans le cas où $\mathbb{D}$ est tel que l'extension L/k est regulière, donc que $\eta = 1$, on a que $\mathbb{D}$ est $\mathrm{RV}_1(r, c_1)^*$, ce qui est exactement la condition $\mathrm{RV}(r, c_1)^*$.

Théorème 1.4.15. *Si un module de Drinfeld ($\mathbb{D}, \Phi$) à caractéristique* 0 *et coefficients dans $\mathcal{F}$ extension finie de k dans $\overline{k}$ a un rang d qui est* 1 *ou un nombre premier et est de type CM, alors il est de type $RV_\eta(1, 1/2d)^*$, où $\eta \in \mathbb{N} \setminus \{0\}$ est tel que $\mathbb{F}_{q^\eta}$ est la clôture algébrique de $\mathbb{F}_q$ dans $End_{\mathcal{F}}(\Phi) \otimes_A k$.*

Démonstration. On sait que tout corps maximal dans D_p, pour tout $p(T) \in S(A)$, contient toujours E_p (nous rappelons que, pour [Goss], Theorem 4.12.7, D_p est centrale sur E_p), et qu'il a degré d sur k. L'extension de Galois de k :

$$End_{\mathcal{F}}(\Phi) \otimes_A k;$$

a un degré d par l'hypothèse CM et coïncidera par conséquent, en la plongeant dans D_p à travers $\widetilde{\Phi^{v_p}}$, avec un corps maximal de D_p (si ce n'était pas le cas elle serait contenue strictement dans un corps maximal, qui devrait donc avoir dimension sur k supérieure à d, en contradiction avec le Théorème 1.4.9, point 3). quelque soit $p(T) \in S(A)$ cette extension contiendra alors toujours E_p. Ce qui veut dire que $F_p \in End_{\mathcal{F}}(\Phi)$, à isogénie près, pour tout $p(T) \in S(A)$. En effet, $End_{\mathcal{F}}(\Phi)$ est un ordre dans $End_{\mathcal{F}}(\Phi) \otimes_A k$ et, par le Lemme 1.4.5, Φ est isogène à un module de Drinfeld de type CM par rapport à l'anneau des entiers $\widetilde{O}$ dans $End_{\mathcal{F}}(\Phi) \otimes_A k$. Comme $F_p \in \widetilde{O}$, on voit, à isogénie près, F_p comme un élément dans $End_{\mathcal{F}}(\Phi)$. L'algèbre de division $A\{F_p\} \otimes_A k$, qu'on obtient en plongeant F_p dans $\mathcal{F}\{\tau\}$ par $\widetilde{\Phi}$, est donc encore un corps $E_p = k(F_p)$, contenu dans $End_{\mathcal{F}}(\Phi) \otimes_A k$, qu'on identifie à travers l'isomorphisme induit par $\widetilde{\Phi^{v_p}}$ avec l'ancien E_p contenu dans $End_{\mathbb{F}_{q^s}}(\Phi^{v_p}) \otimes_A k$ et précédemment décrit.

On applique donc le Théorème 1.4.13 au cas où $L = End_{\mathcal{F}}(\Phi) \otimes_A k$ et $K = k$, sachant que les premiers à réduction supersingulière de Φ contiendrons, au nombre fini des premiers ramifiés près, ceux qui sont totalement inertes dans l'extension de Galois $End_{\mathcal{F}}(\Phi) \otimes_A k$ de k. Les premiers respectants une telle propriété sont exactement ceux dont le groupe de décomposition (cyclique suite à la condition de ces premiers de ne pas se ramifier dans L), est en effet $G(L/k)$, dont on convient d'appeler σ son générateur[14] ; autrement dit, ils sont exactement les $p(T) \in S(A)$ tels que $\left(\frac{L/k}{p}\right) = \{\sigma\}$, soit, tels que $\sigma_p = \sigma$. Comme $K = k$, on est, suivant les mêmes notations du Théorème 1.4.13, dans cette situation :

$$k = \mathbb{F}_q(T) \overset{\eta}{\text{———}} \mathbb{F}_{q^\eta}(T) \overset{\mu}{\text{———}} L \simeq \mathbb{F}_{q^\eta}(T^{1/\mu}) \ ;$$

avec L/k extension finie et de Galois cyclique de degré $d = \eta\mu$, ce qui implique $G(L/\mathbb{F}_{q^\eta}(T)) \simeq \mathbb{Z}/\mu\mathbb{Z}$. La cyclicité des extensions implique alors nécessairement que la restriction à $\mathbb{F}_{q^\eta}$ du générateur σ du groupe cyclique $G(L/k) \simeq \mathbb{Z}/d\mathbb{Z}$ soit générateur du sous-groupe cyclique $G(L/\mathbb{F}_{q^\eta}(T)) \simeq \mathbb{Z}/\mu\mathbb{Z}$. L'indice a tel que $\mathrm{res}_{\mathbb{F}_{q^\eta}}\tau^a = \mathrm{res}_{\mathbb{F}_{q^\eta}}\sigma$ est alors toujours 1 (dans le cas où $\eta = 1$ c'est plus naturel de dire que $a = 0$, mais comme tout nombre naturel est en même temps congru à 0 et à 1 modulo 1, ça ne fait aucune différence de choisir $a = 1$ toujours). Si $L/\mathbb{F}_q$ est une extension régulière, ce qui veut dire que $\eta = 1$, la condition 2 du Théorème 1.4.13 est en effet la seule à être respectée par tout $N \in \mathbb{N}$. Par conséquent :

$$L \simeq \mathbb{F}_q(T^{1/d}) \Longrightarrow \ |C_N(L/k, \{\sigma\})| \sim_{N \to +\infty} \frac{q^N}{dN}.$$

Si par contre $\eta > 1$ on aura que :

$$N \neq 1 \ \ (\eta) \Longrightarrow C_N(L/k, \{\sigma\}) = \emptyset;$$

14. Comme $G(L/k)$ a d éléments et qu'on suppose d premier ou égal à 1, il respecte la condition de cyclicité admettant ainsi l'existence effective des premiers totalement inertes dans L/k, qui ne seront donc pas un ensemble vide, justement comme conséquence du Théorème 1.4.13.

$$N \equiv 1 \ \ (\eta) \Longrightarrow |C_N(L/k, \{\sigma\})| \sim_{N\to+\infty} \frac{q^N}{\mu N}.$$

Le nombre des éléments $p(T) \in S(A)$ totalement inertes dans $\mathcal{O}_L$ et de degré N est alors celui de tels éléments $p(T)$ tels que $N \equiv 1 \ \ (\eta)$. Pour des tels N nous obtenons alors que :

$$|C_N(L/k, \{\sigma\})| \geq \frac{q^N}{2Nd};$$

pour tout $N > N(\Phi)$ tel que $N \equiv 1 \bmod (\eta)$, où $N(\Phi)$ est un nombre naturel assez grand.

□

Pour comparer avec les énoncés du type Lang-trotter qu'on trouve dans C. David ([Dav]), nous donnons maintenant un énoncé où on compte tous les premiers à réduction supersingulière de degré inférieur à un paramètre donné. Nous rappelons d'abord la propriété suivante.

Soit $\{U_i\}_{i\in\mathbb{N}\setminus\{0\}}$ une suite de nombres réels > 0. Soit $R > 1$ un nombre réel. Il est alors possible de montrer que, pour tout $n \in \mathbb{N} \setminus \{0\}$:

$$U_{i+1}/U_i \sim R \Longrightarrow \sum_{i=1}^{n} U_i \sim \frac{R}{R-1} U_n.$$

Le Théorème 1.4.15 nous dit qu'il existe un nombre $N(\Phi) \in \mathbb{N}\setminus\{0\}$ (qui dépend du choix de Φ) assez grand afin que pour tout $N \in \mathbb{N}$ tel que $N \geq N(\Phi)$ et $N \equiv 1 \bmod(\eta)$, on ait $|C_N(L/k, \{\sigma_p\})| \geq \frac{q^N}{2N\mu}$. En appelant $N = N(\Phi) + n\eta$:

$$U_i := \frac{q^{N(\Phi)+(i-1)\eta}}{(N(\Phi) + (i-1)\eta)\mu};$$

on remarquera que :

$$U_{i+1}/U_i \sim q^\eta.$$

En appelant donc $R := q^\eta$ on aura que :

$$\sum_{i=1}^{N} |C_i(L/k, \{\sigma_p\})| \geq \sum_{i=N(\Phi)}^{N-n\eta} U_i \sim \frac{q^\eta}{q^\eta - 1} \frac{q^N}{N\mu}. \tag{1.63}$$

Corollaire 1.4.16. *Nous nous plaçons à nouveau sous les mêmes hypothèses du Théorème 1.4.15. Le nombre des premiers $p(T) \in S(A)$ à réduction supersingulière pour le module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ de rang d et tel qu'il est supposé dans le Théorème 1.4.15, de degré $\deg_T(p(T)) \leq N$, pour tout $N \geq N(\Phi)$, où $N(\Phi)$ est toujours celui qu'on décrit dans la Définition 1.1.4, est au moins $q^N/2dN$.*

Démonstration. On considère toujours l'extension de Galois L/k, de degré d, où $L = End_{\mathcal{F}}(\Phi) \otimes_A k$. Le nombre des éléments $p(T) \in S(A)$ tels que $\deg_T(p(T)) \leq N$, totalement inertes dans $\mathcal{O}_L$, est, suite à (1.63) :

$$\sum_{i=1}^{N} |C_i(L/k, \{\sigma\})| \geq \sum_{i=0}^{n} |C_{N(\Phi)+i\eta}(L/k, \{\sigma\})| \geq \frac{q^\eta}{2(q^\eta - 1)} \frac{q^N}{N\mu};$$

pour tout $N \in \mathbb{N}$ tel que $N \geq N(\Phi)$ et $N \equiv N(\Phi) \bmod(\eta)$, où $N(\Phi)$ est un nombre naturel assez grand (et congru à 1 modulo η) afin que pour tout $M > N(\Phi)$ l'ensemble $C_M(L/k, \{\sigma\})$ respecte la condition 2 du Théorème 1.4.13, et $n := (N - N(\Phi))/\eta$. L'inégalité :

$$\frac{q^\eta}{q^\eta - 1} \frac{q^N}{N\mu} \geq \frac{q^N}{Nd};$$

nous donne alors l'énoncé.

$\square$

Chapitre 2

Points de torsion et variétés

Dans ce chapitre nous proposons une stratégie d'attaque à la conjecture de Manin-Mumford dans le cas des $T-$modules, nous basant sur la méthode présentée par J. Pila et U. Zannier dans [PZ]. Dans un premier paragraphe nous donnerons toutes les définitions des objets traités ainsi que les propriétés dont la connaissance est nécessaire pour comprendre nos objectifs. Nous montrerons en particulier une version du Théorème de la Fonction Implicite pour des ensembles analytiques munis d'une topologie non-archimédienne. Nous présenterons donc dans un deuxième paragraphe les origines de la Conjecture de Manin-Mumford formulée dans le cadre des variétés abéliennes et la façon dont nous allons l'adapter pour aboutir à une conjecture raisonnable dans le cadre des $T-$modules. Dans le troisième paragraphe nous présentons un Théorème pour majorer le nombre de points de torsion d'un $T-$module dans une variété, travail analogue à celui de J.Pila et J. Wilkie [PW], développé à partir de celui de E. Bombieri et J. Pila [BP], sur lequel la stratégie de J. Pila et U. Zannier dans [PZ] est fondée. Dans le quatrième et dernier paragraphe nous tracerons un chemin qui pourrait permettre de prouver la conjecture en exposant les difficultés principales que la structure géométrique non-archimédienne des $T-$modules présente par rapport à celle classique sur les variétés abéliennes.

2.1 Préliminaires

L'objet de notre étude est un problème géométrique sur les $T-$modules. Ces derniers sont une extension naturelle des modules de Drinfeld en dimension ≥ 1. Nous prendrons la définition suivante qui prend son origine dans le texte de G. Anderson ([A]).

On convient de noter $A := \mathbb{F}_q[T]$, où q est une puissance finie du nombre premier p, $k := Frac(A)$ et $\mathcal{C} := (\overline{k_\infty})_\infty$, où ∞ est la place correspondant à $1/T$ dans A. Si K est un corps et n, m deux entiers naturels pas nuls, la notation $K^{n,m}$ indiquera aussi l'anneau des matrices définies sur K, à n lignes et m colonnes. Nous rappelons que τ indique l'automorphisme de Frobenius élévation à la puissance $q-$ième.

Définition 2.1.1. *Un $T-$module $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ de degré $\widetilde{d}$ et dimension m défini sur un corps $\mathcal{F} \subset \overline{k}$ est le groupe algébrique $\mathbb{G}_a^m$, défini sur $\mathcal{F}$, qui a une* *structure de $A-$module donnée par l'homomorphisme de $\mathbb{F}_q-$algèbres :*

$$\Phi : A \to \mathcal{F}^{n,n}\{\tau\}$$

$$T \mapsto \sum_{i=0}^{\widetilde{d}} a_i(T)\tau^i;$$

*où a_0 (la **différentielle** de $\Phi(T)$) est sous la forme :*

$$a_0 = TI_m + N;$$

où N est une matrice nilpotente, et $a_{\widetilde{d}} \neq 0$. Ce qui montre d'ailleurs que Φ est injectif, tout comme dans le cas d'un module de Drinfeld (qui n'est qu'un $T-$module de dimension 1).

Définition 2.1.2. *L'ensemble des points de torsion dans $\mathcal{A}$ est :*

$$\mathcal{A}_{tors.} := \{\overline{x} \in \mathcal{A}, \exists a(T) \in A \setminus \{0\}, \Phi(a)(\overline{x}) = \overline{0}\}.$$

Définition 2.1.3. *Un sous-$T-$module $\mathcal{B}$ d'un $T-$module $\mathcal{A}$ est un sous-groupe algébrique connexe de $(\mathcal{A}, +)$ tel que $\Phi(T)(\mathcal{B}) \subset \mathcal{B}$.*

Remarque 2.1.4. *On indiquera dorénavant par **dimension** d'un sous-$T-$module, sa dimension en tant que variété algébrique. On remarque qu'un sous-$T-$module $\mathcal{B} < \mathcal{A}$ non trivial (donc, $\mathcal{B} \neq \mathcal{A}, 0$) a une dimension strictement inférieure à celle de $\mathcal{A}$. Les sous-$T-$modules d'un $T-$module ne sont donc pas forcément des $T-$modules (bien qu'habituellement ce sont des sous-groupes algébriques isomorphes à des puissances de $\mathbb{G}_a$, voir par exemple [T] pour les sous-$T-$modules des puissances d'un module de Drinfeld) mais cette terminologie fréquente est suffisante pour notre propos.*

Suite à un résultat de I. Barsotti, voir [Ba], Theorem 3.3, nous indiquons ici pourquoi tout sous-$T-$module de dimension d d'un $T-$module $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ est isomorphe en tant que groupe algébrique, s'il est absolumment irréductible dans $\mathcal{C}$, à $\mathbb{G}_a^d$. Il est en effet possible de montrer qu'un tel groupe algébrique ne peut être que le lieu des zéros d'un nombre fini de polynômes additifs, ce qui le rend toujours une variété algébrique régulière (voir Théorème 2.1.36). Comme les hypothèses du Théorème indiqué dans la référence sont respectées, il s'ensuit qu'un tel groupe algébrique est isomorphe au produit direct $\mathbb{G}_a^t \times \mathbb{G}_m^s$, pour des t et s opportuns. Puisqu'il est facile de montrer qu'aucune puissance de $\mathbb{G}_m$ ne peut pas être isomorphe à un sous-groupe de $\mathbb{G}_a^m$ nous avons que $t = d$ et $s = 0$.

Nous donnons maintenant la définition d'un objet très important pour l'étude des $T-$modules, qui a été introduit dans [A].

Définition 2.1.5. *Soit t une indéterminée et soit $\mathcal{F}$ un corps contenant $\mathbb{F}_q$ et t. Soit :*

$$l : A \to \mathcal{F};$$

$$T \mapsto t := l(T)$$

un homomorphisme de $\mathbb{F}_q-$algèbres plongeant A dans $\mathcal{F}$. Etant donné l'automorphisme de Frobenius τ déjà introduit, nous notons :

$$\mathcal{F}[T, \tau] := \mathcal{F} \otimes_{\mathbb{F}_q} A\{\tau\}.$$

Quelque soit un élément générique $h \in \mathcal{F}[T,\tau]$, il s'exprime, pour un certain $N \in \mathbb{N} \setminus \{0\}$, sous la forme suivante :

$$h := \sum_{i=1}^{N} (x_i \otimes_{\mathbb{F}_q} y_i) \in \mathcal{F} \otimes_{\mathbb{F}_q} A\{\tau\};$$

on imposera que :

$$\tau(h) := \sum_{i=1}^{N} (x_i^q \otimes_{\mathbb{F}_q} y_i)\tau.$$

Pour tout $\alpha \in \mathcal{F}$ on aura donc que :

$$T\tau = \tau T;$$

$$T\alpha = \alpha T;$$

$$\tau\alpha = \alpha^q \tau.$$

*Plus précisément, nous remarquons que $\mathcal{F}[T,\tau] = \mathcal{F}\{\tau\}[T]$, anneau de polynômes en T et τ (à coefficients dans $\mathcal{F}$) commutatif en T mais pas en τ. On appelle $T-$**motif** un $\mathcal{F}[T,\tau]-$module à gauche M, libre et de type fini sur $\mathcal{F}\{\tau\}$, tel qu'il existe $n \in \mathbb{N} \setminus \{0\}$ tel que :*

$$(T-t)^n M \subseteq \tau M.$$

Définition 2.1.6. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module défini sur le corps $\mathcal{F} \subset \overline{k}$. On note :*

$$Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a);$$

*le groupe des homomorphismes de groupes $\mathbb{F}_q-$additifs de $\mathcal{A}$ dans $\mathbb{G}_a$ définis sur $\mathcal{F}$. On appelle $Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a)$ le $T-$**motif** associé à $\mathcal{A}$.*

Nous remarquons qu'un tel groupe est bien un $T-$motif. Il est en effet possible de le munir d'une structure de $\mathcal{F} \otimes_{\mathbb{F}_q} A\{\tau\}-$module à gauche de la manière suivante (voir [A] ou [Goss] pour plus de détails).

En appellant :

$$M := Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a);$$

on définit l'action (à gauche) de $\mathcal{F}[T,\tau]$ sur M comme il suit :

$$\forall a \in \mathcal{F}, f \in M; (a, f) \mapsto af;$$

$$\forall f \in M; (T, f) \mapsto f \circ \Phi(T);$$

$$\forall f \in M; (\tau, f) \mapsto \tau \circ f.$$

Il est clair qu'une telle action munit à la fois M d'une structure de $\mathcal{F}[T]-$module et de $\mathcal{F}\{\tau\}-$module.

Comme conséquence d'une telle définition on peut montrer que :

$$Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a) \simeq \mathcal{F}\{\tau\}^m;$$

ce qui respecte la condition d'être un $\mathcal{F}\{\tau\}-$module libre et de type fni, donnée dans la Définition 2.1.5.

Définition 2.1.7. *En appelant $\mathcal{F} \subset \overline{k}$ le corps engendré à partir de k par les composantes des matrices coefficients de $\Phi(T)$, le* ***rang*** *d'un $T-$module $\mathcal{A}$ est le rang sur $\mathcal{F}[T]$ du $\mathcal{F}[T]-$module $Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a)$. On appelle $\mathcal{A}$ un $T-$module* ***abélien*** *si $Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a)$ est de rang fini.*

On peut montrer (voir [Goss], Theorem 5.4.10) que si $\mathcal{A}$ est abélien, $Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a)$ est aussi libre en tant que $\mathcal{F}[T]-$module.

Remarque 2.1.8. *Le foncteur $Hom_{\mathcal{F}}(\cdot, \mathbb{G}_a)$ constitue une anti-équivalence entre la catégorie des $T-$modules abéliens et celle des $T-$motifs libres et de rang fini (voir [Goss], Theorem 5.4.11). Les deux catégories sont abéliennes.*

On peut voir assez facilement qu'en particulier les sous-$T-$modules et les quotients de $T-$modules abéliens sont toujours abéliens. Si on a l'inclusion canonique :

$$i : \mathcal{B} \hookrightarrow \mathcal{A};$$

ça induit le morphisme :

$$i^* : Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a) \to Hom_{\mathcal{F}}(\mathcal{B}, \mathbb{G}_a);$$

de façon naturelle. On sait d'ailleurs que, si $m_{\mathcal{A}} := \dim_{\mathcal{C}}(\mathcal{A})$ et $m_{\mathcal{B}} := \dim_{\mathcal{C}}(\mathcal{B})$, on a $m_{\mathcal{B}} < m_{\mathcal{A}}$ si $\mathcal{B} \neq \mathcal{A}$. Comme $\mathcal{B} \simeq \mathbb{G}_a^{m_{\mathcal{B}}}$ et $\mathcal{A} \simeq \mathbb{G}_a^{m_{\mathcal{A}}}$, on peut voir $Hom_{\mathcal{F}}(\mathcal{B}, \mathbb{G}_a) \subset \mathcal{F}\{\tau\}^{m_{\mathcal{B}}}$ comme agissant sur $\mathbb{G}_a^{m_{\mathcal{A}}}$ en tant qu'élément dans $\mathcal{F}\{\tau\}^{m_{\mathcal{A}}}$ de façon naturelle, l'étendant ainsi à $\mathcal{A}$. Par conséquent, on voit facilement que i^* est surjectif. De la même manière on remarque que le quotient :

$$j : \mathcal{A} \twoheadrightarrow \mathcal{A}/\mathcal{B};$$

induit dans la catégorie duale le morphisme :

$$j^* : Hom_{\mathcal{F}}(\mathcal{A}/\mathcal{B}, \mathbb{G}_a) \to Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a);$$

et que ce dernier est injectif. Comme un $T-$module est abélien si et seulement si son $T-$motif est de type fini sur $\mathcal{F}[T]$ la conclusion suit immédiatement. Se rappelant aussi que si un $T-$module est abélien, alors il est aussi libre, les autres propriétés définissant une catégorie abélienne suivent.

Remarque 2.1.9. *A la différence de ce qui arrive dans le cas des modules de Drinfeld, en dimension supérieure le rang et le degré d'un $T-$module ne sont pas égaux. La situation qu'on va décrire soulignera davantage cette différence.*

En choisissant $\mathcal{A}$ de la forme $(\mathbb{D}_1, \Phi_1) \times ... \times (\mathbb{D}_m, \Phi_m)$, produit de m modules de Drinfeld de rang d_i, $i = 1, ..., m$, $\Phi := \Phi_1 \times ... \times \Phi_m$, on obtient un $T-$module de rang $d = \sum_{i=1}^m d_i$ de **forme diagonale**. Nous remarquons que ceci constitue un exemple où $\widetilde{d} \neq d$, puisque $\widetilde{d} = \max_{i=1,...,m}\{d_i\}$.

Proposition 2.1.10. *Soient $m_1, m_2 \in \mathbb{N} \setminus \{0\}$. Soient $a_0 \in \mathcal{C}^{m_1, m_1}$ et $F \in \mathcal{C}^{m_2, m_1}$. Soient $b_0, b_1, ..., b_s \in \mathcal{C}^{m_2, m_2}$, pour un certain $s \in \mathbb{N} \setminus \{0\}$, telles que :*

$$Fa_0 = b_0F;$$

$$(a_0 - TI_{m_1})^{m_1} = 0;$$

$$(b_0 - TI_{m_2})^{m_2} = 0.$$

Il existe alors unique une fonction $\mathbb{F}_q-$linéaire :

$$\overline{e} : \mathcal{C}^{m_1} \to \mathcal{C}^{m_2};$$

telle que :

$$\overline{e}(\overline{x}) = F\overline{x} + \sum_{i\geq 1} B_i \overline{x}^{q^i};$$

où $B_i \in \mathcal{C}^{m_2,m_1}$ pour tout $i \geq 1$ sont telles que la série converge quelque soit $\overline{x} \in \mathcal{C}^{m_1}$. Une telle fonction respecte l'equation fonctionnelle suivante :

$$\overline{e}(a_0\overline{x}) = \sum_{i=0}^{s} b_i \overline{e}(\overline{x})^{q^i}.$$

Démonstration. Voir [Goss], Proposition 5.9.2. □

Remarque 2.1.11. *Les matrices B_i, $i \geq 0$, coefficients de l'expression explicite de $\overline{e}$ donnée dans la Proposition 2.1.10 ont leur cordonnées dans l'extension finie $\mathcal{F}$ de k engendrée par les cordonnées de chaque matrice $b_0, ..., b_s$.*

Démonstration. Voir [Goss], Lemma 5.9.3. Une telle construction est due à G. Anderson dans son travail [A]. □

Définition 2.1.12. *Un **système de coordonnées** ρ d'un $T-$module abélien $\mathcal{A}$ de dimension m est un isomorphisme de groupes algébriques :*

$$\rho : \mathcal{A} \to \mathbb{G}_a^m;$$

$$\overline{x} \mapsto \begin{pmatrix} \rho_1(\overline{x}) \\ ... \\ \rho_m(\overline{x}) \end{pmatrix};$$

auquel on associe l'isomorphisme de $\mathcal{C}-$espaces vectoriels :

$$\rho_* : Lie(\mathcal{A}) \to \mathbb{G}_a^m;$$

$$\overline{\epsilon} \mapsto \begin{pmatrix} \partial\rho_1(\overline{\epsilon}) \\ ... \\ \partial\rho_m(\overline{\epsilon}) \end{pmatrix};$$

où $\partial\rho_i$ est la différentielle de ρ_i en voyant ce dernier en tant que morphisme $\mathbb{F}_q-$linéaire (voir [Goss], Definition 5.9.4). Un tel isomorphisme montre comment en effet la dimension de $\mathcal{A}$ coïncide avec celle de son algèbre de Lie associée.

Définition 2.1.13. *Soient $\mathcal{A}_1 = (\mathbb{G}_a^{m_1}, \Phi_1)$ et $\mathcal{A}_2 = (\mathbb{G}_a^{m_2}, \Phi_2)$ deux $T-$modules abéliens de dimension, respectivement, m_1 et m_2. Soit f un morphisme de $\mathcal{A}_1$ vers $\mathcal{A}_2$. L'**exponentielle** de f est une application :*

$$\exp_f : Lie(\mathcal{A}_1) \to \mathcal{A}_2;$$

telle que :

1. *Pour tout $\epsilon \in Lie(\mathcal{A}_1)$:*

$$\exp_f(a_0\epsilon) = \Phi_2(T)(\exp_f(\epsilon));$$

où a_0 est le coefficient constant de $\Phi_1(T)$, comme dans la Définition 2.1.1.

2. *Soit $f_* : Lie(\mathcal{A}_1) \to Lie(\mathcal{A}_2)$ le morphisme induit de f à travers la différentielle, de la même manière que dans la définition 2.1.12. Alors :*

$$\exp_{f_*} = f_*;$$

où f_* est le morphisme induit par f sur les algèbres de Lie associées.

3. *Si ρ_1 et ρ_2 sont, respectivement, les systèmes de coordonnées de $\mathcal{A}_1$ et $\mathcal{A}_2$, il existe une fonction entière $\mathbb{F}_q-$linéaire sous la forme $\zeta : \mathcal{C}^{m_1} \to \mathcal{C}^{m_2}$, telle que, si $\epsilon \in Lie(\mathcal{A}_1)$, alors :*

$$\zeta(\rho_{1*}\epsilon) = \rho_2(\exp_f(\epsilon)).$$

Théorème 2.1.14. *Etant donné f un morphisme entre deux $T-$modules $\mathcal{A}_1$ et $\mathcal{A}_2$ comme dans la Définition 2.1.13, il existe unique une fonction exponentielle de f telle qu'elle est décrite dans une telle Définition.*

Démonstration. C'est une conséquence directe de la Proposition 2.1.10. □

Définition 2.1.15. *Soit $\mathcal{A}$ un $T-$module abélien. L'**exponentielle** de $\mathcal{A}$ est le morphisme :*

$$\overline{e} : Lie(\mathcal{A}) \to \mathcal{A};$$

qui est l'exponentielle de l'identité $id_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$.

Nous remarquons que si $\mathcal{B}$ est sous-$T-$module du $T-$module abélien $\mathcal{A}$, l'inclusion canonique :

$$i : \mathcal{B} \hookrightarrow \mathcal{A};$$

induit l'inclusion :

$$\exp_{i_*} : Lie(\mathcal{B}) \hookrightarrow Lie(\mathcal{A}).$$

Il s'agit en effet d'une inclusion comme le plongement naturel $Lie(\mathcal{B}) \subset Lie(\mathcal{A})$, qui suit du fait que $\dim_{\mathcal{C}}(\mathcal{B}) < \dim_{\mathcal{C}}(\mathcal{A})$, respecte les trois propriétés énoncées dans la Définition 2.1.13, ce qui implique par l'unicité que ce plongement est exactement la fonction $\exp_i$.

Supposant $\mathcal{A}$ abélien (voir Définition 2.1.7) on a que, si :

$$\Lambda := Ker(\overline{e});$$

ce noyau est un $A-$réseau dans $Lie(\mathcal{A})$ dont le $A-$rang est inférieur ou égal au rang de $\mathcal{A}$, voir [Goss], Lemma 5.9.12. La fonction exponentielle associée à un $T-$module présente donc des analogies avec l'idée de revêtement entre deux espaces topologiques (un concept qui ne peut pas avoir lieu dans le cadre d'une topologie non-archimédienne, qui est totalement discontinue comme on le soulignera ensuite, ce qui empêche la construction des chemins continus et des faisceaux sur elle). En effet il est possible de montrer qu'une telle fonction est un homéomorphisme local[1]. De la même manière, si $\mathcal{B}$ est sous-$T-$module du $T-$module abélien $\mathcal{A}$, l'unicité de l'exponentielle qu'on lui associe implique que

1. Nous montrerons de façon indirecte une telle propriété au cours de ce chapitre, après avoir introduit la définition de **fonction entière** (voir Définition 2.1.20) nous remarquerons d'abord que la fonction exponentielle est entière (voir Remarque 2.1.11), puis qu'elle est localement inversible avec inverse analytique (voir Théorème 2.1.38 point 1), finalement que toute fonction analytique est continue (voir Lemme 2.3.2).

cette dernière est la restriction à $Lie(\mathcal{B})$ de $\overline{e}$ et, donc, que si $\Lambda_{\mathcal{B}}$ est le réseau associé à $\mathcal{B}$ dans $Lie(\mathcal{B})$ et $\Lambda_{\mathcal{A}}$ celui qu'on associe à $\mathcal{A}$ dans $Lie(\mathcal{A})$, alors :

$$\Lambda_{\mathcal{B}} = Lie(\mathcal{B}) \cap \Lambda_{\mathcal{A}}.$$

Lemme 2.1.16. *Les propriétés suivantes sont équivalentes pour un $T-$module $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ abélien. Nous appelons $\rho(\Lambda_{\mathcal{A}})$ le $A-$rang du réseau associé à $\mathcal{A}$ en tant que noyau de la fonction exponentielle $\overline{e} : Lie(\mathcal{A}) \to \mathcal{A}$. Nous appelons également $\rho(\mathcal{A})$ le rang de $\mathcal{A}$.*

1. *$\rho(\Lambda_{\mathcal{A}}) = \rho(\mathcal{A})$;*
2. *La fonction exponentielle $\overline{e} : Lie(\mathcal{A}) \to \mathcal{A}$ est surjective.*

Démonstration. Voir [Goss], Theorem 5.9.14. □

Définition 2.1.17. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module abélien. S'il respecte les deux conditions équivalentes du Lemme 2.1.16 on dit qu'il est **uniformisable**.*

Remarque 2.1.18. *Si $\mathcal{B}$ est un sous-$T-$module du $T-$module abélien $\mathcal{A}$:*

$$\overline{e}^{-1}(\mathcal{B}) = Lie(\mathcal{B}).$$

Démonstration. Nous remarquons que tout $T-$module est une variété algébrique lisse. Sa dimension coïncide donc avec celle de son espace tangent en n'importe quel point, en tant qu'espace affine sur $\mathcal{C}$. Si ce $T-$module est le sous-$T-$module $\mathcal{B}$ de $\mathcal{A}$, cet espace est canoniquement isomorphe à $Lie(\mathcal{B})$. Comme $\overline{e}$ est définie sur $Lie(\mathcal{A})$, il est clair que $\overline{e}^{-1}(\mathcal{A}) = Lie(\mathcal{A})$. En ce qui concerne $\mathcal{B}$ au contraire, on a seulement que $H := \overline{e}^{-1}(\mathcal{B}) \subset Lie(\mathcal{A})$ est tel que $H \supset Lie(\mathcal{B})$. Suite à la Définition 2.1.12 nous savons que $\mathcal{B} \simeq \mathbb{G}_a^{\dim_{\mathcal{C}}(Lie(\mathcal{B}))}$. D'un autre coté l'exponentielle $\overline{e}$ est un homéomorphisme local par rapport à la même topologie de $\mathcal{A}$ avec $Lie(\mathcal{A})$, ce qui induit par sa restriction à H un homéomorphisme local entre H et $\overline{e}(H) = \mathcal{B}$. Il est donc possible de construire un homéomorphisme local entre H et $Lie(\mathcal{B})$, ce qui implique forcément qu'ils ont la même $\mathcal{C}-$dimension en tant qu'espaces affines et que par conséquent $H = Lie(\mathcal{B})$. Nous remarquons que nous n'avons pas besoin dans cette preuve d'hypothèse sur la surjectivité de $\overline{e}$ ou de sa restriction à $Lie(\mathcal{B})$. □

Remarque 2.1.19. *Les sous-$T-$modules d'un $T-$module abélien et uniformisable sont uniformisables.*

Démonstration. Soit $\mathcal{B}$ sous-$T-$module du $T-$module abélien et uniformisable $\mathcal{A}$. Nous avons déjà remarqué que $\overline{e}^{-1}(\mathcal{B}) = Lie(\mathcal{B})$. Comme $\overline{e}$ est la fonction exponentielle définie sur $Lie(\mathcal{A})$ et non seulement sur $Lie(\mathcal{B})$, si sa restriction à $Lie(\mathcal{B})$ n'est pas surjective, il existe un élément $\overline{x} \in \mathcal{B}$ tel que $\overline{e}^{-1}(\overline{x}) \cap Lie(\mathcal{B}) = \emptyset$, où $\overline{e}^{-1}(\overline{x}) \subset Lie(\mathcal{A})$. Comme $\overline{e}^{-1}(\overline{x}) \subset \overline{e}^{-1}(\mathcal{B}) = Lie(\mathcal{B})$ on a facilement une contradiction. □

2.1.1 Théorème de la Fonction Implicite

Nous donnons ici une version du Théorème de la Fonction Implicite valable pour un corps non-archimédien, version sur laquelle notre travail est fondé.

Comment l'on sait, la preuve de la version classique, ou réelle, de ce Théorème, analysant les zéros de fonctions régulières de la forme :

$$f : \mathbb{R}^n \to \mathbb{R};$$

utilise dans un point essentiel de son développement la relation d'ordre total induite sur $\mathbb{R}$ par la valeur absolue standard. N'ayant pas une telle relation d'ordre sur k_∞, l'analogue naturel de $\mathbb{R}$ dans notre situation, il est nécessaire de re-formuler une version $1/T-$adique du Théorème, et d'en donner une preuve compatible avec la nouvelle structure du corps utilisé.

Définition 2.1.20. *Etant donnés $n, i \in \mathbb{N} \setminus \{0\}$, nous notons :*

$$\Lambda_n(i) := \{(\mu_1, ..., \mu_n) \in \mathbb{N}^n, \sum_{j=1}^{n} \mu_j = i\}.$$

Pour tout $\mu = (\mu_1, ..., \mu_n) \in \mathbb{N}^n$, nous définissons :

$$|\mu| := \sum_{j=1}^{n} \mu_j.$$

Soit K un corps de valuation non-archimédienne complet par rapport à celle-ci et soit $L \subseteq K$ un sous-corps de K. Etant donné $\mu = (\mu_1, ..., \mu_n) \in \Lambda_n(i)$ et un vecteur $\overline{z} = (z_1, ..., z_n) \in K^n$, on définit alors :

$$\overline{z}^\mu = \prod_{j=1}^{n} z_j^{\mu_j}.$$

Soit $U \subset K^n$ un ouvert de K^n par rapport à la topologie induite sur celui-ci par la valeur absolue $1/T-$adique. Une application :

$$f : U \to K;$$

*est $L-$**analytique** si et seulement si on a :*

$$f(\overline{z}) = \sum_{i \geq 0} \sum_{\mu \in \Lambda_n(i)} a_\mu \overline{z}^\mu, \ \ \forall \overline{z} \in U;$$

où $a_\mu \in L$ pour tout $\mu \in \Lambda_n(i)$ et tout $i \geq 0$. En particulier, la série de puissances de $\overline{z}$ formelle qui définit une telle fonction converge sur tout $\overline{z} \in U$ à la valeur $f(\overline{z})$. Soit $\overline{z}_0 \in U(L) = L^n \cap U$. Le changement de variable suivant :

$$\overline{z} \mapsto \overline{z} + \overline{z}_0;$$

induit l'égalité suivante :

$$f(\overline{z}) = \sum_{i \geq 0} \sum_{\mu \in \Lambda_n(i)} a_\mu \overline{z}^\mu = \sum_{i \geq 0} \sum_{\mu \in \Lambda_n(i)} b_\mu (\overline{z} - \overline{z}_0)^\mu;$$

*où les $b_\mu \in L$ sont des coefficients opportuns. Ces coefficients sont appellés les **dérivées divisées** $\frac{\partial^\mu f(\overline{z}_0)}{\partial \overline{z}^\mu}$ de f en $\overline{z}_0$ le long de la direction indiquée par μ.*

On appelle également fonction $L-$analytique sur U tout vecteur de fonctions $L-$analytiques sous la forme suivante :

$$f : U \to K^m;$$

*quelque soit $m \in \mathbb{N} \setminus \{0\}$. Nous disons que f est une fonction $L-$**entière** si $U = K^n$. Une fonction $L-$entière est donc une fonction sous la forme suivante :*

$$f : K^n \to K;$$

$$\overline{z} \mapsto \sum_{i \geq 0} \sum_{\mu \in \Lambda_n(i)} a_\mu \overline{z}^\mu;$$

convergente à $f(\overline{z})$ en tout point $\overline{z} \in K^n$.

Remarque 2.1.21. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module abélien et uniformisable, défini sur le corps $\mathcal{F} \subset \overline{k}$, comme dans la Définition 2.1.1. Nous définissons alors le corps $k_\infty(\Phi) := k_\infty \mathcal{F}$, qui est une extension finie de k_∞. La fonction exponentielle :*

$$\overline{e} : Lie(\mathcal{A}) \to \mathcal{A};$$

qu'on lui associe est alors une fonction $\mathcal{F}-$entière et en particulier $k_\infty(\Phi)$-entière, suite à la Remarque 2.1.11.

On peut remarquer comment la nature non archimédienne de la valuation $1/T-$adique donne lieu au critère suivant de convergence de séries de puissances, plus fort que ceux dont on dispose en Analyse Réelle. Sa preuve est une application mécanique des définitions.

Proposition 2.1.22. *Soit (K, v) corps de valuation non archimédienne. Une série de puissances formelle :*

$$\sum_{i \geq 0} a_i z^i;$$

définie sur K converge sur le disque $B_r(K) := \{x \in K, |x|_v \leq r\}$, pour $r > 0$, si et seulement si :

$$\lim_{i \to +\infty} a_i r^i = 0.$$

En dimension supérieure, on conclut, alors, qu'une série :

$$\sum_{i \geq 0} \sum_{\mu(i) \in \Lambda_n(i)} a_{\mu(i)} \overline{z}^\mu;$$

est convergente dans le polydisque $B_r^n(K)$ si et seulement si :

$$\lim_{i \to +\infty} a_{\mu(i)} r^i = 0;$$

où $\mu(i)$ est multi-indice tel que la somme de ses n composantes est i.

On remarque que cette définition de analyticité est compatible avec celle en dimension 1 qu'on a donné dans le premier chapitre. La construction de la fonction exponentielle qu'on a décrit dans la Proposition 2.1.10 montre que cette fonction est entière en tant que vecteur de fonctions entières.

Nous pouvons donc donner la définition d'un **ensemble analytique**.

Définition 2.1.23. *Soit K un corps complet par rapport à une certaine valuation et soit $L \subseteq K$ un sous-corps de K. Soit $U \subset K^n$ un ouvert de K^n par rapport à la topologie induite sur celui-ci par la valeur absolue $1/T-$adique. Un sous-ensemble $Z \subseteq U$ est un sous-ensemble $L-$**analytique** de U s'il existe un ensemble fini de fonctions $L-$analytiques $\{f_1, ..., f_r\}$ définies sur U et à valeurs dans K, tels que :*

$$Z = \{\overline{z} \in U, f_i(\overline{z}) = 0, \forall i = 1, ..., r\}.$$

*Nous disons que Z est un ensemble $L-$**entier** s'il existe un ensemble fini de fonctions $L-$entières $\{f_1, ..., f_r\}$ définies sur K^n et à valeurs dans K, telles que :*

$$Z = \{\overline{z} \in K^n, f_i(\overline{z}) = 0, \forall i = 1, ..., r\}.$$

Théorème 2.1.24. *Soit K un corps complet contenant k_∞ et contenu dans $\mathcal{C}$. Soit $F : K^n \to K$ une application $K-$analytique sur un certain ouvert de K^n, où $n > 1$. Soit $Z = Z(F)$ le lieu des zéros de F dans K^n. Nous supposons que $Z \neq \emptyset$. Soit $\overline{z}_0 \in Z$ et soit $\overline{z}_0^*$ sa projection sur ses premières $n-1$ composantes. Supposons que :*

$$\frac{\partial F(\overline{z}_0)}{\partial z_n} \neq 0.$$

Il existe, alors, un voisinage ouvert $U_{\overline{z}_0} \subset K^n$ de $\overline{z}_0$, dont on appelle $U^*_{\overline{z}_0} \subset K^{n-1}$ la projection sur les premières $n-1$ composantes (qui contiendra évidemment $\overline{z}_0^*$), et une fonction analytique :

$$f : U^*_{\overline{z}_0} \to K;$$

tels que, pour tout $\overline{z} \in U_{\overline{z}_0}$, en exprimant ce dernier comme :

$$\overline{z} = (\overline{z}^*, z_n) \in K^{n-1} \times K;$$

on ait :

$$z_n = f(\overline{z}^*).$$

Démonstration. Un premier pas dans la preuve consiste à montrer un Théorème de la Fonction Inverse, et donc, de la Fonction Implicite, formel. Nous nous posons dans la situation où $\overline{z}_0 = \overline{0}$ pour simplifier les notations, sans cependant rien perdre en généralité. Il s'ensuit que $F(\overline{0}) = 0$. On exprime, dans le voisinage U de $\overline{0}$, F sous la forme :

$$F(\overline{z}) = \sum_{i \geq 1} \sum_{\mu \in \Lambda_n(i)} a_\mu \overline{z}^\mu.$$

On définit :

$$G \in (K[[z_1, ..., z_n]])^n;$$

qui définit une fonction $K-$analytique :

$$G : K^n \to K^n;$$

telle que :

$$G(\overline{z}) = (\overline{z}^*, F(\overline{z}));$$

où $\overline{z}^*$ est la projection de $\overline{z}$ sur ses premières $n-1$ composantes dans K^{n-1}. Nous cherchons une **fonction inverse** :

$$H : K^n \to K^n;$$

s'annulant en $\overline{0}$ à l'ordre 1, de la même forme que G, telle que :

$$H \circ G = G \circ H = 1.$$

Autrement dit, on demande que, pour tout $\overline{z}$ vecteur formel à n composantes, on ait :

$$(G \circ H)(\overline{u}) = (\overline{u}^*, (F \circ H)(\overline{u})) = \overline{u}.$$

La série formelle avec laquelle H s'exprime est donc de la forme :

$$H(\overline{u}) = (\overline{u}^*, h(\overline{u}));$$

avec :

$$h : K^n \to K;$$

telle que :

$$F(H(\overline{u})) = F(\overline{u}^*, h(\overline{u})) = u_n;$$

et en même temps telle que :

$$h(G(\overline{z})) = h(\overline{z}^*, F(\overline{z})) = z_n.$$

On remarque que :

$$h(G(\overline{0})) = 0;$$

nous donnant l'annulation en $\overline{0}$ de H, comme $G(\overline{0}) = \overline{0}$, puisque $\overline{0}$ est un zéro de F. Il s'ensuit que :

$$F(H(\overline{0})) = 0;$$

également. On exprime, donc, h sous la forme :

$$h(\overline{u}) = \sum_{i\geq 1} \sum_{\eta\in\Lambda_n(i)} b_\eta \overline{u}^\eta.$$

En imposant la condition :

$$F(\overline{u}^*, h(\overline{u})) = u_n;$$

on obtient donc :

$$\sum_{i\geq 1} \sum_{\eta\in\Lambda_n(i)} a_\eta H(\overline{u})^\eta = \sum_{j=1}^{n-1} a_j u_j + a_n h(\overline{u}) + \sum_{i\geq 2} \sum_{\eta\in\Lambda_n(i)} a_\eta (\overline{u}^*, h(\overline{u}))^\eta = u_n.$$

Nous développons le calcul des séries jusqu'à l'ordre 3 pour donner l'idée de la méthode avec laquelle nous donnons les coefficients b_μ de h. Nous avons :

$$F(H(\overline{u})) = \sum_{i=1}^{n-1} a_i u_i + a_n (\sum_{i=1}^{n} b_i u_i + \sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j} u_i u_j + \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} b_{i,j,k} u_i u_j u_k + ...) +$$

$$+\sum_{i=1}^{n-1}\sum_{j=1}^{n-1} a_{i,j}u_iu_j+\sum_{i=1}^{n-1} a_{i,n}u_i(\sum_{i=1}^{n} b_iu_i+\sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}u_iu_j+\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} b_{i,j,k}u_iu_ju_k+...)+$$

$$+a_{n,n}(\sum_{i=1}^{n} b_iu_i+\sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}u_iu_j+\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} b_{i,j,k}u_iu_ju_k+...)^2+\sum_{i=1}^{n-1}\sum_{j=1}^{n-1}\sum_{k=1}^{n-1} a_{i,j,k}u_iu_ju_k+$$

$$+\sum_{i=1}^{n-1}\sum_{j=1}^{n-1} a_{i,j,n}u_iu_j(\sum_{i=1}^{n} b_iu_i + \sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}u_iu_j + \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} b_{i,j,k}u_iu_ju_k + ...)+$$

$$+\sum_{i=1}^{n-1} a_{i,n,n}u_i(\sum_{i=1}^{n} b_iu_i + \sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}u_iu_j + \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} b_{i,j,k}u_iu_ju_k + ...)^2+$$

$$+a_{n,n,n}(\sum_{i=1}^{n} b_iu_i + \sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}u_iu_j + \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} b_{i,j,k}u_iu_ju_k + ...)^3 + ... = u_n.$$

Nous associons maintenant à chaque monôme $\overline{u}^{\mu}$ le coefficient lui correspondant dans l'égalité formelle :

$$F(H(\overline{u})) - u_n = 0.$$

Cette association est la suivante :

u_n	$a_nb_n - 1$	
u_i	$a_nb_i + a_i$	$\forall i = 1, ..., n-1$
u_iu_j	$a_nb_{i,j} + a_{i,j} + a_{i,n}b_j + a_{j,n}b_i + 2a_{n,n}b_ib_j$	$\forall i, j = 1, ..., n-1$
u_iu_n	$a_nb_{i,n} + a_{i,n}b_n + 2a_{n,n}b_ib_n$	$\forall i = 1, ..., n-1$
u_n^2	$a_nb_{n,n} + a_{n,n}b_n^2$	
$u_iu_ju_k$	$a_nb_{i,j,k} + a_{i,n}b_{j,k} + a_{j,n}b_{i,k} + a_{k,n}b_{i,j}+$ $+2a_{n,n}(b_ib_{j,k} + b_jb_{i,k} + b_kb_{i,j}) + a_{i,j,k}+$ $+a_{i,j,n}b_k + a_{i,k,n}b_j + a_{j,k,n}b_i+$ $+2(a_{i,n,n}b_jb_k + a_{j,n,n}b_ib_k + a_{k,n,n}b_ib_j)+$ $+3a_{n,n,n}b_ib_jb_k$	$\forall i, j, k = 1, ..., n-1$
$u_iu_ju_n$	$a_nb_{i,j,n} + a_{i,n}b_{j,n} + a_{j,n}b_{i,n}+$ $+2a_{n,n}(b_ib_{j,n} + b_jb_{i,n} + b_nb_{i,j})+$ $+a_{i,j,n}b_n + 2(a_{i,n,n}b_jb_n + a_{j,n,n}b_ib_n)+$ $+3a_{n,n,n}b_ib_jb_n$	$\forall i, j = 1, ..., n-1$
$u_iu_n^2$	$a_nb_{i,n,n} + 2a_{n,n}b_ib_{n,n}+$ $+a_{i,n,n}b_n^2 + 3a_{n,n,n}b_ib_n^2$	$\forall i = 1, ..., n-1$
u_n^3	$a_nb_{n,n,n} + 2a_{n,n}b_nb_{n,n} + 3a_{n,n,n}b_n^3$	
...	...	...

Nous introduisons ici une nouvelle notation pour indiquer le même indice multiple $\mu \in \mathbb{N}^n$ quelconque quand une expression en série formelle :

$$E(\overline{X}) := \sum_{i\geq 1}\sum_{\mu\in\Lambda_n(i)} c_\mu\overline{X}^{\mu};$$

s'écrit aussi sous la forme suivante :

$$E(\overline{X}) := \sum_{i=1}^{n} c_iX_i + \sum_{i_1=1}^{n}\sum_{i_2=1}^{n} c_{i_1,i_2}X_{i_1}X_{i_2} + ... + \sum_{i_1=1}^{n} ... \sum_{i_k=1}^{n} c_{i_1,...,i_k}\prod_{h=1}^{k} X_{i_h} + ...$$

Nous remarquons en effet que dans ce cas, bien que la série formelle soit toujours la même, l'ordre de sommation des monômes peut changer et les indices des coefficients n'ont pas une longueur bornée, à la différence de ce qui arrive avec la notation précédente. Nous appelons $i(\mu) \in \mathbb{N} \setminus \{0\}$ la longueur k de l'indice multiple $(i_1, ..., i_k)$ dans la deuxième notation correspondant à μ dans la première. Autrement dit, tel que :

$$\overline{X}^{\mu} = \prod_{h=1}^{k} X_{i_h}.$$

Nous remarquons que chacun de ces nouveaux indices multiples $(i_1, ..., i_k)$ est toujours tel que $i_1 \leq ... \leq i_k$ suite au fait que les produits sont commutatifs. L'annulation de tous les coefficients de la série formelle $F(H(\overline{u})) - u_n$ nous emmène au système suivant, que nous appelons S1 :

$$\begin{cases} a_n b_n = 1 & \\ a_n b_i = a_i & \forall i = 1, ..., n-1; \\ a_n b_\mu = -P_\mu(\{a_\eta\}, \{b_{\mu'}\}) & \forall |\mu| \geq 2, |\eta| \leq |\mu|, i(\mu') < i(\mu); \end{cases}$$

où P_μ est pour chaque $\mu \in \Lambda_n(i)$, $i \geq 2$, un polynôme à coefficients dans $\mathbb{F}_q$ et tel que le signe devant chacun de ses monômes est toujours positif. Ce système se résout par récurrence sur la valeur de $i(\mu)$. Nous remarquons d'abord que :

$$b_n = \frac{1}{a_n};$$

et que :

$$b_i = \frac{a_i}{a_n}, \ \ \forall i = 1, ..., n-1.$$

Des telles solutions existent puisque les hypothèses que nous sommes en train de supposer prévoient la condition $a_n \neq 0$. En remplaçant ces solutions dans les équations de la forme $a_n b_\mu = -P_\mu(\{a_\eta\}, b_i)$, où $i(\mu) = 2$ et $i = 1, ..., n$, nous obtenons b_μ. En général, nous remplaçons donc la solution $b_{\mu'}$ dans l'équation $a_n b_\mu = -P_\mu(\{a_\eta\}, \{b_{\mu'}\})$ pour tout $1 \leq i(\mu') < i(\mu)$.

En procédant par récurrence on trouve finalement la série formelle h (et, par conséquent H) cherchée. On remarque, en plus, que $\frac{\partial}{\partial u_n} h(\overline{0}) \neq 0$, comme $b_n \neq 0$. Par conséquent, h respecte les mêmes hypothèses, en tant que série formelle, que F. Il existe, donc, en répétant le même raisonnement pour H, un vecteur de séries formelles :

$$H_1 : K^n \to K^n;$$

tel que :

$$H \circ H_1 = 1.$$

Par conséquent :

$$G = G \circ H \circ H_1 = H_1;$$

ce qui prouve :

$$G \circ H = H \circ G = 1.$$

On remarque, finalement, qu'une telle H est unique, puisqu'elle est déterminée comme unique solution du système S1 qu'on a construit. En restreignant h à la projection de K^n sur ses premières $n-1$ composantes on obtient une série formelle :

$$\widetilde{h} : K^{n-1} \to K;$$

telle que :

$$\widetilde{h}(\overline{z}^*) := h(\overline{z}^*, 0);$$

ce qui prouve aussi le Théorème de la Fonction Implicite Formel, comme :

$$F(\overline{z}^*, \widetilde{h}(\overline{z}^*)) = 0;$$

en tant qu'identité formelle.

Le deuxième pas à faire est de montrer qu'une telle $\widetilde{h}$ est une série convergente sur un voisinage ouvert pas singulier de $\overline{0}$ (soit, différent de $\{\overline{0}\}$). Autrement dit, que la série formelle $\widetilde{h}$ a un rayon de convergence pas nul. Nous définissons alors une **série majorante** :

$$\overline{F} : \mathbb{R}^n \to \mathbb{R};$$

telle que :

$$\overline{F}(X_1, ..., X_n) := -\sum_{i=1}^{n-1} A_i X_i + A_n X_n - \sum_{i\geq 2} \sum_{\mu \in \Lambda_n(i)} A_\mu \overline{X}^\mu;$$

où $A_\mu \geq 0$ pour tout $\mu \in \Lambda_n(i)$, $i \geq 1$, et que :

$$|a_\mu|_{1/T} \leq A_\mu \ \ \forall \mu \in \Lambda_n(i), i \geq 2;$$

$$A_i = |a_i|_{1/T} \ \ \forall i = 1, ..., n.$$

En particulier, $\overline{F}(\overline{0}) = \overline{0}$ et, comme $A_n = |a_n|_{1/T} \neq 0$, $\overline{F}$ vérifie les mêmes hypothèses de régularité en $\overline{0}$ que F, mais sur $\mathbb{R}^n$. Nous définissons aussi :

$$\overline{G} : \mathbb{R}^n \to \mathbb{R}^n;$$

$$\overline{G}(\overline{X}) := (\overline{X}^*, \overline{F}(\overline{X})).$$

S'agissant de séries formelles, la structure topologique des corps induite par la valuation choisie ne joue aucun rôle, nous permettant donc de répéter sans aucune différence les mêmes passages que dans le cas de F et G, en trouvant donc une série formelle inverse $\overline{H}$ de $\overline{G}$, telle que la série H précédemment trouvée pour G. Elle prendra alors la forme :

$$\overline{H}(Y_1, ..., Y_n) := (\overline{Y}^*, \overline{h}(\overline{Y})) := (Y_1, ..., Y_{n-1}, \sum_{i=1}^{n} B_i Y_i + \sum_{i\geq 2} \sum_{\mu \in \Lambda_n(i)} B_\mu \overline{Y}^\mu).$$

Nous allons appliquer les définitions pour répéter les calculs d'avant dans cette nouvelle situation pour exprimer les coefficients de $\overline{h}$ en fonction de ceux de $\overline{F}$. Nous obtenons par conséquent :

$$\overline{F}(\overline{H}(\overline{Y})) = -\sum_{i=1}^{n-1} A_i Y_i + A_n (\sum_{i=1}^{n} B_i Y_i + \sum_{i=1}^{n} \sum_{j=1}^{n} B_{i,j} Y_i Y_j + ...) +$$

$$-\sum_{i=1}^{n-1}\sum_{j=1}^{n-1}A_{i,j}Y_iY_j-\sum_{i=1}^{n-1}A_{i,n}Y_i(\sum_{i=1}^{n}B_iY_i+\sum_{i=1}^{n}\sum_{j=1}^{n}B_{i,j}Y_iY_j+...)+$$
$$-A_{n,n}(\sum_{i=1}^{n}B_iY_i+\sum_{i=1}^{n}\sum_{j=1}^{n}B_{i,j}Y_iY_j-...)^2-...=Y_n.$$

Les coefficients B_μ de $\overline{H}$ sont alors obtenus, en répétant les mêmes passages déjà faits pour trouver h, en tant que solutions du système suivant, que nous appelons S2 et qu'on construit de la même façon que S1, où les P_μ sont les mêmes polynômes à coefficients dans $\mathbb{F}_q$ que nous avons introduits précédemment :

$$\begin{cases} A_nB_n=1 & \\ -A_i+A_nB_i=0 & \forall i=1,...,n-1 \\ A_nB_\mu=P_\mu(\{A_\eta\},\{B_{\mu'}\}) & \forall|\mu|\geq 2, |\eta|\leq|\mu|, i(\mu')<i(\mu); \end{cases}$$

Nous obtenons finalement :

$$|a_ib_n|_{1/T}=|b_i|_{1/T}\ \ \forall i=1,...,n-1.$$

Donc :

$$|b_i|_{1/T}=\frac{A_i}{A_n}\ \ \forall i=1,...,n-1.$$

En même temps :

$$B_i=\frac{A_i}{A_n}=\frac{|a_i|_{1/T}}{|a_n|_{1/T}}=|b_i|_{1/T}\ \ \forall i=1,...,n-1. \tag{2.1}$$

D'un autre côté :

$$B_n=\frac{1}{A_n}=\frac{1}{|a_n|_{1/T}}=|b_n|_{1/T}.$$

Suite au système S1 on a :

$$|b_\mu|_{1/T}=\frac{|P_\mu(\{a_\eta\},\{b_{\mu'}\})|_{1/T}}{|a_n|_{1/T}}\leq\frac{P_\mu(\{A_\eta\},\{|b_{\mu'}|_{1/T}\})}{A_n}; \tag{2.2}$$

où $i(\mu)\geq 2$, $|\eta|\leq|\mu|$ et $i(\mu')<i(\mu)$, puisque le polynôme P_μ est toujours tel que le signe devant chacun de ses monômes est toujours positif, en nous rappelant que $|a_\eta|_{1/T}\leq A_\eta$ pour tout $i(\eta)>1$, alors que $|a_i|_{1/T}=A_i$ pour tout $i=1,...,n$. En même temps le système S2 nous dit que :

$$B_\mu=\frac{P_\mu(\{A_\eta\},\{B_{\mu'}\})}{A_n};$$

pour tout $\mu\in\Lambda_n(i)$, $i\geq 2$, $|\eta|\leq|\mu|$, $i(\mu')<i(\mu)$.

Nous appliquons la récurrence sur la valeur de $i(\mu)$ en utilisant (2.1) à l'inégalité (2.2). On peut voir alors comment :

$$|b_\mu|_{1/T}\leq B_\mu; \tag{2.3}$$

pour tout $\mu\in\Delta_n[i]$, quelque soit $i\geq 2$. La série formelle $\overline{h}$ est, donc, série majorante de h.

Soit $r > 0$ un nombre réel strictement inférieur au rayon de convergence de F en $\overline{0}$. On a, alors :

$$\lim_{|\mu|\to+\infty} |a_\mu|_{1/T} r^{|\mu|} = 0.$$

Il existe, donc :

$$M := \max_{|\mu|\geq 1}\{|a_\mu|_{1/T} r^{|\mu|}\} > 0.$$

En posant :

$$A_i := |a_i|_{1/T} \ \ \forall i = 1, ..., n;$$

$$A_\mu := \frac{M}{r^{|\mu|}} \ \ \forall |\mu| \geq 2; \tag{2.4}$$

on a :

$$\overline{F}(\overline{X}) = -\sum_{i=1}^{n-1} A_i X_i + A_n X_n - \sum_{i\geq 2}\sum_{\mu\in\Lambda_n(i)} A_\mu \overline{X}^\mu =$$

$$= -\sum_{i=1}^{n-1} A_i X_i + A_n X_n - \sum_{i\geq 2}\frac{M}{r^i}\sum_{\mu\in\Lambda_n(i)} \overline{X}^\mu.$$

Soit :

$$||.||_\infty : \mathbb{R}^n \to \mathbb{R};$$

la norme sur $\mathbb{R}$ donnée comme il suit :

$$||(X_1, ..., X_n)||_\infty := \max_{i=1,...,n}\{|X_i|\};$$

on a :

$$|\overline{X}^\mu| \leq ||\overline{X}||_\infty^{|\mu|}.$$

Pour tout $\overline{X} \in \mathbb{R}^n$ tel que $||\overline{X}||_\infty < r$, la valeur $\overline{F}(\overline{X})$, exprimée par la série précédente est, donc, définie par la convergence en sens absolu de cette série. Plus précisément, on a la situation suivante :

$$-\sum_{i=1}^{n-1} A_i X_i + A_n X_n - \sum_{i\geq 2}\frac{M}{r^i}\sum_{\mu\in\Lambda_n(i)} \overline{X}^\mu = -\sum_{i=1}^{n-1} A_i X_i + A_n X_n - M(\sum_{i=1}^{n}\sum_{j\geq 2}(\frac{X_i}{r})^j +$$

$$+\sum_{h=1}^{\binom{n}{2}}(\sum_{j\geq 1}(\frac{X_{i_1(h)}}{r})^j)(\sum_{j\geq 1}(\frac{X_{i_2(h)}}{r})^j)+...+\sum_{h=1}^{\binom{n}{n-1}}\prod_{i(h)=1}^{n-1}(\sum_{j\geq 1}(\frac{X_{i(h)}}{r})^j)+\prod_{i=1}^{n}(\sum_{j\geq 1}(\frac{X_i}{r})^j)).$$

La condition $||\overline{X}||_\infty < r$ implique la convergence en sens absolu des séries géométriques dans l'inégalité précédente, qui se présenteront alors sous la forme :

$$-\sum_{i=1}^{n-1} A_i X_i + A_n X_n - \sum_{i\geq 2}\frac{M}{r^i}\sum_{\mu\in\Lambda_n(i)} \overline{X}^\mu = -\sum_{i=1}^{n-1} A_i X_i + A_n X_n - M(\sum_{i=1}^{n}\frac{(\frac{X_i}{r})^2}{1-\frac{X_i}{r}} +$$

$$+\sum_{h=1}^{\binom{n}{2}}(\frac{\frac{X_{i_1(h)}}{r}}{1-\frac{X_{i_1(h)}}{r}})(\frac{\frac{X_{i_2(h)}}{r}}{1-\frac{X_{i_2(h)}}{r}}) + ... + \sum_{h=1}^{\binom{n}{n-1}}\prod_{i(h)=1}^{n-1}\frac{\frac{X_{i(h)}}{r}}{1-\frac{X_{i(h)}}{r}} + \prod_{i=1}^{n}\frac{\frac{X_i}{r}}{1-\frac{X_i}{r}}).$$

Nous observons que les dénominateurs sont toujours différents de 0 par la condition $||\overline{X}||_\infty < r$. En imposant, donc, la condition définissant $\overline{H}$:

$$\overline{F}(\overline{H}(\overline{Y})) = Y_n;$$

on obtiendra une équation rationnelle de degré 2 en $X_n = \overline{h}(\overline{Y})$, de la forme :

$$-\sum_{i=1}^{n-1} A_iY_i + A_nX_n - M(\alpha_1 + \frac{\frac{X_n^2}{r^2}}{1-\frac{X_n}{r}} + \alpha_2 + \alpha_3\frac{\frac{X_n}{r}}{1-\frac{X_n}{r}} + ... + \alpha_{2n-2} + \alpha_{2n-1}\frac{\frac{X_n}{r}}{1-\frac{X_n}{r}} + \alpha_{2n}\frac{\frac{X_n}{r}}{1-\frac{X_n}{r}}) = Y_n;$$

où $\alpha_1, ..., \alpha_{2n}$ sont des polynômes en $\frac{Y_i}{r}$ et $\frac{Y_i}{r}/(1-\frac{Y_i}{r})$ avec $i = 1, ..., n-1$ dont le degré est ≥ 1. Plus précisément, en regardant l'expression de $\overline{F}(\overline{X})$ précédente ces expressions rationnelles en $Y_1, ..., Y_{n-1}$ sont de la forme suivante :

$$\alpha_1 := \sum_{i=1}^{n-1} \frac{(\frac{Y_i}{r})^2}{1-(\frac{Y_i}{r})};$$

$$\alpha_2 := \sum_{h=1}^{\binom{n-1}{2}} (\frac{\frac{Y_{i_1(h)}}{r}}{1-\frac{Y_{i_1(h)}}{r}})(\frac{\frac{Y_{i_2(h)}}{r}}{1-\frac{Y_{i_2(h)}}{r}});$$

$$\alpha_3 := \sum_{i=1}^{n-1} \frac{\frac{Y_i}{r}}{1-\frac{Y_i}{r}};$$

$$\cdots;$$

$$\alpha_{2n} := \prod_{i=1}^{n-1} \frac{\frac{Y_i}{r}}{1-\frac{Y_i}{r}}.$$

Nous remarquons en particulier que α_3 s'annule en $\overline{0}$ avec une multiplicité 1 alors que toutes les α_i telles que $i \neq 3$ ont toujours un ordre d'annulation en $\overline{0}$ qui est ≥ 2. En multipliant tous les termes par $1-(X_n/r)$ on obtient :

$$(1-X_n/r)A_nX_n - MX_n^2/r^2 - M(1-X_n/r)(\alpha_1 + \sum_{i=1}^{n-1}\alpha_{2i}) +$$

$$-M(\sum_{i=1}^{n-1}\alpha_{2i+1} + \alpha_{2n})X_n/r - (1-X_n/r)(\sum_{i=1}^{n-1}A_iY_i + Y_n) = 0.$$

Donc :

$$(A_n/r + M/r^2)X_n^2 + (1/r(M(\sum_{i=1}^{n-1}\alpha_{2i+1} + \alpha_{2n} - \alpha_1 - \sum_{i=1}^{n-1}\alpha_{2i}) - \sum_{i=1}^{n-1}A_iY_i - Y_n) - A_n)X_n +$$

$$+M(\alpha_1 + \sum_{i=1}^{n-1}\alpha_{2i}) + \sum_{i=1}^{n-1}A_iY_i + Y_n = 0.$$

En approximant à l'ordre 1 l'expression à gauche d'une telle égalité, pour $||\overline{Y}||_\infty$ qui tend vers 0 les termes $\alpha_1, ..., \alpha_{2n}$ deviennent négligeables avec la seule exception de α_3 :

$$(A_n/r + M/r^2)X_n^2 + (1/r(-\sum_{i=1}^{n-1}A_iY_i - Y_n) - A_n + M\alpha_3)X_n + \sum_{i=1}^{n-1}A_iY_i + Y_n = 0.$$

En approximant toujours à l'ordre 1 pour $||\overline{Y}||_\infty \to 0$ le discriminant :

$$\Delta = A_n^2 - 2/r(-\sum_{i=1}^{n-1} A_iY_i - Y_n + M\sum_{i=1}^{n-1}\frac{Y_i/r}{1-Y_i/r}) + 4(A_n/r + M/r^2)(-\sum_{i=1}^{n-1} A_iY_i - Y_n).$$

Cette dernière expression est une fonction de $\mathbb{R}^n$ dans $\mathbb{R}$ continue dans un voisinage ouvert de $\overline{0}$ opportun qui soit contenu dans la sphère ouverte de centre $\overline{0}$ et rayon 1 dans $\mathbb{R}^n$. Comme $\Delta(\overline{0}) = A_n^2 > 0$, il existe, alors, un voisinage ouvert suffisamment petit de $\overline{0}$ tel que $\Delta(\overline{Y}) > 0$, pour tout $\overline{Y}$ qui en fait partie. Il existe, donc, $\overline{Y} \neq \overline{0}$ dans $\mathbb{R}^n$ tel que :

$$X_n = \overline{h}(\overline{Y}) \in \mathbb{R};$$

en tant que nombre réel fini. La série majorante $\overline{h}$ de h a donc un rayon de convergence en $\overline{0}$ pas nul et par conséquent il en est de même pour h et donc finalement pour $\widetilde{h}$. □

Corollaire 2.1.25. *Soit $\overline{F} : K^{n+m} \to K^m$ un vecteur de fonctions analytiques sur un certain ouvert de K^n, tel que sa matrice Jacobienne $J_{\overline{z}_0}(\overline{F})$ en un point $\overline{z}_0 \in Z(\overline{F})$, soit telle que ses lignes sont linéairement indépendantes (autrement dit, elle a un rang qui est égal à m). A une permutation près dans l'ordre des colonnes on peut partager cette matrice en deux blocs de colonnes de la façon suivante :*

$$J_{\overline{z}_0}(\overline{F}) = (J_{n,m}(\overline{F}(\overline{z}_0))|J_{m,m}(\overline{F}(\overline{z}_0)));$$

avec $J_{m,m}(\overline{F}(\overline{z}_0))$ matrice carrée inversible. Il existe alors un voisinage ouvert de la forme $U_{\overline{z}_0} \times V_{\overline{z}_0} \subset K^n \times K^m$, et un vecteur de fonctions analytiques :

$$\overline{f} : U_{\overline{z}_0} \to V_{\overline{z}_0};$$

tels que pour tout $\overline{z}_* \in U_{\overline{z}_0}$, on ait :

$$\overline{F}(\overline{z}_*, \overline{f}(\overline{z}_*)) = 0.$$

Démonstration. Comme le rang de la Jacobienne est m, quitte à permuter les colonnes de la matrice (donc les variables de l'espaces de départ), on peut supposer que la matrice extraite de la Jacobienne, constitué du bloc des m dernières colonnes à droite et d'ordre $m \times m$, est inversible. Appelons $J_{m,m}(\overline{F}(\overline{z}_0))$ cette matrice. Maintenant nous remarquons que la méthode de triangularisation des matrices carrées de Gauss (la méthode du pivot) est valable dans n'importe quel corps, donc dans notre situation aussi. Il existe donc une matrice inversible $P \in K^{m,m}$ telle que :

$$PJ_{m,m}(\overline{F}(\overline{z}_0));$$

est triangulaire supérieure. A une composition à gauche par l'application linéaire répresentée par P nous pouvons alors supposer que la fonction analytique $\overline{F}$ est telle que la matrice $J_{m,m}(\overline{F}(\overline{z}_0))$ est triangulaire supérieure avec aucun terme nul dans sa diagonale. Cela ne nous fait pas perdre en généralité. En effet, si nous composons à gauche $\overline{F}$ par l'application linéaire qu'on a introduit et nous notons :

$$P\begin{pmatrix} F_1(\overline{z}) \\ \cdots \\ F_m(\overline{z}) \end{pmatrix} = \begin{pmatrix} G_1(\overline{z}) \\ \cdots \\ G_m(\overline{z}) \end{pmatrix};$$

nous avons que :

$$\begin{pmatrix} F_1(\overline{z}) \\ \cdots \\ F_m(\overline{z}) \end{pmatrix} = P^{-1} \begin{pmatrix} G_1(\overline{z}) \\ \cdots \\ G_m(\overline{z}) \end{pmatrix}.$$

S'il existe un voisinage ouvert $U_{\overline{z}_0} \times V_{\overline{z}_0} \subset K^n \times K^m$ de $\overline{z}_0$ et une fonction analytique :

$$\overline{f} : U_{\overline{z}_0} \to V_{\overline{z}_0};$$

telle qu'on ait l'identité fonctionnelle suivante :

$$\overline{G}(z_1, ..., z_n, \overline{f}(z_1, ..., z_n)) = \overline{0};$$

nous voyons que :

$$\overline{F}(z_1, ..., z_n, \overline{f}(z_1, ..., z_n)) = \overline{0};$$

aussi, pour tout $\overline{z} \in U_{\overline{z}_0}$. Nous supposons donc sans perte de généralité que $J_{m,m}(\overline{F}(\overline{z}_0))$ est triangulaire supérieure. Par conséquent il s'ensuit que :

$$\frac{\partial}{\partial z_{n+i}} F_j(\overline{z}_0) = 0 \ \ \forall i < j.$$

Le Théorème 2.1.24 appliqué à $F_1, ..., F_m : K^{n+m} \to K$ nous dit maintenant que pour chaque F_i, $i = 1, ..., m$, il existe un voisinage $D^i_{\overline{z}_0}$ de $\overline{z}_0$ dans K^{n+m} dans lequel les points de notre ensemble analytique s'expriment sous la forme suivante :

$$(\overline{z}_*, z_{n+1}, ..., z_{n+i-1}, f_i(\overline{z}^{i*}), z_{n+i+1}, ..., z_{n+m});$$

où, si on appelle $\overline{z}^{i*}$ la projection d'un point quelconque de K^{n+m} sur toutes ses coordonnées différentes de la $(n+i)-$ième :

$$f_i : W^i_{\overline{z}_0} \to K;$$

est une fonction analytique définie sur le voisinage ouvert $W^i_{\overline{z}_0} \subset K^n \times K^{m-1}$ de $\overline{z}_0^{i*}$ projection de $D^i_{\overline{z}_0}$ sur toutes ses coordonnées différentes de la $(n+i)-$ième et cette f_i est telle que, pour tout $\overline{z}^{i*} = (\overline{z}_*, z_{n+1}, ..., z_{n+i-1}, z_{n+i+1}, ..., z_{n+m}) \in W^i_{\overline{z}_0}$:

$$F_i(\overline{z}_*, z_{n+1}, ..., f_i(\overline{z}^{i*}), ..., z_{n+m}) = 0;$$

avec $\overline{z}_*$ qui est la projection de $\overline{z}$ sur ses n premières composantes. On a alors l'identité fonctionnelle suivante :

$$\begin{cases} F_1(\overline{z}_*, f_1(\overline{z}^{1*}), z_{n+2}, ..., z_{n+m}) = 0 \\ F_2(\overline{z}_*, z_{n+1}, f_2(\overline{z}^{2*}), ..., z_{n+m}) = 0 \\ ... \\ F_m(\overline{z}_*, z_{n+1}, ..., z_{n+m-1}, f_m(\overline{z}^{m*})) = 0 \end{cases} \tag{2.5}$$

avec des fonctions f_i, $i = 1, ..., m$ définies sur $W^i_{\overline{z}_0}$, $i = 1, ..., m$ (projection sur toutes ses coordonnées sauf la $(n+i)-$ième d'un différent $D^i_{\overline{z}_0}$, $i = 1, ..., m$) en $n + m - 1$ variables sous la forme suivante :

$$\begin{cases} z_{n+1} = f_1(\overline{z}_*, z_{n+2}, ..., z_{n+m}) \\ ... \\ z_{n+m} = f_m(\overline{z}_*, z_{n+1}, ..., z_{n+m-1}) \end{cases}$$

Soit $W_{\overline{z}_0} \subset K^{n+m}$ l'intersection de tous les $D^i_{\overline{z}_0}$. Pour tout $\overline{z} \in W_{\overline{z}_0}$ la condition $\overline{F}(\overline{z}) = \overline{0}$ est équivalente à la suivante :

$$\begin{cases} z_{n+1} = f_1(\overline{z}_*, f_2(\overline{z}^{2*}), z_{n+3}, ..., z_{n+m}) \\ z_{n+2} = f_2(\overline{z}_*, z_{n+1}, f_3(\overline{z}^{3*}), ..., z_{n+m}) \\ ... \\ z_{n+m} = f_m(\overline{z}_*, f_1(\overline{z}^{1*}), ..., z_{n+m-1}) \end{cases}$$

En appelant :

$$\begin{cases} g_1(\overline{z}) := z_{n+1} - f_1(\overline{z}_*, f_2(\overline{z}^{2*}), ..., z_{n+m}) \\ ... \\ g_m(\overline{z}) := z_{n+m} - f_m(\overline{z}_*, f_1(\overline{z}^{*1}), ..., z_{n+m-1}) \end{cases}$$

nous obtenons que dans le voisinage ouvert $W_{\overline{z}_0}$ de $\overline{z}_0$ le lieu des zéros du vecteur des fonctions analytiques $\overline{F}$ s'exprime de façon équivalente sous la forme suivante :

$$\begin{cases} g_1(\overline{z}_*, z_{n+1}, z_{n+3}, ..., z_{n+m}) = 0 \\ ... \\ g_m(\overline{z}_*, z_{n+2}, z_{n+3}, ..., z_{n+m}) = 0 \end{cases}$$

où les fonctions $g_1, ..., g_m$ sont analytiques. Nous nous sommes donc ramenés localement en $\overline{z}_0$ à un système sous la forme suivante :

$$\overline{g}(\overline{z}) = \overline{0};$$

où les m fonctions analytiques indiquées par le vecteur $\overline{g}$ en $\overline{z} \in W_{\overline{z}_0} \subset K^{n+m}$ sont en fait exprimées en $n+m-1$ variables chacune. Il nous reste à montrer que la condition sur la matrice Jacobienne ne change donc pas. La règle de calcul de la dérivée d'une composition de deux fonctions (voir [Teich]) nous permet alors de dire suite à (2.6), en faisant la dérivée divisée en $z_{n+1}, ..., z_{n+m}$ de chaque équation de ce système (en tenant compte du fait que la dérivée divisée en z_{n+i} de la $i-$ième équation de celui-ci est identiquement 0), que :

$$\begin{cases} \partial_{n+1}F_1(\overline{z}_0)\partial_{n+2}f_1(\overline{z}_0^{*1}) + \partial_{n+2}F_1(\overline{z}_0) = 0 \\ ... \\ \partial_{n+1}F_1(\overline{z}_0)\partial_{n+m}f_1(\overline{z}_0^{1*}) + \partial_{n+m}F_1(\overline{z}_0) = 0 \\ ... \\ \partial_{n+m}F_m(\overline{z}_0)\partial_{n+1}f_m(\overline{z}_0^{m*}) + \partial_{n+1}F_m(\overline{z}_0) = 0 \\ ... \\ \partial_{n+m}F_m(\overline{z}_0)\partial_{n+1}f_m(\overline{z}_0^{*m}) + \partial_{n+1}F_m(\overline{z}_0) = 0 \end{cases}$$

La condition sur la diagonale de la matrice $J_{\overline{z}_0}(\overline{F})$ nous permet donc d'exprimer :

$$\begin{cases} \partial_{n+i}f_1(\overline{z}_0^{*1}) = -\frac{\partial_{n+i}F_1(\overline{z}_0)}{\partial_{n+1}F_1(\overline{z}_0)} \ \ \forall i \neq 1 \\ ... \\ \partial_{n+i}f_m(\overline{z}_0^{*m}) = -\frac{\partial_{n+i}F_m(\overline{z}_0)}{\partial_{n+m}F_m(\overline{z}_0)} \ \ \forall i \neq m \end{cases}$$

La sous-matrice $J_{m,m}(\overline{g}(\overline{z}_0))$ de la matrice Jacobienne $J_{\overline{z}_0}(\overline{g})$ est d'un autre côté sous la forme suivante :

$$\partial_{n+i}g_i(\overline{z}_0) = 1 - \partial_{n+i}f_i(\overline{z}_0^{i*})\partial_{n+i}f_{i+1}(\overline{z}_0^{(i+1)*});$$

$$\partial_{n+i+1}g_i(\overline{z}_0) = 0;$$
$$\partial_{n+i}g_j(\overline{z}_0) = -\partial_{n+i}f_j(\overline{z}_0^{j*}) - \partial_{n+j+1}f_j(\overline{z}_0^{j*})\partial_{n+i}f_{j+1}(\overline{z}_0^{(j+1)*}) \ \ \forall i \neq j, j+1;$$

où tous les indices i et j indiquent les uniques entiers entre 1 et m dans leur même classe de congruence modulo m. Comme :

$$\partial_{n+i}F_j(\overline{z}_0) = 0 \ \ \forall i < j;$$

les conditions que nous avons trouvé précédemment nous permettent de dire que :

$$\partial_{n+i}f_j(\overline{z}_0^{j*}) = 0 \ \ \forall i < j.$$

La matrice carrée $J_{m,m}(\overline{g}(\overline{z}_0))$ définie avant de la même façon que $J_{m,m}(\overline{F}(\overline{z}_0))$ est par conséquent sous la forme suivante :

$$J_{m,m}(\overline{g}(\overline{z}_0)) = \begin{pmatrix} 1 & 0 & \partial_{n+3}g_1(\overline{z}_0) & \cdots & \partial_{n+m}g_1(\overline{z}_0) \\ 0 & 1 & 0 & \cdots & \partial_{n+m}g_2(\overline{z}_0) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Nous voyons qu'il s'agit d'une matrice inversible et triangulaire supérieure.

Nous nous sommes donc finalement ramenés à pouvoir supposer sans perte de généralité que chaque équation $F_i(\overline{z}) = 0$ pour chaque $i = 1, ..., m$ n'implique que $n + m - 1$ variables et plus précisément, qu'elle peut s'écrire sous la forme suivante :

$$F_i(\overline{z}^{i*}) = 0;$$

pour tout $i = 1, ..., m$. En répétant donc les mêmes passages $m - 1$ fois encore nous obtenons que dans $W_{\overline{z}_0}$ les solutions du système sont sous la forme suivante :

$$\begin{cases} z_{n+1} = h_1(\overline{z}_*) \\ ... \\ z_{n+m} = h_m(\overline{z}_*) \end{cases}$$

En particulier, $W_{\overline{z}_0} = U_{\overline{z}_{0*}} \times V_{\overline{z}_0^*} \subset K^n \times K^m$ et on a que le vecteur de fonctions analytiques $\overline{h} := (h_1, ..., h_m)$ qu'on a construit est tel que :

$$\overline{h} : U_{\overline{z}_{0*}} \to V_{\overline{z}_0^*};$$

et elle est par conséquent la fonction implicite cherchée.

□

Remarque 2.1.26. *Nous remarquons que la fonction implicite $\overline{h} : U_{\overline{z}_0} \to V_{\overline{z}_0}$ qu'on vient de construire dans le Corollaire 2.1.25 induit un homéomorphisme entre $U_{\overline{z}_0}$ et l'intersection du lieu des zéros $Z(\overline{F})$ de $\overline{F}$ dans K^{n+m} avec un voisinage ouvert contenant $\overline{z}_0$. Cet homéomorphisme se présente sous la forme suivante :*

$$\Phi_{\overline{z}_0} : U_{\overline{z}_0} \to Z(\overline{F}) \cap V_{\overline{z}_0};$$
$$(z_1, ..., z_n) \mapsto (z_1, ..., z_n, \overline{h}(z_1, ..., z_n)).$$

Nous voyons en effet qu'il s'agit d'une fonction analytique injective. Les contructions d'avant nous permettent de dire que la matrice Jacobienne $J(\Phi_{\overline{z}_0})$ a un rang maximal et donc de déduire que la fonction inverse de $\Phi_{\overline{z}_0}$ est toujours une fonction analytique. Comme nous le montrerons plus loin, voir Lemme 2.3.2, tout fonction analytique est continue, ce qui prouve que $\Phi_{\overline{z}_0}$ est un homéomorphisme entre $U_{\overline{z}_0}$ et $\Phi_{\overline{z}_0}(U_{\overline{z}_0})$.

Définition 2.1.27. *Soit $X \subset K^n$ un sous-ensemble $K-$entier de K^n pour un certain $n \in \mathbb{N} \setminus \{0\}$. On dira que X est* ***analytiquement paramétrisable*** *sur K s'il existe un nombre $d \in \mathbb{N} \setminus \{0\}$ tel que $d < n$ ainsi qu'une famille $\mathcal{R}$ de fonctions $K-$analytiques de la forme suivante :*

$$f : B_1^d(K) \to X;$$

telles que :

$$X \subseteq \bigcup_{f \in \mathcal{R}} f(B_1^d(K)).$$

On appellera une telle famille $\mathcal{R}$ un ***recouvrement analytique*** *sur K de X.*

2.1.2 Ensembles analytiques

A la différence de ce qui se passe sur des corps de nombres, les propriétés topologiques très strictes d'un corps de valuation non-archimédienne interdisent de prolonger une fonction analytique (qui sur les corps de nombres est appelée analytique) définie sur un ouvert à une fonction analytique sur un ouvert plus grand. En effet dans notre situation l'intersection non vide de deux polydisques est nécessairement l'un des deux, ce qui ne permet pas aux fonctions analytiques de constituer un moyen de mise en relation entre deux régions différentes du même domaine de définition. Il s'agit d'un obstacle décisif à toute tentative de construire des faisceaux sur une variété définie sur des corps de valuation non-archimédienne et par conséquent de pouvoir utiliser de telles fonctions pour décrire les propriétés d'une telle variété. Nous allons adapter ici les instruments classiques d'étude des sous-ensembles $K-$analytiques de K^n, pour un certain $n \in \mathbb{N} \setminus \{0\}$ où K est un corps de valuation non-archimédien et complet, à notre situation particulière où K est un corps de valuation $1/T-$adique complet qui est une extension finie de k_∞ contenue dans $\mathcal{C}$. Plus précisément nous allons introduire les **espaces affinoïdes**, un objet mathématique spécifiquement conçu (dont la construction est due à J. Tate) pour analyser localement le comportement et les propriétés des lieux des zéros d'un certain nombre des fonctions $K-$analytiques dans le domaine de définition de ces dernières.

Définition 2.1.28. *Soit K une extension algébrique de k_∞ qui soit aussi un corps complet contenu dans $\mathcal{C}$. Soit $n \in \mathbb{N} \setminus \{0\}$. Soit donné l'ensemble qui suit :*

$$T_n(K) := K \ll z_1, ..., z_n \gg := \{\sum_{i \geq 0} \sum_{\mu \in \Lambda_n(i)} a_\mu \overline{z}^\mu \in K[[z_1, ..., z_n]], \lim_{|\mu| \to +\infty} a_\mu = 0\};$$

nous remarquons qu'il s'agit d'une algèbre, qu'on appelle ***algèbre affinoïde libre****. Nous remarquons également qu'il s'agit de l'anneau de toutes les séries formelles à coefficients dans K en $z_1, ..., z_n$ qui sont convergentes dans le polydisque unitaire (avec "bord") $B_1^n(\mathcal{C}) \subset \mathcal{C}^n$. Soit $I \subseteq T_n(K)$ un idéal dans cette algèbre. Nous appelons :*

$$\widetilde{X} := Sp(T_n(K)/I);$$

le spectre maximal du quotient d'une telle algèbre par I. On dit que $\widetilde{X}$ est un ***espace affinoïde*** *et que l'algèbre quotient $T_n(K)/I$ est une* ***algèbre de Tate****. On dit aussi que $\widetilde{X}$ est* ***irréductible*** *si I est un idéal premier dans $T_n(K)$.*

Théorème 2.1.29. *1. Toute algèbre de Tate est Noethérienne.*

2. *$T_n(K)$ est un anneau factoriel dont la dimension de Krull est n.*
3. *Pour tout idéal $I \subseteq T_n(K)$ il existe un unique nombre $d \in \mathbb{N} \setminus \{0\}$ et un morphisme de $K-$algèbres fini et injectif :*

$$T_d(K) \hookrightarrow T_n(K)/I;$$

la dimension de Krull de $T_n(K)/I$ est d.
4. *Pour tout idéal maximal $\mathcal{M}$ dans $T_n(K)$ le corps quotient $T_n(K)/\mathcal{M}$ est une extension finie de K.*

Démonstration. Voir [V-F], Theorem 3.2.1, page 48. □

Nous remarquons que le Théorème 2.1.29 est l'analogue dans le cas des séries de puissances convergentes dans $B_1^n(K)$ du Théorème de la Base Transcendante en Géométrie Algébrique. Nous remarquons aussi que puisque $T_n(K)$ est une algèbre Noethérienne I n'est contenu que dans un nombre fini r d'idéaux premiers $P_1, ..., P_r$ minimaux parmi ceux qui contiennent I dans $T_n(K)$. Soit $\overline{K} \subset \mathcal{C}$ la clôture algébrique de K contenue dans $\mathcal{C}$. Soit $\mathcal{M} \in Sp(T_n(K))$. Suite au Théorème 2.1.29 point 4 nous avons que $T_n(K)/\mathcal{M}$ est une extension finie de K contenue dans $\overline{K}$. Soit $\Gamma := Aut(\overline{K}/K)$ le groupe d'automorphismes de $\overline{K}$ sur K. Nous définissons :

$$\chi : B_1^n(\overline{K}) \to Sp(T_n(K));$$

$$\overline{z}_0 \mapsto \mathcal{M}_{\overline{z}_0} := \{f \in T_n(K), \ \ f(\overline{z}_0) = 0\}.$$

Suite à [BGR], Section 7.1.1, Proposition 1, page 260, nous savons que χ est surjective puisque tout idéal maximal $\mathcal{M} \in Sp(T_n(K))$ est tel qu'il induit un morphisme du type :

$$\varphi_{\mathcal{M}} : T_n(K) \to B_1^n(\overline{K});$$

$$f \mapsto [f]_{\mathcal{M}};$$

où $[f]_{\mathcal{M}}$ est la classe résiduelle de f modulo $\mathcal{M}$ dans $T_n(K)$, elle correspond donc à un point dans $B_1^n(\overline{K})$. Le noyau de $\varphi_{\mathcal{M}}$ est $\mathcal{M}$. En particulier, $\mathcal{M} = \mathcal{M}_{\overline{z}_0}$ où $\overline{z}_0 = (\varphi(z_1), ..., \varphi(z_n))$ et si $\mathcal{M} \in Sp(T_n(K))$ nous avons que $\chi^{-1}(\mathcal{M}) = \chi^{-1}(\mathcal{M}_{\overline{z}_0}) = Orb_\Gamma(\overline{z}_0)$. Autrement dit, χ induit une correspondance biunivoque entre $Sp(T_n(K))$ et les classes de conjugaison sur K des points de $B_1^n(\overline{K})$. Il s'ensuit que si K est algébriquement clos une telle correspondance biunivoque est valable entre $B_1^n(K)$ et $Sp(T_n(K))$. Dans le cas contraire nous avons que la restriction de χ à l'ensemble $B_1^n(K)$ des points $K-$rationnels de $B_1^n(\overline{K})$ est injective.

Si nous appelons :

$$Sp^*(T_n(K)) := \chi(B_1^n(K));$$

nous définissons :

$$X := Sp^*(T_n(K)/I) = \{\mathcal{M} \in Sp^*(T_n(K)), \ \ \mathcal{M} \supseteq I\}.$$

Comme nous l'avons remarqué χ induit un plongement des points $K-$rationnels de $B_1^n(\overline{K})$ dans $Sp(T_n(K))$, ce qui implique qu'il nous est possible d'identifier X avec un sous-ensemble $K-$analytique de $B_1^n(K)$.

Une version du Nullstellensatz dans le cas des espaces affinoïdes nous dit que :

$$\mathcal{I}(\widetilde{X}) := \bigcap_{\mathcal{M}\in Sp(T_n(K)),\ \mathcal{M}\supseteq I} \mathcal{M} = \sqrt{I};$$

où $\widetilde{X} = Sp(T_n(K)/I)$. Voir [BGR], Section 7.1.2, Theorem 3. Il s'ensuit que $\widetilde{X} = Sp(T_n(K)/\mathcal{I}(\widetilde{X}))$ et que $X = Sp^*(T_n(K)/\mathcal{I}(\widetilde{X}))$. Soit :

$$\mathcal{I}(X) := \mathcal{I}(\widetilde{X}).$$

Nous appelons également :

$$\mathcal{O}(X) := T_n(K)/\mathcal{I}(X).$$

Si $I \subset T_n(K)$ est un idéal dans $T_n(K)$ nous remarquons que :

$$Sp^*(T_n(K)/I) = Sp^*(T_n(K)/\mathcal{I}(X)).$$

Si en effet un idéal maximal contient un idéal il contient aussi l'idéal radical de ce dernier. Nous remarquons que nous ne sommes pas en condition de pouvoir associer de façon univoque un espace affinoïde à un sous-ensemble $K-$analytique dans $B_1^n(K)$. Deux espaces affinoïdes différents peuvent en effet s'intersecter dans les mêmes points $K-$rationnels dans $B_1^n(K)$ (qui correspondent aux idéaux maximaux contenus dans l'ensemble $\chi(B_1^n(K))$ que nous avons introduit avant). Nous donnons alors la définition suivante.

Définition 2.1.30. *Un **espace** $K-$**analytique** dans $B_1^n(K)$ est un couple (I,X) constitué d'un idéal $I \subseteq T_n(K)$ et de l'ensemble $K-$analytique X constitué du lieu des points dans $B_1^n(K)$ qui sont les zéros de tout système minimal de générateurs de I, à la relation d'équivalence suivante près :*

$$(I,X) \sim (I',X) \Longleftrightarrow \sqrt{I} = \sqrt{I'} \subseteq T_n(K).$$

*Soit (I,X) un espace $K-$analytique dans $B_1^n(K)$. Nous disons qu'un espace $K-$analytique (J,Y) dans $B_1^n(K)$ est un **sous-espace** $K-$**analytique** de (I,X) si et seulement si $Y \subseteq X$ et $J \supseteq I$.*

Nous remarquons qu'en général deux idéaux $I, I' \subseteq T_n(K)$ tels que $\sqrt{I} \neq \sqrt{I'}$ peuvent définir le même sous-ensemble $K-$analytique X dans $B_1^n(K)$ qui aura donc en principe des propriétés différentes (comme la dimension ou le lieu des points réguliers, que nous allons définir plus loin) en fonction de l'idéal $I \subseteq T_n(K)$ qu'on choisit pour le représenter. Nous construisons donc la bijection suivante entre la famille des espaces $K-$analytiques de $B_1^n(K)$ et celle des espaces affinoïdes sur K :

$$(I,X) \longleftrightarrow \widetilde{X};$$

où X est le sous-ensemble $K-$analytique dans $B_1^n(K)$ qui est lieu des zéros d'un idéal $I \subseteq T_n(K)$ tel que nous appelons $\mathcal{I}(X) := \sqrt{I}$ et $\widetilde{X}$ est l'espace affinoïde qu'on définit à partir de l'idéal $\mathcal{I}(\widetilde{X}) := \mathcal{I}(X)$ comme expliqué avant. Plus précisément, X et $\widetilde{X}$ sont définis à partir de l'idéal I comme il suit :

$$X = Sp^*(T_n(K)/I) = Sp^*(T_n(K)/\mathcal{I}(X)) \texttt{ et } \widetilde{X} = Sp(T_n(K)/I) = Sp(T_n(K)/\mathcal{I}(\widetilde{X})).$$

Comme des tels objets sont univoquement définis par l'idéal $\mathcal{I}(X) = \mathcal{I}(\widetilde{X})$ et comme les idéaux que nous traiterons dans la suite seront toujours sous une telle forme (idéaux radicaux des idéaux $I \subseteq T_n(K)$ qui définissent les ensembles $K-$analytiques auxquels nous serons intéressés) nous indiquerons directement avec la même lettre X l'espace $K-$analytique que nous associons à chaque sous-ensemble $K-$analytique de $B_1^n(K)$ puisque l'idéal I qui définit ce dernier sera toujours fixé au départ. De cette façon si $\widetilde{Y} \subseteq \widetilde{X}$ est un sous-espace affinoïde de $\widetilde{X}$ il correspondera biunivoquement à un idéal réduit $\mathcal{I}(\widetilde{Y}) \supseteq \mathcal{I}(\widetilde{X})$ tel que la restriction de $\widetilde{Y}$ à $B_1^n(K)$ soit l'ensemble $K-$analytique $Y = Sp^*(T_n(K)/\mathcal{I}(\widetilde{Y}))$ auquel on associe comme précédemment l'espace affinoïde $\widetilde{Y}$. Une fois choisie cette méthode d'attribution d'un espace affinoïde à un espace $K-$analytique dans $B_1^n(K)$ nous pouvons développer les calculs sur les espaces affinoïdes en utilisant les méthodes algébriques disponibles pour ces derniers en sachant toujours qu'ils correspondent aux espaces $K-$analytiques de $B_1^n(K)$ auxquels nous sommes finalement intéressés.

2.1.3 Notion de dimension locale

Soit maintenant $X \subset B_1^n(K)$ un espace $K-$analytique dans $B_1^n(K)$ auquel on associe comme expliqué avant l'espace affinoïde $\widetilde{X} = Sp(\mathcal{O}(X))$ tel que $X = B_1^n(K) \cap \widetilde{X}$. Nous disons que X est **irréductible** si $\mathcal{I}(X)$ est un idéal premier dans $T_n(K)$. Si X est le lieu des zéros dans K^n de $f_1, ..., f_s$ fonctions $K-$entières définies sur K^n et à valeurs dans K, nous avons que $f_1, ..., f_s \in T_n(K)$ en particulier. Nous appelons $\mathcal{I}(X) = \sqrt{(f_1, ..., f_r)} \subseteq T_n(K)$ et $\mathcal{O}(X) = T_n(K)/\mathcal{I}(X)$. Nous supposons que :

$$B_1^n(K) \cap X \neq \emptyset.$$

Il s'ensuit que :

$$X \cap B_1^n(K) = Sp^*(T_n(K)/(f_1, ..., f_s)) = Sp^*(\mathcal{O}(X)) \subset Sp(\mathcal{O}(X)).$$

Nous remarquons que puisque $T_n(K)$ est une algèbre Noethérienne $\mathcal{I}(X)$ n'est contenu que dans un nombre fini r d'idéaux premiers minimaux $P_1, ..., P_r$ dans $T_n(K)$. Nous appelons :

$$B_1^n(K) \cap X_i := Sp^*(T_n(K)/P_i) \subseteq B_1^n(K) \cap X, \ \ \forall i = 1, ..., r;$$

les **composantes irréductibles** de $B_1^n(K) \cap X$. Nous remarquons en particulier que l'analogue du Nullstellensatz Fort que nous avons énoncé pour les espaces affinoïdes nous permet d'associer biunivoquement les sous-espaces $K-$analytiques irréductibles de $B_1^n(K) \cap X$ aux idéaux premiers dans $T_n(K)$ qui contiennent $\mathcal{I}(X)$ puisque ceux-ci correspondent aux sous-espaces affinoïdes irréductibles de l'espace affinoïde $\widetilde{X}$ que nous avons associé à X comme expliqué avant. Si nous appelons **degré de liberté** d'un espace $K-$analytique X dans $B_1^n(K)$ la valeur de $d \in \mathbb{N}$ telle que $T_d(K)$ s'injecte comme expliqué dans le Théorème 2.1.29 point 3 dans $\mathcal{O}(X)$, celui-ci est en effet la dimension de Krull de l'algèbre de Tate $\mathcal{O}(X)$, que nous appelons $\dim(\mathcal{O}(X))$. Pour tout $\overline{z}_0 \in X$ nous appelons donc **dimension** de X en $\overline{z}_0$ la valeur suivante :

$$\dim_{\overline{z}_0}(X) := \dim(\mathcal{O}(X)_{\mathcal{M}_{\overline{z}_0}}).$$

Nous appelons aussi **dimension** de X la valeur suivante :

$$\dim(X) := \sup_{\overline{z}_0 \in X} \{\dim_{\overline{z}_0}(X)\}.$$

Remarque 2.1.31. *Si $X \subset B_1^n(K)$ est un espace $K-$analytique irréductible dans $B_1^n(K)$ et $\mathcal{M} \in Sp^*(\mathcal{O}(X))$, nous avons que :*

$$\dim(\mathcal{O}(X)) = \dim(\mathcal{O}(X)_{\mathcal{M}}).$$

Autrement dit, la dimension de X irréductible est la dimension locale en chaque point de X.

Démonstration. Grâce au Théorème 2.1.29 point 3, si $d = \dim(\mathcal{O}(X))$ alors nous avons que $\mathcal{O}(X)$ est une extension entière de $T_d(K)$. Nous remarquons que suite aux hypothèses $T_d(K)$ et $\mathcal{O}(X)$ sont des anneaux intègres et que $T_d(K)$ est aussi intégralement fermé dans son corps des fractions (c'est une conséquence immédiate du fait que $T_d(K)$ est un anneau factoriel, suite au Théorème 2.1.29 point 2). Nous savons par conséquent (voir [At-Mac], Lemma 11.26, page 125) que :

$$\dim(\mathcal{O}(X)_{\mathcal{M}}) = \dim(T_d(K)_{\mathcal{M}\cap T_d(K)}).$$

Comme le Théorème 2.1.29 nous dit que :

$$\dim(T_d(K)) = d;$$

nous pouvons nous ramener à montrer cette propriété dans le cas où $X = B_1^d(K)$ sans perte de généralité. Comme nous le savons il y a une correspondance biunivoque entre $Sp^*(T_d(K))$ et les points de $B_1^d(K)$. Soit $\overline{z}_0 \in B_1^d(K)$ le point correspondant à l'idéal maximal $\mathcal{M} \in Sp^*(T_d(K))$. A une translation près nous pouvons donc supposer que $\overline{z}_0 = \overline{0}$ et que :

$$\mathcal{M} = (z_1, ..., z_d).$$

On voit maintenant que :

$$\dim(T_d(K)_{\mathcal{M}}) = d.$$

En effet les idéaux premiers de $T_d(K)_{\mathcal{M}}$ sont en correspondance biunivoque avec ceux de $T_d(K)$ qui sont contenus dans $\mathcal{M}$. Ce qui montre que :

$$\dim(T_d(K)_{\mathcal{M}}) \leq \dim(T_d(K)).$$

D'un autre côté la chaîne d'idéaux premiers suivants :

$$(z_1, ..., z_d) \supset (z_1, ..., z_{d-1}) \supset ... \supset (z_1);$$

nous montre que $d \leq \dim(T_d(K)_{\mathcal{M}})$ puisqu'ils sont tous contenus dans $\mathcal{M}$. Comme nous savons que $d = \dim(T_d(K))$ suite au Théorème 2.1.29 point 2 il s'ensuit que :

$$\dim(T_d(K)) \leq \dim(T_d(K)_{\mathcal{M}}).$$

□

Soit maintenant un espace affinoïde $\widetilde{X}$ défini sur K. Soit $\mathcal{O}(\widetilde{X}) = T_n(K)/I$ l'algèbre de Tate qu'on lui associe. Tout idéal maximal $\mathcal{M} \in \widetilde{X} = Sp(\mathcal{O}(\widetilde{X}))$ correspond à un idéal maximal de $T_n(K)$ qui contient I. Soit $f \in T_n(K)$. Nous définissons $f(\mathcal{M}) \in \overline{K}$ en tant que la classe de reste modulo $\mathcal{M}$ de f dans $T_n(K)/\mathcal{M}$, qui est une extension finie de K contenue dans $\overline{K}$.

Définition 2.1.32. *Soit $\widetilde{X}$ un espace affinoïde défini sur K. Nous considérons la famille des **ensembles rationnels** $U \subseteq \widetilde{X}$, donnée dans [V-P], telle que pour chaque élément U d'une telle famille il existe $s \in \mathbb{N}$, $f_0, ..., f_s \in \mathcal{O}(\widetilde{X})$ tels que $(f_0, ..., f_s) = \mathcal{O}(\widetilde{X})$, pour lesquels on a que :*

$$U = R_{\widetilde{X}}(f_0, ..., f_s) := \{\mathcal{M} \in \widetilde{X}, |f_0(\mathcal{M})|_{1/T} \geq |f_i(\mathcal{M})|_{1/T}, \ \forall i = 1, ..., s\}.$$

*Nous disons aussi qu'un recouvrement d'un tel U est **admissible** s'il est un recouvrement d'ensembles rationnels dans U (qu'on peut montrer être aussi des rationnels dans $\widetilde{X}$, voir [V-F], Lemma 4.1.3) tel qu'il admet un sous-recouvrement fini. Dans le même travail il est montré que cette famille de sous-ensembles de $\widetilde{X}$ munie des tels recouvrements est une **G-topologie** (ou **topologie de Grothendieck**) (voir [V-F], Lemma 4.1.3) que nous appelons $\mathcal{G}$, ce qui permet de construire le préfaisceau :*

$$U \mapsto \mathcal{O}(U) := \mathcal{O}(\widetilde{X}) \ll z_{n+1}, ..., z_{n+s} \gg /(f_1 - z_{n+1}f_0, ..., f_s - z_{n+s}f_0);$$

*des **fonctions analytiques** ou **régulières** sur U. Un Théorème du à J. Tate (voir [V-F], Theorem 4.2.2) permet de montrer que ce préfaisceau est en effet un faisceau. Nous appellons $(\widetilde{X}, \mathcal{G}, \mathcal{O}_{\widetilde{X}})$ un **espace analytique rigide** muni du faisceau $\mathcal{O}_{\widetilde{X}}$ de fonctions régulières sur la G-topologie $\mathcal{G}$. Pour tout $\overline{z} \in \widetilde{X}$ nous appelons $\mathcal{O}_{\widetilde{X},\overline{z}}$ l'anneau des germes des fonctions analytiques associé à $\mathcal{O}_{\widetilde{X}}$ en $\overline{z}$. Nous remarquons qu'un tel anneau est local et que son unique idéal maximal est constitué des classes d'équivalence de suites compatibles dans $\lim_{\rightarrow (U \ni x)} \mathcal{O}(U)$ ultimement nulles en $\overline{z}$ (voir [V-F], Definition 4.5.6). Nous appelons **dimension** de $\widetilde{X}$ en $\overline{z}$ la valeur suivante :*

$$\dim_{\overline{z}}(\widetilde{X}) := \dim(\mathcal{O}_{\widetilde{X},\overline{z}}).$$

Nous appelons aussi :

$$\dim(\widetilde{X}) := \sup_{\overline{z} \in X}\{\dim_{\overline{z}}(\widetilde{X})\}.$$

Nous remarquons que si X est l'espace $K-$analytique de $B_1^n(K)$ qu'on associe à $\widetilde{X}$ comme expliqué avant nous obtenons que :

$$\dim_{\overline{z}}(\widetilde{X}) = \dim_{\overline{z}}(X), \ \forall \overline{z} \in X.$$

On a donc pour K général et $L \subseteq K$ un sous-corps de K les inclusions suivantes de familles :

$$\{\texttt{Sous-variétés } L-\texttt{algébriques dans } K^n\} \subset$$

$$\subset \{\texttt{Sous-ensembles } L-\texttt{entiers dans } K^n\} \subset$$

$$\subset \{\texttt{Sous-espaces } L-\texttt{analytiques dans } K^n\} \subset$$

$$\subset \{\texttt{Points } K-\texttt{rationnels d'un espace analytique rigide défini sur } L\}.$$

Dans les raisonnements qui suivent nous nous proposons d'adapter à notre situation un Théorème connu en Géométrie Algébrique qui met en relation la notion de dimension locale d'une variété en un point choisi (vue comme la dimension de l'espace tangent la variété en ce point, espace qui est le noyau de la matrice Jacobienne associée à la variété en ce point) avec la dimension de Krull de l'anneau des fonctions régulières localisé en ce point. Un analogue de ce résultat est déjà connu pour des espace affinoïdes définis sur un corps séparable (voir [V-F], Theorem 3.6.3).

Soit A un anneau Noethérien local et soit $\mathcal{M}$ son unique idéal maximal. On dit qu'il est **régulier** si :

$$[\mathcal{M}/\mathcal{M}^2 : A/\mathcal{M}] = \dim(A).$$

Soit $X \subset B_1^n(K)$ un espace $K-$analytique. Si $\mathcal{O}(X) = T_n(K)/\mathcal{I}(X)$ où $\mathcal{I}(X) = (f_1, ..., f_s)$ nous définissons aussi le $\mathcal{O}(X)-$module suivant des formes différentielles divisées :

$$\Omega_{\mathcal{O}(X)/K} := \mathcal{O}(X) \otimes_{T_n(K)} (\sum_{i=1}^{n} T_n(K) dz_i / \sum_{i=1}^{s} T_n(K) df_i);$$

où la différentielle divisée en $z_1, ..., z_n$ est celle qui est induite par la dérivée divisée. Si $\mathcal{M} \in Sp(\mathcal{O}(X))$ est associé à un point $\overline{z}_0 \in X$ nous appellons **espace cotangent** X en $\overline{z}_0$ le $\mathcal{O}(X)_{\mathcal{M}}/\mathcal{M}_{\mathcal{M}}-$espace vectoriel $\mathcal{M}_{\mathcal{M}}/\mathcal{M}_{\mathcal{M}}^2$. Comme $T_n(K)$ est un anneau Noethérien, $\mathcal{M}_{\mathcal{M}}$ est un $\mathcal{O}(X)_{\mathcal{M}}-$module de type fini. Le Lemme de Nakayama nous montre par conséquent que :

$$\dim_{\mathcal{O}(X)_{\mathcal{M}}/\mathcal{M}_{\mathcal{M}}}(\mathcal{M}_{\mathcal{M}}/\mathcal{M}_{\mathcal{M}}^2) \geq \dim(\mathcal{O}(X)_{\mathcal{M}}). \tag{2.6}$$

Ce Lemme (voir [At-Mac], page 21) appliqué au $\mathcal{O}(X)_{\mathcal{M}}-$module de type fini $\mathcal{M}_{\mathcal{M}}$, vu aussi en tant qu'idéal dans $\mathcal{O}(X)_{\mathcal{M}}$ (contenu dans le radical de Jacobson comme cet anneau est local) et au sous-$\mathcal{O}(X)_{\mathcal{M}}-$module de $\mathcal{M}_{\mathcal{M}}$ constitué des représentants des éléments d'une $\mathcal{O}(X)_{\mathcal{M}}/\mathcal{M}_{\mathcal{M}}-$base de $\mathcal{M}_{\mathcal{M}}/\mathcal{M}_{\mathcal{M}}^2$ implique en effet que :

$$\dim_{\mathcal{O}(X)_{\mathcal{M}}/\mathcal{M}_{\mathcal{M}}}(\mathcal{M}_{\mathcal{M}}/\mathcal{M}_{\mathcal{M}}^2) = \min\{i \in \mathbb{N}, \ \ \mathcal{M}_{\mathcal{M}} = (f_1, ..., f_i), \ \ f_1, ..., f_i \in \mathcal{O}(X)_{\mathcal{M}}\};$$

alors que les propriétés classiques de l'Algèbre Commutative (voir [Ash], Chapter 5, Proposition 5.4.1) nous montrent que :

$$\dim(\mathcal{O}(X)_{\mathcal{M}}) = \min\{i \in \mathbb{N}, \ \ \mathcal{M}_{\mathcal{M}} = \sqrt{(f_1, ..., f_i)}, \ \ f_1, ..., f_i \in \mathcal{O}(X)_{\mathcal{M}}\};$$

puisque $\mathcal{O}(X)_{\mathcal{M}}$ est un anneau Noethérien local.

Théorème 2.1.33. *Soit $X \subset B_1^n(K)$ un ensemble $K-$analytique, où K est un corps de valuation non-archimédienne complet et parfait qui est contenu dans $\mathcal{C}$. Soit $\mathcal{M} = \mathcal{M}_{\overline{z}_0} \in Sp^*(T_n(K))$ idéal maximal contenant $\mathcal{I}(X)$ associé au point $\overline{z}_0 \in X$ comme expliqué avant. Les propriétés suivantes sont équivalentes.*

1. *L'anneau local $\mathcal{O}(X)_{\mathcal{M}_{\overline{z}_0}}$ est régulier.*
2. *$[\Omega_{\mathcal{O}(X)/K}/\mathcal{M}\Omega_{\mathcal{O}(X)/K} : \mathcal{O}(X)/\mathcal{M}] = \dim(\mathcal{O}(X)_{\mathcal{M}})$.*
3. *La matrice Jacobienne $J_{\overline{z}_0}(\mathcal{I}(X))$ qu'on construit en $\overline{z}_0$ à partir des générateurs $f_1, ..., f_s$ de $\mathcal{I}(X)$ que nous regardons en tant que fonctions en n variables $z_1, ..., z_n$ a un rang[2] qui est $n - \dim(\mathcal{O}(X)_{\mathcal{M}_{\overline{z}_0}})$.*

2. Nous remarquons que suite aux règles de la dérivation divisée d'une composition de fonctions analytiques il est facile de voir que la matrice Jacobienne en $\overline{z}_0$ qu'on construit à partir d'un système de générateurs du même idéal $\mathcal{I}(X)$ a un rang qui est indépendant du choix d'un tel système.

Démonstration. Voir [V-F] Theorem 3.6.3. □

Soit X un sous-ensemble $K-$entier contenu dans K^n tel que $B_1^n(K) \cap X$ est un espace affinoïde irréductible sur K, où K est un corps comme dans les hypothèses du Théorème 2.1.33. Si $\mathcal{I}(X)$ est engendré par un système minimal de r générateurs nous avons que :

$$r \geq n - \dim(B_1^n(K) \cap X).$$

En effet suite au Théorème 2.1.29 point 3 $\dim(B_1^n(K) \cap X)$ est le degré de liberté de $B_1^n(K) \cap X$, ce qui signifie que $\dim(B_1^n(K) \cap X) \geq n - r$. Suite au Théorème 2.1.33 nous avons que :

$$\rho(J_{\overline{z}_0}(\mathcal{I}(X))) \leq n - \dim(B_1^n(K) \cap X) \leq r, \ \ \forall \overline{z}_0 \in B_1^n(K) \cap X.$$

(Nous disons que $B_1^n(K) \cap X$ est une **intersection complète** si $r = n - \dim(B_1^n(K) \cap X)$).

Nous supposons par la suite que K ne soit pas un corps parfait. Soit X un sous-espace $K-$analytique contenu dans $B_1^n(K)$. Nous définissons le lieu des **points réguliers** de X l'ensemble suivant :

$$X_{reg.} := \{\overline{z}_0 \in X, \ \ \rho(J_{\overline{z}_0}(\mathcal{I}(X))) = n - \dim(\mathcal{O}(X)_{\mathcal{M}_{\overline{z}_0}})\}.$$

Nous définissons d'un autre côté le lieu des **points singuliers** de X comme il suit :

$$X_{sing.} := X \setminus X_{reg.}.$$

Nous remarquons que la définition qu'on donne généralement des points réguliers d'un espace analytique rigide (qui dans notre situation est celui qu'on associe à l'espace affinoïde $\widetilde{X}$ défini par $\mathcal{I}(X)$) est la suivante :

$$\widetilde{X}_{reg.} := \{\overline{z}_0 \in \widetilde{X}, \ \ \rho(J_{\overline{z}_0}(\mathcal{I}(X))) = n - \dim(\mathcal{O}_{\widetilde{X},\overline{z}_0})\}.$$

Cette définition appliquée aux points $K-$rationnels de $\widetilde{X}$ n'est pas en contradition avec celle qui précède puisqu'on peut montrer (voir [V-F], Proposition 4.6.1) que :

$$\widehat{\mathcal{O}_{\widetilde{X},\overline{z}_0}} \simeq \widehat{\mathcal{O}(X)_{\mathcal{M}_{\overline{z}_0}}};$$

où pour tout anneau local et Noethérien R nous désignons par $\widehat{R}$ son complété par rapport à son unique idéal maximal, et suite à [At-Mac], Corollary 11.19, pour tout tel R nous avons que $\dim(R) = \dim(\widehat{R})$.

Remarque 2.1.34. *Il est très important de remarquer qu'on ne peut pas donner une définition de dimension globale ou de point régulier pour un ensemble $K-$entier X contenu dans K^n. L'algèbre des fonctions $K-$entières de la forme $f : K^n \to K$ n'est pas Noethérienne en général et il nous est impossible d'associer à X un idéal $\mathcal{I}(X)$ comme nous avons fait avant pour le sous-ensemble $K-$analytique $B_1^n(K) \cap X$ dans $B_1^n(K)$ qui nous permette de répéter sur X les mêmes raisonnements que nous avons développés pour $B_1^n(K) \cap X$. Comme nous l'avons déjà remarqué précédemment la nature non-archimédienne de la topologie induite sur K^n par la valeur absolue $1/T-$adique ne permet pas la construction d'un faisceau sur K^n en utilisant les fonctions $K-$analytiques sur* *les ouverts U de K^n, ce qui nous oblige à étudier localement les propriétés de X en regardant chaque intersection de ce dernier avec un polydisque de rayon 1 dans K^n en tant qu'espace $K-$analytique après lui avoir donné un idéal dans $T_n(K)$ comme expliqué avant. Chacun de ces espaces $K-$analytiques construits à partir des sous-ensembles $K-$analytiques de X que nous avons défini ici n'a aucune relation avec les autres et il peut avoir des propriétés très différentes.*

2.1.4 Densité des points réguliers

Définition 2.1.35. *Soit $K_1 \subset K_2$ une extension de corps. Soit X un espace affinoïde irréductible dans $B_1^n(K_1)$. Nous disons qu'il est **absolument irréductible** dans K_2 si l'idéal premier $\mathcal{I}(X)$ dans $T_n(K_1)$ associé à X comme il suit :*

$$\mathcal{I}(X) := \{f \in T_n(K_1),\ \ f(\overline{z}) = 0,\ \ \forall \overline{z} \in X\};$$

est tel que l'idéal $\mathcal{I}(X)T_n(K_2)$ dans $T_n(K_2)$ est encore premier.

Nous remarquons que si K_2 est une extension algébrique de K_1 tout espace affinoïde irréductible X dans $B_1^n(K_1)$ se décompose en un nombre fini de composantes absolument irréductibles dans K_2 quitte à remplacer K_1 par une extension finie dans K_2.

Théorème 2.1.36. *Soit X un espace affinoïde dans $B_1^n(K)$, où K est un corps de valuation $1/T-$adique complet. Nous supposons que X soit absolument irréductible dans la clôture parfaite de K dans $\mathcal{C}$, que nous appelons $\mathbb{K}$. Les points réguliers de X sont denses dans X par rapport à la topologie induite par la valeur absolue $1/T-$adique.*

Démonstration. Nous montrons d'abord le Théorème en supposant que $K = \mathbb{K}$. Suite à la Remarque 2.1.31 nous avons que :

$$\dim_{\overline{z}}(X) = \dim(X);$$

pour tout $\overline{z} \in X$, puisque X est irréductible. Nous avons par conséquent que :

$$\overline{z} \in X_{sing.} \iff \rho(J_{\overline{z}}(\mathcal{I}(X))) < n - \dim(X).$$

Une telle condition est équivalente à dire que tous les mineurs d'ordre $n-\dim(X)$ de $J_{\overline{z}}(\mathcal{I}(X))$ sont nuls. Comme $\dim(X)$ ne dépend pas du point $\overline{z} \in X$ une telle condition est équivalente à demander que $\overline{z}$ soit contenu dans le sous-espace $K-$analytique de X qu'on définit en ajoutant au système minimal de générateurs choisi de $\mathcal{I}(X)$ la condition d'annulation des mineurs de $J_{\overline{z}}(\mathcal{I}(X))$ que nous avons donné avant. Il s'ensuit que $X_{sing.}$ est un sous-espace affinoïde de X. Nous montrons que cette inclusion est stricte. Soit $d := \dim(X)$. Le Théorème 2.1.29 implique qu'il existe un plongement entier comme il suit :

$$T_d(\mathbb{K}) \hookrightarrow T_n(\mathbb{K})/\mathcal{I}(X) = \mathcal{O}(X).$$

Ce qui veut dire que $T_d(\mathbb{K}) \subset \mathcal{O}(X)$ est une extension entière d'anneaux. Suite à [At-Mac] Corollary 5.8 cela induit un morphisme de restriction surjectif et fini sur les spectres maximaux de la forme suivante :

$$f : Sp^*(\mathcal{O}(X)) = X \twoheadrightarrow B_1^d(\mathbb{K}).$$

Suite au Théorème 2.1.33 et comme $\mathbb{K}$ est un corps parfait nous pouvons dire que les points $\overline{z}_0 \in X_{reg.}$ correspondent aux idéaux maximaux $\mathcal{M}_{\overline{z}_0} \in Sp^*(\mathcal{O}(X))$ tels que :

$$[\mathcal{M}_{\overline{z}_0 \mathcal{M}_{\overline{z}_0}}/\mathcal{M}^2_{\overline{z}_0 \mathcal{M}_{\overline{z}_0}} : \mathcal{O}(X)_{\mathcal{M}_{\overline{z}_0}}/\mathcal{M}_{\overline{z}_0 \mathcal{M}_{\overline{z}_0}}] = d.$$

On peut montrer (voir [Col-Maz] Lemma 1.2.2) que cela implique que $X_{sing.}$ est contenu dans l'ensemble des points de ramification de f. Soit en effet $\mathcal{I}(X) = (f_1, ..., f_r) \subset T_n(\mathbb{K})$ et soit $\mathcal{M}_{\overline{z}_0} \in Sp^*(\mathcal{O}(X))$ un idéal maximal dont la restriction à $T_d(\mathbb{K})$ correspond au point $\overline{z}_0^* := (z_{0,1}, ..., z_{0,d}) \in B_1^d(\mathbb{K})$. Il correspond donc à un point $\overline{z}_0 \in X \subset B_1^n(\mathbb{K})$ qui est une racine $\mathbb{K}-$rationnelle du système d'équations suivantes :

$$\begin{cases} f_1(\overline{z}) = 0 \\ \quad \cdots \\ f_r(\overline{z}) = 0 \\ z_1 = z_{0,1} \\ \quad \cdots \\ z_d = z_{0,d} \end{cases}$$

Soit $m_{\overline{z}_0^*} \in Sp(T_d(\mathbb{K}))$ l'idéal maximal dans $T_d(\mathbb{K})$ associé au point $\overline{z}_0^*$. Il s'ensuit que :

$$\mathcal{O}(X)_{\mathcal{M}_{\overline{z}_0}}/\mathcal{M}_{\overline{z}_0 \mathcal{M}_{\overline{z}_0}} = \mathbb{K} \ll \overline{z}_0 \gg = \mathbb{K} = \mathbb{K} \ll \overline{z}_0^* \gg = T_d(\mathbb{K})_{m_{\overline{z}_0^*}}/m_{\overline{z}_0^* m_{\overline{z}_0^*}};$$

puisque $\overline{z}_0$ et $\overline{z}_0^*$ sont des points $\mathbb{K}-$rationnels. D'un autre côté $B_1^d(\mathbb{K})$ est tel que tous ses points sont réguliers, donc $\overline{z}_0^*$ l'est aussi. Il s'ensuit que $\overline{z}_0$ est un point de ramification au dessus de $\overline{z}_0^*$ si et seulement si :

$$[\mathcal{M}_{\overline{z}_0 \mathcal{M}_{\overline{z}_0}}/\mathcal{M}^2_{\overline{z}_0 \mathcal{M}_{\overline{z}_0}} : \mathbb{K}] > [m_{\overline{z}_0^* m_{\overline{z}_0^*}}/m^2_{\overline{z}_0^* m_{\overline{z}_0^*}} : \mathbb{K}] = d.$$

La dimension de l'espace cotangent qu'on associe à $T_d(\mathbb{K})$ en $\overline{z}_0^*$ est en effet d suite au Théorème 2.1.33 puisque $\mathbb{K}$ est un corps parfait et comme nous l'avons remarqué précédemment $B_1^d(\mathbb{K})$ est un espace affinoïde qui ne contient pas de points singuliers. Nous considérons le morphisme de restriction induit sur les spectres suivant :

$$g : Spec\ \mathcal{O}(X) \twoheadrightarrow Spec\ T_d(\mathbb{K}).$$

L'idéal premier 0 de $T_d(\mathbb{K})$ correspond au point générique η de $B_1^d(\mathbb{K})$ (voir [Hart] Example 2.3.3). Ce morphisme restreint à $g^{-1}(\eta)$ induit un morphisme fini sur les anneaux localisés en 0 qui correspond à une extension finie de corps comme $\mathcal{O}(X)$ est un anneau intègre et donc 0 est un idéal premier de ce dernier. En effet $T_d(\mathbb{K})_\eta = T_d(\mathbb{K})_0$ est le corps de fractions de $T_d(\mathbb{K})$ et $\mathcal{O}(X)_\eta = \mathcal{O}(X)_0$ celui de $\mathcal{O}(X)$. Nous appelons ces deux corps :

$$\mathbb{K}\{\{z_1, ..., z_d\}\} := T_d(\mathbb{K})_0;$$

$$\mathbb{K}(X) := \mathcal{O}(X)_0.$$

Nous montrons qu'une telle extension de corps :

$$\mathbb{K}\{\{z_1, ..., z_d\}\} \subseteq \mathbb{K}(X);$$

est séparable. Nous savons suite au Théorème 2.1.29 point 3 qu'il existe $n - d$ éléments $z_{d+1}, ..., z_n \in \mathbb{K}(X)$ qui engendrent l'extension des corps $\mathbb{K}\{\{z_1, ..., z_d\}\} \subseteq$

$\mathbb{K}(X) = \mathbb{K}\{\{z_1, ..., z_d, z_{d+1}, ..., z_n\}\}$. Comme z_{d+1} est algébrique sur $\mathbb{K}\{\{z_1, ..., z_d\}\}$ il existe un polynôme irréductible $F(X) \in \mathbb{K}\{\{z_1, ..., z_d\}\}[X] \setminus \{0\}$ tel que :

$$F(z_{d+1}) = 0.$$

Il existe donc un élément $f \in T_{d+1}(\mathbb{K}) \setminus \{0\}$ irréductible tel que :

$$f(z_1, ..., z_d, z_{d+1}) = 0.$$

Il doit alors exister au moins une variable z_j, pour un j compris entre 1 et $d+1$, telle que la dérivée partielle divisée de $f(z_1, ..., z_{d+1})$ en z_j n'est pas 0. Dans le cas contraire, puisque $\mathbb{K}$ est un corps parfait on a en effet l'existence d'un nombre $s \in \mathbb{N} \setminus \{0\}$ et un élément $g(z_1, ..., z_{d+1}) \in T_{d+1}(\mathbb{K}) \setminus \{0\}$ tels que :

$$f(z_1, ..., z_{d+1}) = g(z_1, ..., z_{d+1})^{p^s}.$$

Ce qui est en contradition avec l'hypothèse que $f(z_1, ..., z_{d+1})$ est irréductible. Comme la variable z_j apparaît sans doute dans l'expression de $f(z_1, ..., z_{d+1})$ il s'ensuit que les éléments $z_1, ..., z_{j-1}, z_{j+1}, ..., z_{d+1}$ sont libres sur $\mathbb{K}$. Ce qui veut dire que $\mathbb{K} \ll z_1, ..., z_{j-1}, z_{j+1}, ..., z_{d+1} \gg = T_d(\mathbb{K})$. En effet z_j n'est pas libre sur $\mathbb{K}\{\{z_1, ..., z_{j-1}, z_{j+1}, ..., z_{d+1}\}\}$ et si ces éléments $z_1, ..., z_{j-1}, z_{j+1}, ..., z_{d+1}$ n'étaient pas libres sur $\mathbb{K}$ on en déduirait que le corps $\mathbb{K}\{\{z_1, ..., z_{d+1}\}\}$ a un degré de liberté sur $\mathbb{K}$ strictement inférieur à d, ce qui est en contradition avec les hypothèses sur X. Comme :

$$\mathbb{K}\{\{z_1, ..., z_{j-1}, z_{j+1}, ..., z_{d+1}\}\}(z_j) = \mathbb{K}\{\{z_1, ..., z_d\}\}(z_{d+1});$$

nous pouvons modifier le choix au début des d éléments $\mathbb{K}-$algébriquement indépendants parmi les générateurs $z_1, ..., z_n$ de $\mathbb{K}(X)$ sur $\mathbb{K}$. Le Théorème 2.1.29 point 3 n'oblige pas en effet à un choix univoque. Nous avons que $\mathbb{K}(X)$ est une extension finie de $\mathbb{K}\{\{z_1, ..., z_{j-1}, z_{j+1}, ..., z_{d+1}\}\}$. Nous changeons donc éventuellement la numérotation de ces générateurs pour remplacer z_j par z_{d+1} sans perdre en généralité. Il s'ensuit finalement que z_{d+1} est séparable sur $\mathbb{K}\{\{z_1, ..., z_d\}\}$ comme le polynôme minimal $f(X_1, ..., X_{d+1})$ qu'on lui associe était séparable en X_j (et donc, avec le changement de numérotation qui nous a fait remplacer z_j avec z_{d+1}, il est maintenant séparable en X_{d+1}). Maintenant z_{d+2} est algébrique sur $\mathbb{K}\{\{z_1, ..., z_d\}\}$ lui aussi. Avec les mêmes raisonnements nous montrons que nous pouvons supposer sans perte de généralité qu'il soit lui aussi séparable sur $\mathbb{K}\{\{z_1, ..., z_d\}\}$. En répétant le même raisonnement pour $z_{d+3}, ..., z_n$ nous pouvons finalement dire sans perte de généralité que l'extension des corps :

$$\mathbb{K}\{\{z_1, ..., z_d\}\} \subseteq \mathbb{K}(X);$$

est donc séparable.

Une telle extension des corps admet donc un idéal discriminant qui est engendré par celui de l'extension des corps correspondante et qui ne peut pas être 0. Il s'ensuit que $X_{sing.}$ est un sous-espace affinoïde strict de X. Par conséquent $\dim(X_{sing.}) < \dim(X)$. Nous supposons maintenant que X soit défini sur K et nous considérons l'espace affinoïde $X(K)$ dans K^n. Si ce dernier est irréductible nous avons que :

$$\dim_K(X(K)) = \dim_{\mathbb{K}}(X).$$

Soit en effet $\mathcal{I}(X(K)) \subset T_n(K)$ l'idéal associé à $X(K)$. Comme l'extension d'anneaux suivante :
$$T_n(K) \subset T_n(\mathbb{K});$$
est entière et $\mathcal{I}(X(K))$ est un idéal premier dans $T_n(K)$ il s'ensuit que :
$$\mathcal{I}(X(K)) = (\mathcal{I}(X(K))T_n(\mathbb{K})) \cap T_n(K);$$
voir [At-Mac] Theorem 5.10. Nous pouvons donc construire un plongement naturel de la forme suivante :
$$T_n(K)/\mathcal{I}(X(K)) \hookrightarrow T_n(\mathbb{K})/\mathcal{I}(X(K))T_n(\mathbb{K}).$$
Une telle injection est encore un morphisme entier comme on peut le remarquer. Les propriétés des extensions entières d'anneaux impliquent donc que :
$$\dim_K(T_n(K)/\mathcal{I}(X(K))) = \dim_{\mathbb{K}}(T_n(\mathbb{K})/\mathcal{I}(X(K))T_n(\mathbb{K}));$$
(voir [At-Mac] Corollary 5.9 et Theorem 5.11). La version du Nullstellensatz Fort pour les espaces affinoïdes implique maintenant que :
$$\dim_{\mathbb{K}}(T_n(\mathbb{K})/\mathcal{I}(X(K))T_n(\mathbb{K})) = \dim_{\mathbb{K}}(T_n(K)/\mathcal{I}(X));$$
ce qui implique l'égalité des dimensions des deux espaces affinoïdes. Nous remarquons en particulier avec les mêmes raisonnements que :
$$\dim_K(X'(K)) = \dim_{\mathbb{K}}(X');$$
pour tout sous-espace affinoïde irréductible X' de X. Nous supposons maintenant que $X(K)$ est absolument irréductible dans $\mathbb{K}$. Soit X l'espace affinoïde contenu dans $\mathbb{K}^n$ défini sur K par les générateurs de l'idéal $\mathcal{I}(X(K))$ que nous avons précédemment introduit et soit $\mathcal{I}(X)$ celui qui est associé à X comme expliqué avant. Comme $X(K)$ est absolument irréductible dans $\mathbb{K}$ l'idéal $\mathcal{I}(X(K))T_n(\mathbb{K})$ est encore un idéal premier dans $T_n(\mathbb{K})$. En particulier nous avons que :
$$\mathcal{I}(X) = \mathcal{I}(X(K))T_n(\mathbb{K}).$$
Il s'ensuit qu'en tout point $\overline{z}_0 \in X(K)$ la matrice Jacobienne $J_{\overline{z}_0}(\mathcal{I}(X(K)))$ de $X(K)$ en $\overline{z}_0$ est aussi la matrice Jacobienne $J_{\overline{z}_0}(\mathcal{I}(X))$ de X. En particulier :
$$\rho_K(J_{\overline{z}_0}(\mathcal{I}(X(K)))) \geq \rho_{\mathbb{K}}(J_{\overline{z}_0}(\mathcal{I}(X))), \ \ \forall \overline{z}_0 \in X(K);$$
ce qui implique que :
$$X(K)_{sing.} = X_{sing.}(K).$$
En effet il s'agit des mêmes points dans $X(K)$ tels qu'ils respectent les mêmes équations algébriques induites sur K^n par l'annulation des mineurs d'ordre $n - \dim(X)$ de la même matrice Jacobienne. On peut avoir des points $\overline{z}_0 \in X(K)$ tels que le rang de $J_{\overline{z}_0}(\mathcal{I}(X(K)))$ sur K est strictement plus grand que celui sur $\mathbb{K}$ mais les générateurs minimaux de $\mathcal{I}(X(K))$ ne restent pas forcément minimaux dans $\mathbb{K}[X_1, ..., X_n]$ ce qui impliquerait si cela n'est pas le cas que le nombre des lignes de la matrice $J_{\overline{z}_0}(\mathcal{I}(X))$ construite comme expliqué avant est $> n - \dim(X)$. Les raisonnements précédents nous permettent maintenant de dire que :
$$\dim_K(X(K)_{sing.}) = \dim_K(X_{sing.}(K)) = \dim_{\mathbb{K}}(X_{sing.}) < \dim_{\mathbb{K}}(X) = \dim_K(X(K)).$$
□

2.1.5 Etude sur l'espace tangent

Dans cette dernière sous-section des préliminaires nous allons utiliser les notions introduites précédemment pour parvenir aux conclusions fondamentales qui nous permettent d'appliquer (au niveau de l'espace tangent $Lie(\mathcal{A})$ d'un $T-$module $\mathcal{A}$ respectant les hypothèses que nous expliquerons dans la section suivante) la méthode de J. Pila et J. Wilkie à notre situation spécifique.

Lemme 2.1.37. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module abélien et uniformisable de dimension m et de rang d défini sur le corps $\mathcal{F} \subset \overline{k}$. La fonction exponentielle $\overline{e}$ définie sur $\mathcal{A}$, de réseau Λ, induit alors les isomorphismes suivants de $A-$modules :*

$$\mathcal{A}(\mathcal{C}) \simeq \mathcal{C}^m/\Lambda \simeq (k_\infty/A)^d \oplus Lib;$$

où Lib est la partie libre de $\mathcal{C}^m/\Lambda$ en tant que $k_\infty-$espace.

Démonstration. L'exponentielle est un morphisme surjectif de groupes additifs de $\mathcal{C}^m$ vers $\mathcal{A}$ dont le noyau est Λ. Le Lemme de Factorisation nous donne alors l'isomorphisme de groupes :

$$\mathcal{A}(\mathcal{C}) \simeq \mathcal{C}^m/\Lambda;$$

qu'on vérifie facilement être aussi un isomorphisme de $A-$modules. D'un autre coté $\mathcal{C}^m$ est un $k_\infty-$espace de dimension infinie et son quotient par Λ est la somme directe d'une partie de torsion de dimension d avec une partie libre de dimension infinie. Si, donc, $\overline{z} \in Lie(\mathcal{A}) \simeq \mathcal{C}^m$, on aura :

$$\overline{z} = (z_1, ..., z_d, z') \in \bigoplus_{i=1}^{d} \overline{\omega}_i k_\infty \oplus Lib;$$

où $\Lambda =< \overline{\omega}_1, ..., \overline{\omega}_d >_A$. Comme les périodes $\overline{\omega}_1, ..., \overline{\omega}_d$ sont $k_\infty-$linéairement indépendantes on peut les choisir en tant que base sur k_∞ du sous-espace de torsion en les complétant à une base de $\mathcal{C}^m$ sur k_∞. Quitte à choisir de façon arbitraire un tel complété, nous construisons donc un isomorphisme :

$$\phi : \mathcal{C}^m \to \mathcal{C}^m;$$

de $k_\infty-$espaces vectoriels de dimension infinie qui fixe la base de $Lib.$ et il est tel que :

$$\phi(\overline{\omega}_i) := \overline{v}_i;$$

pour tout $i = 1, ..., d$, où $\overline{v}_1, ..., \overline{v}_d$ sont les vecteurs de la base canonique de k_∞^d. Autrement dit l'isomorphisme ϕ agit comme il suit :

$$\phi : \bigoplus_{i=1}^{d} k_\infty \overline{\omega}_i \oplus Lib. \to k_\infty^d \oplus Lib.$$

L'homomorphisme $\pi_{A^d} : k_\infty^d \oplus Lib. \twoheadrightarrow (k_\infty/A)^d \times \{0\}$ quotient de $k_\infty^d \oplus Lib.$ par $A^d \times \{\overline{0}\}$ induit la composition d'homomorphismes suivante :

$$\pi_{A^d} \circ \phi : \bigoplus_{i=1}^{d} k_\infty \overline{\omega}_i \oplus Lib. \to (k_\infty/A)^d \oplus Lib.$$

dont le noyau est évidemment $< \overline{\omega}_1, ..., \overline{\omega}_d >_A \simeq \Lambda$. Ce qui induit les isomorphismes énoncés. □

Soit X une sous-variété algébrique irréductible et définie sur $\overline{k}$ d'un $T-$module $\mathcal{A}$. Nous définissons $K_X \subset \overline{k}$ le corps engendré par un système de polynômes fixés définissant X, qui est donc une extension finie de k. Soit alors :

$$K := K_X \mathcal{F}.$$

Comme $K \subset \overline{k_\infty}$, il est un corps de valuation par rapport à la valuation induite de façon univoque par la valuation $1/T-$adique de k_∞ sur sa clôture algébrique. Nous définissons donc $\widehat{K}$ en tant que le complétés de K par rapport à une telle valuation. Il s'ensuit que $\widehat{K}$ est une extension finie de k_∞. Nous considérons les projections suivantes :

$$\Pi_i : \mathcal{C}^m \to \mathcal{C}, \ \ \forall i = 1, ..., m;$$

sur chaque composante de $\mathcal{C}^m$ respectivement. Nous définissons :

$$\Lambda_i := \Pi_i(\Lambda);$$

pour tout $i = 1, ..., m$. Il s'agit de m $A-$réseaux dans $\mathcal{C}$ tels que :

$$\Lambda = \bigoplus_{i=1}^{m} \Lambda_i.$$

Nous définissons le corps suivant :

$$K_\infty := \widehat{K}(\widehat{\Lambda_1, ..., \Lambda_m});$$

qui est le complété de $\widehat{K}(\Lambda_1, ..., \Lambda_m)$ par rapport à l'unique valuation induite par celle de $\widehat{K}$. Nous remarquons que :

$$\overline{e}(K_\infty^m) \subset K_\infty^m.$$

Théorème 2.1.38. *Soit $\mathcal{A}$ un $T-$module de dimension m et de rang d, et X une sous-variété algébrique de $\mathcal{A}$ comme dans les hypothèses de la Conjecture 6. Nous supposons que les composantes absolument irréductibles de X dans la clôture parfaite de son corps des coefficients restent absolument irréductibles dans $T_m(K_\infty)$. Soit $\overline{e} : Lie(\mathcal{A}) \to \mathcal{A}$ la fonction exponentielle associée à $\mathcal{A}$. Soit :*

$$Y := \overline{e}^{-1}(X) \subset Lie(\mathcal{A})(\mathcal{C}).$$

Alors, quitte à étendre K_∞ à une extension finie L et en appellant $n := [L : k_\infty]$, on a les propriétés suivantes :

1. *$B_1^m(L) \cap Y(L) \neq \emptyset$;*
2. *Y est un sous-ensemble $L-$entier de $Lie(\mathcal{A})(\mathcal{C})$;*
3. *$Y(L)$ est un sous-ensemble $L-$entier de $Lie(\mathcal{A})(L)$;*
4. *$B_1^m(L) \cap Y(L)_{reg.}$ est dense dans $B_1^m(L) \cap Y(L)$;*
5. *L'isomorphisme ϕ de la preuve du Lemme 2.1.37 se restreint aux points $L-$rationnels de $\mathcal{C}^m$ à un isomorphisme de $k_\infty-$espaces vectoriels (qu'on notera toujours ϕ) sous la forme qui suit :*

$$\phi : L^m \to k_\infty^{nm}.$$

Nous avons la décomposition suivante :

$$\mathcal{A}(L) \simeq L^m/\Lambda \simeq (k_\infty/A)^d \bigoplus Lib(L).$$

De plus si $Y(L)$ est un sous-ensemble $L-$entier de L il s'ensuit que $Y'(k_\infty) := \phi(Y(L))$ est donc un sous-ensemble $k_\infty-$entier dans k_∞^{nm}.

Démonstration. 1. Comme le corps K_X de définition de X est contenu dans K et donc dans L on a que X est définie sur L. Quitte à étendre L à une extension finie on a que $B_1^m(L) \cap X(L) \neq \emptyset$. Maintenant nous nous rappelons que la fonction exponentielle est une fonction $K-$entière sous la forme suivante :

$$\overline{e}(\overline{z}) = \sum_{i \geq 0} B_i \overline{z}^{q^i};$$

pour tout $\overline{z} \in Lie(\mathcal{A})(\mathcal{C})$, et qu'elle est en même temps un homéomorphisme local. Pour chaque $\overline{w}_0 \in X(L)$ il existe donc un voisinage ouvert $V_{\overline{w}_0} \subset \mathcal{A}(\mathcal{C})$ de celui-ci, un point $\overline{z}_0 \in \overline{e}^{-1}(\overline{w}_0)$, un voisinage ouvert $U_{\overline{z}_0} \subset Lie(\mathcal{A})(\mathcal{C})$ de $\overline{z}$ et une fonction $\mathcal{C}-$analytique sous la forme suivante :

$$\overline{\log_{\overline{z}_0}} : V_{\overline{w}_0} \to U_{\overline{z}_0};$$

qui est homéomorphisme entre les deux ouverts. La construction explicite d'une telle fonction et la preuve de sa convergence sur $U_{\overline{w}_0}$ assez petit est exactement la même que celle qu'on a fait dans le Théorème de la Fonction Implicite pour prouver l'existence de la fonction inverse. Or nous remarquons que si nous choisissons $\overline{w}_0 = \overline{0} \in \mathcal{A}$ et $\overline{z}_0 = \overline{0} \in Lie(\mathcal{A})$, la fonction logarithmique :

$$\overline{\log_{\overline{0}}} : V_{\overline{0}} \to U_{\overline{0}};$$

est $K-$analytique, suite à la construction de son expression formelle en séries de puissances :

$$\overline{\log_{\overline{0}}}(\overline{w}) = \sum_{i \geq 0} A_i \overline{w}^{q^i};$$

on s'aperçoit facilement que les matrices A_i sont à composantes dans K et donc dans L. Comme $\overline{0} \in V_{\overline{0}} \cap B_1^m(L) \neq \emptyset$ nous pouvons supposer sans perte de généralité que $V_{\overline{0}}$ soit un polydisque de rayon ≤ 1 qui contient $\overline{0}$ quitte à retrecier la fonction logarithmique $\overline{\log_{\overline{0}}}$ à un polydisque contenu dans $V_{\overline{0}}$ et contenant $\overline{0}$. Il s'ensuit que :

$$\overline{\log_{\overline{0}}}(V_{\overline{0}} \cap X(L)) \subset Y(L).$$

Si $V_{\overline{0}} \cap X(L) \neq \emptyset$ nous avons terminé. Supposons donc que $\overline{w} \in \mathcal{A} \setminus V_{\overline{0}}$ pour tout $\overline{w} \in X(L)$. Soit $\overline{z} \in \overline{e}^{-1}(\overline{w})$. Soit $D'_{\overline{0}}$ un polydisque de rayon $\delta_0 > 0$ contenant $\overline{0}$ et contenu dans $U_{\overline{0}}$. Comme la fonction $\overline{\log_{\overline{0}}}$ est continue il s'ensuit que $\overline{e}(D'_{\overline{0}})$ est un ouvert dans $V_{\overline{0}}$ et il contient par conséquent un polydisque $D_{\overline{0}}$ de rayon $\epsilon_0 > 0$ contenant $\overline{0}$. Pour tout $\overline{u} \in D'_{\overline{0}}$, on a que $||\overline{u}||_\infty \leq \delta_0$. Suite à la Définition 2.1.1 nous savons qu'il existe un nombre $s \in \mathbb{N} \setminus \{0\}$ tel que la différentielle de $\Phi(T^{q^s})$ est une matrice diagonale sous la forme $T^{q^s} I_m$. Soit $a \in \mathbb{N}$ le plus petit nombre entier tel que :

$$|T^{-q^s a} \overline{z}|_{1/T} \leq \delta_0.$$

Comme $\overline{u} := T^{-q^s a}\overline{z} \in D_{\overline{0}}$, nous avons que $\overline{\log_{\overline{0}}}(\overline{u}) \in D'_{\overline{0}}(L)$, quitte à étendre encore L en y ajoutant les solutions de l'équation polynomiale suivante :

$$\Phi(T^{q^s a})(\overline{x}) - \overline{w} = \overline{0}.$$

Comme le $T-$module est de rang fini, on sait que l'équation en question n'a qu'un nombre fini de solutions. Comme :

$$\overline{u} \in \overline{e}^{-1}(\overline{x});$$

à une extension finie près de L nous avons par conséquent que :

$$B_1^m(L) \cap Y(L) \neq \emptyset.$$

2. Nous savons que X est défini en tant que lieu de zéros d'un nombre fini r de polynômes $P_1, ..., P_r$ à coefficients dans K_X et donc dans L. A l'isomorphisme $Lie(\mathcal{A})(\mathcal{C}) \simeq \mathcal{C}^m$ près nous voyons que Y est un sous-ensemble $L-$entier de $\mathcal{C}^m$. En effet, chaque P_i $(i = 1, ..., r)$ représente une fonction $L-$entière agissant de $\mathcal{C}^m$ vers lui-même ; la fonction exponentielle est d'ailleurs elle aussi une fonction $K-$entière agissant sur $\mathcal{C}^m$ vers lui-même suite à la Remarque 2.1.11. Y est alors le lieu des zéros dans $\mathcal{C}^m$ des r fonctions $L-$entières $f_1 := P_1 \circ \overline{e}, ..., f_r := P_r \circ \overline{e}$. Il est par conséquent un sous-ensemble $L-$entier de $\mathcal{C}^m$.
3. Nous notons que $Y(L)$ est un sous-ensemble $L-$entier de $Lie(\mathcal{A})(L)$ puisque Y est le lieu des zéros d'un nombre fini de fonctions $L-$entières qui sont à valeurs dans L si restreintes à L^m. Nous remarquons quand-même qu'une telle implication, apparemment évidente, n'est pas forcément valable dans le cas où f_i soit une fonction $L-$analytique seulement. En effet, pour tout $\overline{z}_0 \in V$ il existerait un voisinage ouvert $U_{\overline{z}_0} \subset \mathcal{C}^m$ tel que $f_i(\overline{z})$ est une série de puissances (à coefficients dans L) de $\overline{z} - \overline{z}_0$ pour tout $\overline{z} \in U_{\overline{z}_0}$, mais comme L n'est pas dense dans $\mathcal{C}$, l'intersection de ce voisinage avec L^m pourrait être vide. Même si $Y(L)$ n'était pas vide il ne serait donc pas forcément $L-$analytique.
4. Nous supposons que l'espace $L-$analytique $B_1^m(L) \cap Y(L)$ soit irréductible mais qu'il ne soit pas absolument irréductible dans la clôture parfaite $\mathbb{K}$ de L dans $\mathcal{C}$. Comme l'extension $L \subseteq \mathbb{K}$ est purement inséparable l'idéal premier $\mathcal{I}(Y(L))$ est un idéal primaire dans $T_m(\mathbb{K})$ et son idéal radical dans $T_m(\mathbb{K})$ est $\mathcal{I}(Y(\mathbb{K}))$. Si $f \in \mathcal{I}(Y(\mathbb{K}))$ il est en particulier un élément de $T_m(\mathbb{K})$ qui est purement inséparable sur $T_m(L)$. Il existe donc un nombre $n \in \mathbb{N} \setminus \{0\}$ tel que $f^{p^n} \in T_m(\mathbb{K})$. D'un autre côté tout polynôme unitaire $P(X) \in T_m(L)[X]$ tel que $P(f) = 0$ a un degré qui est divisible par une puissance de p. Il existe aussi un nombre $n' \in \mathbb{N} \setminus \{0\}$ minimal tel que $f^{n'} \in \mathcal{I}(Y(L))$. Le polynôme $P(X) = X^{n'} - f^{n'} \in T_m(L)[X]$ est donc tel que $P(f) = 0$ et par conséquent il existe un nombre $n \in \mathbb{N} \setminus \{0\}$ tel que $n' = p^n$. Tout système minimal fini de générateurs de $\mathcal{I}(Y(\mathbb{K}))$ est donc un ensemble fini de racines p^h-ièmes (pour des $h \in \mathbb{N} \setminus \{0\}$ opportuns) d'autant d'éléments de $\mathcal{I}(Y(L))$. Si donc nous appelons :

$$\mathcal{I}(Y(\mathbb{K})) = (g_1, ..., g_r) \subset T_m(\mathbb{K});$$

nous obtenons que :

$$\mathcal{I}(Y(L)) = (f_1, ..., f_r) = (g_1^{p^{n_1}}, ..., g_r^{p^{n_r}}) = \mathcal{I}(Y(\mathbb{K}))^{p^n};$$

où $p^n := \max_{i=1,...,r}\{p^{n_i}\}$. Les coefficients des générateurs $g_1, ..., g_r$ de $\mathcal{I}(Y(\mathbb{K}))$ sont donc contenus dans une extension de L de degré $\leq p^n$ dans $\mathbb{K}$. Nous pouvons donc supposer à une extension finie de L près que $B_1^m(L) \cap Y(L)$ soit absolument irréductible dans $\mathbb{K}$. Un tel espace affinoïde respecte les hypothèses du Théorème 2.1.36 et donc $B_1^m(L) \cap Y(L)_{reg.}$ est dense dans $B_1^m(L) \cap Y(L)$.

5. Chaque fonction $f : \mathcal{C}^m \to \mathcal{C}$ définissant Y est sous la forme suivante :

$$f(\overline{z}) = \sum_{j\geq 0} \sum_{\mu \in \Lambda_m(j)} a_\mu \overline{z}^\mu \ \ \forall \overline{z} \in \mathcal{C}^m;$$

où les $a_\mu \in L$. Nous introduisons la notation suivante pour exprimer tout élément $\overline{z} \in L^m$. Soit $\overline{v}_{1,1}, ..., \overline{v}_{n,m}$ la base canonique de k_∞^{nm} sur k_∞, où nous numérotons les indices doubles (i, j), $i = 1, ..., m$, $j = 1, ..., n$ de la façon qui suit :

$$(i, j) < (i, j + 1) < (i + 1, j).$$

Nous remarquons maintenant que :

$$[k_\infty : k_\infty^p] = p;$$

le résultat de M. F. Becker et S. MacLane [B-M] nous permet alors de remarquer qu'il existe un élément primitif $\alpha \in L$ tel que $L = k_\infty(\alpha)$. Soit donc $1, \alpha, ..., \alpha^{n-1}$ une base de L sur k_∞. Soit $\overline{e}_1, ..., \overline{e}_m$ la base canonique de L^m sur L. Nous définissons la **base adaptée** $\overline{u}_{1,1}, ..., \overline{u}_{m,n}$ de L^m sur k_∞ de la façon suivante :

$$\overline{u}_{i,j} := \alpha^{j-1}\overline{e}_i, \ \ \forall i = 1, ..., m, \forall j = 1, ..., n.$$

Il est facile de voir qu'il s'agit en effet d'un système de vecteurs $k_\infty-$linéairement indépendants dans L^m.

Nous définissons l'isomorphisme suivant entre L^m et k_∞^{nm} :

$$\psi : L^m \to k_\infty^{nm};$$

$$\overline{u}_{i,j} \mapsto \overline{v}_{i,j};$$

qui met en correspondace biunivoque la base adaptée de L^m sur k_∞ avec la base canonique de k_∞^{nm} sur k_∞. Comme $\overline{\omega}_1, ..., \overline{\omega}_d$ sont eux aussi des vecteurs $k_\infty-$linéairement indépendants de L^m on peut les compléter (à une renumérotation près) en une base de L^m sur k_∞ en y ajoutant $nm - d$ éléments de la base adaptée de L^m sur k_∞. En utilisant en effet le système de numérotation des indices doubles $i = 1, ..., m$, $j = 1, ..., n$ que nous avons introduit nous numérotons les éléments de la base adaptée de L^m sur k_∞ avec un seul indice, ce qui nous permet d'exprimer le complété d'avant des vecteurs $\overline{\omega}_1, ..., \overline{\omega}_d$ à une base de L^m sur k_∞ comme il suit :

$$\overline{\omega}_1, ..., \overline{\omega}_d, \overline{u}_{d+1}, ..., \overline{u}_{nm}.$$

Soit :

$$\mathcal{L} : k_\infty^{nm} \to k_\infty^{nm};$$

$$\psi(\overline{\omega}_i) \mapsto \overline{v}_i;$$

l'isomorphisme sur k_∞ de k_∞^{nm} vers lui-même qui envoit $\psi(\overline{\omega}_i)$ vers $\overline{v}_i$ pour tout $i = 1, ..., d$ en fixant la base canonique $\overline{v}_{d+1}, ..., \overline{v}_{nm}$ de $\psi(Lib.(L)) = \bigoplus_{i=d+1}^{nm} k_\infty$ sur k_∞, suite à la décomposition de L^m suivante :

$$L^m = \bigoplus_{i=1}^{d} k_\infty \overline{\omega}_i \oplus Lib.(L);$$

induite par celle du Lemme 2.1.37 par l'isomorphisme ψ. Nous considérons l'isomorphisme $\phi : \mathcal{C}^m \to \mathcal{C}^m$ introduit dans le Lemme 2.1.37 en choisissant un complété à une base (infinie) de $\mathcal{C}^m$ sur k_∞ des vecteurs $\overline{\omega}_1, ..., \overline{\omega}_d$ qui se restreint à L^m au complété de ces vecteurs par la base adaptée de L^m sur k_∞ que nous avons défini avant. L'isomorphisme ϕ d'espaces vectoriels sur k_∞ que nous avons défini respecte donc la propriété suivante :

$$\phi = \mathcal{L} \circ \psi.$$

Il est donc tel que pour tout $\overline{z} \in L^m$ qui s'exprime sous la forme suivante :

$$\overline{z} = \sum_{i=1}^{d} w_i \overline{\omega}_i + \sum_{i=d+1}^{nm} w_i \overline{u}_i;$$

nous avons que :

$$\phi(\overline{z}) = \overline{w} = (w_1, ..., w_{nm}).$$

Nous avons que :

$$f(\overline{z}) = \sum_{h \geq 0} \sum_{\mu \in \Lambda_m(h)} a_\mu (\sum_{i=1}^{m} \sum_{j=1}^{n} w_{i,j} \overline{u}_{i,j})^\mu = 0, \ \ \forall \overline{z} \in Y(L);$$

où les coefficients $w_{i,j}$ d'une telle combination linéaire de la base adaptée de L^m sur k_∞ sont dans k_∞. En particulier, étant donné la restriction à L^m de l'isomorphisme ψ que nous avons donné avant, nous avons que :

$$\psi(\overline{z}) = \overline{w} := (w_{1,1}, ..., w_{1,n}, ..., w_{m,1}, ..., w_{m,n}).$$

Pour tout $j \geq 0$, $\mu = (r_1, ..., r_m) \in \Lambda_m(j)$, chaque terme $\overline{z}^\mu$ s'exprime sous la forme suivante :

$$(\sum_{i=1}^{m} \sum_{j=1}^{n} w_{i,j} \alpha^{j-1} \overline{e}_i)^\mu = \prod_{h=1}^{m} (\sum_{j=1}^{n} w_{h,i} \alpha^{j-1})^{r_h} =$$

$$= \prod_{h=1}^{m} \sum_{s_1 + ... + s_n = r_h} \binom{r_h}{s_1, ..., s_n} \prod_{j=1}^{n} w_{h,j}^{s_j} \alpha^{s_j(j-1)}.$$

Il s'ensuit que :

$$(f \circ \psi^{-1})(\overline{w}) = \sum_{j \geq 0} \sum_{\mu = (r_1, ..., r_h) \in \Lambda_m(j)} a_\mu \prod_{h=1}^{m} \sum_{s_1 + ... + s_n = r_h} \binom{r_h}{s_1, ..., s_n} \prod_{j=1}^{n} w_{h,j}^{s_j} \alpha^{s_j(j-1)}.$$

Soit :

$$h : k_\infty^{nm} \to L;$$

la fonction $L-$analytique suivante :

$$h := f \circ \psi^{-1}.$$

Il est donc possible d'exprimer $f(\overline{z})$ dans la nouvelle forme qui suit :

$$h(\overline{w}) = \sum_{i\geq 0} \sum_{\eta\in\Lambda_{nm}(i)} c_\eta \overline{w}^\eta;$$

où chaque coefficient $c_\eta \in L$ s'exprime comme il suit. Pour chaque $i \geq 0$, si $\mu = (r_1, ..., r_m) \in \Lambda_m(i)$, pour chaque r_h, $h = 1, ..., m$ nous définissons comme avant $(s_1(h), ..., s_n(h)) \in \Lambda_n(r_h)$. Nous définissons donc :

$$\eta(\mu) := (s_j(h))_{j=1,...,n,h=1,...,m} \in \Lambda_{nm}(i);$$

en ordonnant ses composantes suivant le critère de numérotation des indices doubles (h, j) introduit avant. Pour tout $\eta \in \Lambda_{nm}(i)$ quelque soit $i \geq 0$ nous définissons $\mathcal{I}(\eta) := \{\mu \in \Lambda_m(i), \eta(\mu) = \eta\}$. Nous appelons :

$$\overline{\alpha} := (\alpha, ..., \alpha) \in L^{nm}.$$

Soit $\eta(\mu)$ comme nous l'avons défini avant. Nous avons que :

$$\eta(\mu) := (s_1(1), ..., s_n(1), ..., s_1(m), ..., s_n(m)).$$

Nous appelons :

$$\widetilde{\eta}(\mu) := (0, s_2(1), 2s_3(1), ..., (n-1)s_n(1), ..., 0, s_2(m), 2s_3(m), ..., (n-1)s_n(m)) \in \mathbb{N}^{nm}.$$

Nous avons donc la propriété suivante :

$$c_\eta = \sum_{\mu\in\mathcal{I}(\eta)} a_\mu \prod_{h=1}^{m} \sum_{s_1+...+s_n=r_h} \binom{r_h}{s_1, ..., s_n} \overline{\alpha}^{\widetilde{\eta}(\mu)}.$$

Il s'ensuit que :

$$|c_\eta|_{1/T} \leq \max_{\mu\in\mathcal{I}(\eta)} |a_\mu|_{1/T} {|\alpha|_{1/T}}^{m(n-1)|\eta|};$$

qui converge vers 0 quand $|\eta|$ tend vers l'infini puisque $f : L^m \to L$ est une fonction entière. Nous remarquons également que nous pouvons exprimer chaque coefficient $c_\eta \in L$ pour tout $\eta \in \Lambda_{nm}(i)$ quelque soit $i \geq 0$ en tant que combinaison linéaire sur k_∞ par rapport à la base $1, \alpha, ..., \alpha^{n-1}$ de L sur k_∞. Nous obtenons donc qu'il existe des uniques $b_{\eta,1}, ..., b_{\eta,n} \in k_\infty$ tels que :

$$c_\eta = \sum_{j=1}^{n} b_{\eta,j} \alpha^{j-1};$$

pour tout $\eta \in \mathbb{N}^{nm}$. Il existe donc les séries formelles suivantes :

$$h_1, ..., h_n \in k_\infty[[\overline{w}]];$$

$$h_j(\overline{w}) := \sum_{i\geq 0} \sum_{\eta\in\Lambda_{nm}(i)} b_{\eta,j} \overline{w}^\eta, \ \forall j = 1, ..., n;$$

telles que :

$$h(\overline{w}) = \sum_{j=1}^{n} h_j(\overline{w})\alpha^{j-1}.$$

Nous montrons maintenant que $h_1, ..., h_n$ sont convergentes avec un rayon de convergence infini.

En effet, suite au résultat de K. Mahler [Mah], page 491, il existe une constante $\gamma > 0$ telle que pour tout c_η coefficient de h, on ait que :

$$|c_\eta|_{1/T} \geq \gamma \max_{j=1,...,n}\{|b_{\eta,j}|_{1/T}|\alpha^{j-1}|_{1/T}\}.$$

Quitte à modifier éventuellement la valeur de γ nous pouvons supposer que :

$$|c_\eta|_{1/T} \geq \gamma \max_{j=1,...,n}\{|b_{\eta,j}|_{1/T}\};$$

pour tout coefficient c_η de h. La convergence de la série $h(\psi(\overline{z}))$ implique donc celle de $h_j(\psi(\overline{z}))$ pour tout $j = 1, ..., n$. Maintenant soit $\mathcal{L} : k_\infty^{nm} \rightarrow k_\infty^{nm}$ l'isomorphisme sur k_∞ que nous avons défini avant et qui envoit le système $\{\psi(\overline{\omega}_1), ..., \psi(\overline{\omega}_d)\}$ d'éléments linéairement indépendants sur k_∞ vers les d premiers éléments $\{\overline{v}_1, ..., \overline{v}_d\}$ de la base canonique de k_∞^{nm} sur k_∞ ordonnés suivant le critère de numérotation des indices doubles que nous avons décri précédemment. Il agit sur k_∞^{nm} comme une matrice inversible contenue dans $k_\infty^{nm,nm}$. Il est donc immédiat de remarquer qu'il s'agit d'une fonction $k_\infty-$entière de k_∞^{nm} vers lui-même. Nous avons vu que :

$$\phi = \mathcal{L} \circ \psi.$$

Comme nous avons montré que la fonction suivante :

$$f \circ \psi^{-1} : k_\infty^{nm} \rightarrow L;$$

s'exprime comme il suit :

$$f \circ \psi^{-1} = \sum_{j=1}^{n} \alpha^{j-1} h_j;$$

où $h_1, ..., h_j$ sont des fonctions $k_\infty-$entières de k_∞^{nm} vers k_∞ et puisque la composition de deux fonctions entières est encore une fonction entière il s'ensuit que la fonction :

$$h \circ \mathcal{L}^{-1} = f \circ \psi^{-1} \circ \mathcal{L}^{-1} = f \circ \phi^{-1};$$

est encore une fois une combinaison linéaire des éléments de la base $\{1, \alpha, ..., \alpha^{n-1}\}$ de L sur k_∞ par des fonctions $k_\infty-$analytiques :

$$\widetilde{h}_1 := h_1 \circ \mathcal{L}^{-1}, ..., \widetilde{h}_n := h_n \circ \mathcal{L}^{-1};$$

de k_∞^{nm} vers k_∞. Autrement dit :

$$f \circ \phi^{-1} = \sum_{j=1}^{n} \alpha^{j-1}\widetilde{h}_j.$$

En appellant :

$$Y' := \{\overline{w} \in \mathcal{C}^{mn},\ \widetilde{h}_{i,j}(\overline{w}) = 0,\ \forall i = 1, ..., r,\ \forall j = 1, ..., n\};$$

où :

$$Y(L) = \{\overline{y} \in L^m,\ f_i(\overline{y}) = \sum_{j=1}^{n} \alpha^{j-1} \widetilde{h}_j(\phi(\overline{y})) = 0,\ \forall i = 1, ..., r\};$$

on a que $Y'(k_\infty) = \phi(Y(L))$ et que $Y'(k_\infty)$ est un sous-ensemble $k_\infty-$entier dans $\phi(Lie(\mathcal{A})(L)) \simeq k_\infty^{mn}$.

□

Soit $\alpha \in L$ l'élément primitif de l'extension des corps $k_\infty \subseteq L$ que nous avons introduit dans le Théorème 2.1.38 point 5. Nous choisissons $a(T), b(T) \in k_\infty$ tels que $|a(T)\alpha|_{1/T} < 1$ et $|b(T)|_{1/T} = 1$. Nous appellons :

$$\beta := a(T)\alpha + b(T).$$

Comme :

$$\alpha \in k_\infty(\beta);$$

il s'ensuit que β est un élément primitif de l'extension des corps $k_\infty \subseteq L$ aussi. Nous pouvons donc remplacer α par β et supposer donc sans perte de généralité que :

$$|\alpha|_{1/T} = 1.$$

Définition 2.1.39. *Soit un point $\overline{z} = (z_1, ..., z_m) \in L^m$ quelconque. Nous exprimons ce point de façon unique comme il suit :*

$$\overline{z} = (z_1, ..., z_m) = (\sum_{j=1}^{n} \alpha^{j-1} w_{1,j}, ..., \sum_{j=1}^{n} \alpha^{j-1} w_{m,j});$$

où :

$$w_{1,1}, ..., w_{m,n} \in k_\infty.$$

Nous définissons la norme suivante sur L^m en tant qu'espace vectoriel sur k_∞ :

$$F_\alpha(\overline{z}) := ||(w_{1,1}, ..., w_{m,n})||_\infty = \max\{|w_{1,1}|_{1/T}, ..., |w_{m,n}|_{1/T}\}.$$

Il est immédiat de remarquer qu'il s'agit bien d'une norme de L^m sur k_∞. Soit $r > 0$ un nombre réel positif. Nous définissons le sous-ensemble de L^m suivant :

$$B^m_{r,\alpha}(L) := \{\overline{z} \in L^m,\ F_\alpha(\overline{z}) \leq r\}.$$

Remarque 2.1.40. *La norme F_α sur L^m est équivalente à celle que nous avons appellé $||.||_\infty$ sur ce même ensemble vu en tant qu'espace vectoriel sur L par rapport à la base canonique :*

$$||\overline{z}||_\infty := \max\{|z_1|_{1/T}, ..., |z_m|_{1/T}\}.$$

Démonstration. Suite à [BGR] Corollary 2.1.9/4 page 78 il nous est suffisant de montrer qu'il existe $r_1, r_2 \in \mathbb{R}_{>0}$ tels que :

$$r_1 F_\alpha(\overline{z}) \leq ||\overline{z}||_\infty \leq r_2 F_\alpha(\overline{z}), \ \ \forall \overline{z} \in L^m.$$

Puisque la valeur absolue $1/T-$adique est non-archimédienne nous pouvons remarquer tout de suite que :

$$r_2 = 1.$$

L'inégalité qui nous reste à montrer suit du résultat dû à K. Mahler, voir [Mah] page 491, que nous avons déjà utilisé dans la preuve du Théorème 2.1.38 point 5 et qui implique que :

$$r_1 = \gamma;$$

où la constante $\gamma > 0$ dépend de α et elle est celle qui suit du résultat de K. Mahler en utilisant F_α en tant que norme sur L^m comme expliqué dans l'énoncé indiqué dans la référence. □

Il s'ensuit que l'ensemble $B^m_{r,\alpha}(L)$ contenu dans L^m est aussi un ouvert par rapport à la topologie $1/T-$adique que nous avons utilisé jusqu'ici. En particulier les isomorphismes $\phi : L^m \to k_\infty^{nm}$ et $\psi : L^m \to k_\infty^{nm}$ d'espaces vectoriels sur k_∞ que nous avons introduit dans la preuve du Théorème 2.1.38 point 5 sont des homéomorphismes.

Remarque 2.1.41. *Soit X un sous-ensemble $L-$analytique dans L^m et soit $\overline{z}_0 \in X$ comme dans les hypothèses du Corollaire 2.1.25, en supposant que X soit le lieu des zéros d'un nombre m' de fonctions $L-$analytiques définies sur un ouvert U de L^m dont nous appelons :*

$$\overline{F} : U \to L^{m'};$$

le vecteur de fonctions qu'ils forment (et qui dépend de leur numérotation), telles que $m' < m$. Il existe donc un voisinage ouvert de $\overline{z}_0$ dans L^m de la forme $B^{m-m'}_{1,\alpha}(L) \times V_{\overline{z}_0}$ ainsi qu'une fonction $L-$analytique de la forme suivante :

$$f_{\overline{z}_0} : B^{m-m'}_{1,\alpha}(L) \to V_{\overline{z}_0} \subset L^{m-m'} \times L^{m'};$$

telle que pour tout $\overline{z}^* \in B^{m-m'}_{1,\alpha}(L)$ la propriété suivante soit valable :

$$\overline{F}(\overline{z}^*, f_{\overline{z}_0}(\overline{z}^*)) = 0, \ \ \forall \overline{z}^* \in B^{m-m'}_{1,\alpha}(L).$$

Démonstration. Suite au Corollaire 2.1.25 il existe un voisinage ouvert $U_{\overline{z}_0} \times V_{\overline{z}_0} \subset L^{m-m'} \times L^{m'}$ de $\overline{z}_0$ ainsi qu'une fonction $L-$analytique $f : U_{\overline{z}_0} \to V_{\overline{z}_0}$ telle que :

$$\overline{F}(\overline{z}^*, f(\overline{z}^*)) = 0, \ \ \forall \overline{z}^* \in U_{\overline{z}_0}.$$

A une composition de f par une translation dans $L^{m-m'}$ près nous supposons que $\overline{z}_0 = \overline{0}$. Nous choisissons un ouvert $B^{m-m'}_{r,\alpha}(L) \subset U_{\overline{0}}$ avec $r \in |k^*_\infty|_{1/T}$. La restriction de f à $B^{m-m'}_{r,\alpha}(L)$ est encore une fonction $L-$analytique et elle est définie sur $B^{m-m'}_{r,\alpha}(L)$. On compose maintenant f par une transformation linéaire sur L de la forme suivante :

$$t : B^{m-m'}_{1,\alpha}(L) \to B^{m-m'}_{r,\alpha}(L);$$

$$\overline{z}^* \mapsto c\overline{z}^*;$$

où $c \in k_\infty$ est tel que $|c|_{1/T} = r$. Ce qui nous fait obtenir une fonction $L-$analytique sous la forme suivante :

$$f \circ t : B_{1,\alpha}^{m-m'}(L) \to V_{\overline{0}};$$

telle que :

$$\overline{F}(\overline{z}^*, (f \circ t)(\overline{z}^*)) = 0, \ \forall \overline{z}^* \in B_{1,\alpha}^{m-m'}(L).$$

Quitte à nous composer à nouveau $f \circ t$ par la translation :

$$\overline{z} \mapsto \overline{z} + \overline{z}_0;$$

nous obtenons un voisinage de $\overline{z}_0$ dans $L^{m-m'} \times L^{m'}$ et une fonction $L-$analytique comme dans l'énoncé. $\square$

Définition 2.1.42. *Soit X un sous-ensemble analytique dans L^m défini sur un ouvert U de L^m. Nous disons que X est **analytiquement $\alpha-$paramétrisable** s'il existe un nombre $d(X) \in \mathbb{N} \setminus \{0\}$ ainsi qu'une famille $\mathcal{R}$ de fonctions $L-$analytiques de la forme suivante :*

$$f : B_{1,\alpha}^{d(X)}(L) \to X;$$

telles que :

$$X \subseteq \bigcup_{f \in \mathcal{R}} f(B_{1,\alpha}^{d(X)}(L)).$$

*Nous appellons une telle famille un **recouvrement $\alpha-$analytique** de X sur L.*

Théorème 2.1.43. *1. Soit $Y(L)$ défini comme dans le Théorème 2.1.38. Si $B_1^m(L) \cap Y(L)_{reg.}$ est dense dans $B_1^m(L) \cap Y(L)$ alors $B_1^m(L) \cap Y(L)$ est analytiquement $\alpha-$paramétrisable sur L.*

2. Soit $Y(L)$ et soit $Y'(k_\infty)$ définis comme dans le Théorème 2.1.38. Alors $B_1^{nm}(k_\infty) \cap Y'(k_\infty)$ est analytiquement paramétrisable sur k_∞.

Démonstration. 1. Soit $\mathcal{I}(Y(L)) = (f_1, ..., f_r) \subset T_m(L)$ l'idéal premier associé à $B_1^m(L) \cap Y(L)$. Soit $\overline{y}_0 \in B_1^m(L) \cap Y(L)_{reg.}$. Soit $d := \dim_L(B_1^m(L) \cap Y(L)) = \dim_{\mathbb{K}}(B_1^m(\mathbb{K}) \cap Y(\mathbb{K}))$. L'égalité suit des passages dans la preuve du Théorème 2.1.36. L'hypothèse que $B_1^m(L) \cap Y(L)$ soit absolument irréductible dans $\mathbb{K}$ nous permet aussi de dire que $r \geq m-d$. A une numérotation différente près des générateurs $f_1, ..., f_r$ de $\mathcal{I}(Y(L))$ il s'ensuit que :

$$\rho_L(J_{\overline{y}_0}(f_1, ..., f_{m-d})) = \rho_{\mathbb{K}}(J_{\overline{y}_0}(f_1, ..., f_{m-d})) = m-d.$$

Nous appelons :

$$Z(f_1, ..., f_{m-d}) := \{\overline{y} \in B_1^m(L), \ \ f_1(\overline{y}) = ... = f_{m-d}(\overline{y}) = 0\}.$$

Il s'ensuit que $B_1^m(L) \cap Y(L) \subseteq Z(f_1, ..., f_{m-d})$. Suite au Corollaire 2.1.25, au Théorème 2.1.36 et à la Remarque 2.1.41 il existe donc un recouvrement $\alpha-$analytique $\mathcal{R}$ de $B_1^m(L) \cap Y(L)$ constitué par des fonctions $L-$analytiques de la forme suivante :

$$f : B_{1,\alpha}^d(L) \to Z(f_1, ..., f_{m-d}).$$

En particulier nous obtenons que :

$$B_1^m(L) \cap Y(L) \subseteq \bigcup_{f \in \mathcal{R}} f(B^d_{1,\alpha}(L)).$$

Soit $T \subseteq Z(f_1, ..., f_{m-d})$ l'unique composante irréductible de $Z(f_1, ..., f_{m-d})$ qui est absolument irréductible dans $\mathbb{K}$ et qui contient $B_1^m(L) \cap Y(L)$. Soit $d' := \dim_L(T)$. Alors $d' \geq d$. Maintenant :

$$(f_1, ..., f_{m-d}) \subseteq \mathcal{I}(T) = (g_1, ..., g_s).$$

Alors pour tout f_i, où $i = 1, ..., m-d$, il existe $a_{i,1}, ..., a_{i,s} \in T_m(L)$ tels que :

$$f_i = \sum_{j=1}^{s} a_{i,j} g_j.$$

Comme $\overline{y}_0 \in T$ il s'ensuit que :

$$J_{\overline{y}_0}(f_i) = \sum_{j=1}^{s} a_{i,j}(\overline{y}_0) J_{\overline{y}_0}(g_j), \ \ \forall i = 1, ..., r.$$

Si :

$$\rho_L(J_{\overline{y}_0}(f_1, ..., f_{m-d})) = m - d;$$

il s'ensuit que :

$$\rho_L(J_{\overline{y}_0}(\mathcal{I}(T))) \geq m - d.$$

Comme T est absolument irréductible dans $\mathbb{K}$ nous avons aussi que :

$$\rho_L(J_{\overline{y}_0}(\mathcal{I}(T))) \leq m - d'.$$

Il s'ensuit que $d' = d$. Par conséquent :

$$B_1^m(L) \cap Y(L) = T.$$

Maintenant si S est une autre composante irréductible de $Z(f_1, ..., f_{m-d})$:

$$\dim_L(S \cap T) < \dim_L(S), \dim_L(T).$$

En effet, soit $R \subseteq S \cap T$ une composante irréductible de $S \cap T$ telle que $\dim_L(R) = \dim_L(S \cap T)$. Comme :

$$S \cap T \subsetneqq S, T;$$

il s'ensuit que :

$$\dim_L(R) < \dim(S), \dim_L(T).$$

A un sous-espace affinoïde de dimension $< d$ de $B_1^m(L) \cap Y(L)$ près nous pouvons alors supposer que $\overline{y}_0$ ne soit contenu que dans une seule composante irréductible de $Z(f_1, ..., f_{m-d})$ qui est $B_1^m(L) \cap Y(L)$. Par conséquent $B_1^m(L) \cap Y(L)$ contient un sous-ensemble dense de points $\overline{z}_0 \in B_1^m(L) \cap Y(L)_{reg.}$ tels qu'il existe pour chacun d'entre eux une fonction $L-$analytique f définie sur un voisinage ouvert opportun $V_{\overline{z}_0}$ de $\overline{z}_0$ tel que $V_{\overline{z}_0} \setminus \{\overline{z}_0\} \neq \emptyset$ et telle que $f(V_{\overline{z}_0})$ (qui est un sous-ensemble de

$Z(f_1, ..., f_{m-d}))$ soit entièrement contenu dans la composante irréductible $B_1^m(L) \cap Y(L)$ de $Z(f_1, ..., f_{m-d})$. Suite à la Remarque 2.1.41 nous pouvons donc supposer sans perte de généralité que toute fonction $L-$analytique $f \in \mathcal{R}$ soit telle que :

$$f : B_{1,\alpha}^d(L) \to B_1^m(L) \cap Y(L).$$

2. Soient $f_1, ..., f_r$ comme dans le point précédent. L'isomorphisme ϕ sur k_∞ de L^m vers k_∞^{nm} est tel que :

$$Y'(k_\infty) = \{\overline{w} \in k_\infty^{nm}, \ \ (f_i \circ \phi^{-1})(\overline{w}) = 0, \ \ \forall i = 1, ..., r\}.$$

Dans la preuve du Théorème 2.1.38 point 5 nous avons en effet associé à chaque f_i pour $i = 1, ..., r$ les n fonctions $k_\infty-$entières $\widetilde{h}_{i,1}, ..., \widetilde{h}_{i,n}$ telles que :

$$(f_i \circ \phi^{-1}) = \sum_{j=1}^{n} \alpha^{j-1} \widetilde{h}_{i,j}, \ \ \forall i = 1, ..., r.$$

Nous rappelons d'avoir défini en particulier la transformation linéaire sur k_∞ suivante :

$$\psi : L^m \to k_\infty^{nm};$$

qui envoit la base adaptée $\{\alpha^{j-1}\overline{e}_i\}$ de L^m sur k_∞ vers la base canonique de k_∞^{nm} sur k_∞, ainsi que l'isomorphisme d'espaces vectoriels sur k_∞ suivant :

$$\mathcal{L} : k_\infty^{nm} \to k_\infty^{nm};$$

qui envoit les images $\psi(\overline{\omega}_1), ..., \psi(\overline{\omega}_d)$ par ψ des d périodes fixées précédemment $\overline{\omega}_1, ..., \overline{\omega}_d$ de Λ vers les d premiers éléments $\overline{v}_1, ..., \overline{v}_d$ de la base canonique de k_∞^{nm} sur k_∞ suivant le critère de numérotation des indices doubles que nous avons introduit dans la preuve du Théorème 2.1.38 point 5. La transformation $k_\infty-$linéaire ψ entre L^m et k_∞^{nm} est une isométrie entre ces deux espaces vectoriels sur k_∞ par rapport à la valeur absolue $1/T-$adique sur k_∞^{nm} et à la norme F_α que nous avons introduit dans la Définition 2.1.39 sur L^m. Nous obtenons donc que :

$$\psi^{-1}(B_1^{nm}(k_\infty)) = B_{1,\alpha}^m(L).$$

Maintenant la valeur $\dim_L(Y(L))$ est aussi la valeur constante telle que la paramétrisation $\alpha-$analytique $\mathcal{R}$ de $B_1^m(L) \cap Y(L)$ qui suit du point 1 est telle que pour chaque $f \in \mathcal{R}$ une telle fonction $L-$analytique est de la forme suivante :

$$f : B_{1,\alpha}^{\dim_L(Y(L))}(L) \to B_1^m(L) \cap Y(L).$$

Soit $d_L(Y) := \dim_L(Y(L))$. Soit $d(Y'(k_\infty)) := nd_L(Y)$. Nous définissons donc la transformation linéaire ψ sur k_∞ de la même façon qu'avant mais cette fois-ci entre $L^{d_L(Y)}$ et $k_\infty^{d(Y'(k_\infty))}$. L'isomorphisme $\psi : L^{d_L(Y)} \to k_\infty^{nd_L(Y)}$ d'espaces vectoriels sur k_∞ que nous avons défini est aussi une bijection entre $B_{1,\alpha}^{d_L(Y)}(L)$ et $B_1^{d(Y'(k_\infty))}(k_\infty)$ et il est tel que pour chaque $f \in \mathcal{R}$ la fonction suivante :

$$g : B_1^{d(Y'(k_\infty))}(k_\infty) \to B_1^{nm}(k_\infty) \cap Y'(k_\infty);$$

telle que :
$$g := \phi \circ f \circ \psi^{-1};$$
est une fonction $k_\infty-$analytique. Il est en effet immédiat de remarquer que ψ^{-1} est une fonction $L-$analytique et que par conséquent $f \circ \psi^{-1}$ est une fonction $L-$analytique elle aussi. En particulier, elle est de la forme suivante :
$$(f \circ \psi^{-1})(\overline{w}) = \sum_{i\geq 0} \sum_{\mu \in \Lambda_m(i)} a_\mu \psi^{-1}(\overline{w})^\mu.$$
En répétant les mêmes passages contenus dans la preuve du Théorème 2.1.38 point 5 nous pouvons exprimer $f \circ \psi^{-1}$ sous la forme suivante :
$$(f \circ \psi^{-1})(\overline{w}) = \sum_{j=1}^{n} \alpha^{j-1} h_j(\overline{w});$$
où $h_1(\overline{w}), ..., h_n(\overline{w})$ sont n fonctions $k_\infty-$analytiques de $B_1^{d(Y'(k_\infty))}(k_\infty)$ vers k_∞^m. Il est très important de remarquer que dans la preuve du Théorème 2.1.38 point 5 nous avons obtenu un tel résultat avec des fonctions $h_1, ..., h_n$ qui étaient $k_\infty-$entières sur k_∞^{nm} et à valeurs dans k_∞ comme les hypothèses dans ce Théorème prévoyaient que f était une fonction $L-$entière sur L^m ce qui n'est plus vrai dans notre nouvelle situation. Une telle hypothèse était toutefois nécessaire comme les puissances de la valeur absolue $1/T-$adique de l'élément primitif α de l'extension de degré fini des corps $k_\infty \subseteq L$ n'étaient pas bornées. Comme nous avons montré qu'il est possible de supposer sans perte de généralité que :
$$|\alpha|_{1/T} = 1;$$
le même raisonnement reste valable dans le cas où f est une fonction $L-$analytique définie sur $B_{1,\alpha}^{d_L(Y)}(L)$. Les fonctions $k_\infty-$analytiques $h_1, ..., h_n$ de $B_1^{d(Y'(k_\infty))}(k_\infty)$ vers k_∞^m que nous avons construit ici sont en particulier n vecteurs de m fonctions $k_\infty-$analytiques de $B_1^{d(Y'(k_\infty))}(k_\infty)$ vers k_∞ de la forme suivante :
$$h_j(\overline{w}) := (h_{1,j}(\overline{w}), ..., h_{m,j}(\overline{w})), \ \ \forall j = 1, ..., n.$$
Il s'ensuit que :
$$(\psi \circ f \circ \psi^{-1})(\overline{w}) = (h_{1,1}(\overline{w}), ..., h_{m,n}(\overline{w})), \ \ \forall \overline{w} \in B_1^{d(Y'(k_\infty))}(k_\infty).$$
La fonction $\psi \circ f \circ \psi^{-1}$ que nous avons défini est donc $k_\infty-$analytique sur $B_1^{d(Y'(k_\infty))}(k_\infty)$. Comme nous avons montré que $\mathcal{L}$ est une fonction $k_\infty-$entière de k_∞^{nm} vers lui-même et que $\phi = \mathcal{L} \circ \psi$ nous obtenons finalement que g est une fonction $k_\infty-$analytique de $B_1^{d(Y'(k_\infty))}(k_\infty)$ vers $B_1^{nm}(k_\infty) \cap Y'(k_\infty)$. La famille suivante :
$$\mathcal{R}' := \{g = \phi \circ f \circ \psi^{-1}, \ \ \forall f \in \mathcal{R}\};$$
est donc un recouvrement $k_\infty-$analytique de $Y'(k_\infty)$ sous la forme induite par le Corollaire 2.1.25.

□

On définit les fonctions de projection triviales de $\phi(Lie(\mathcal{A})(L))$ sur ses deux facteurs que nous déduisons de celles donnés par l'isomorphisme introduit dans le Théorème 2.1.38 :

$$\pi_1 : \phi(Lie(\mathcal{A})(L)) \twoheadrightarrow k_\infty^d;$$
$$\pi_2 : \phi(Lie(\mathcal{A})(L)) \twoheadrightarrow Lib(L).$$

Autrement dit, π_1 est la projection de $\phi(Lie(\mathcal{A})(L)) = k_\infty^{nm}$ sur ses d premières composantes et π_2 est sa projection sur les $nm-d$ dernières composantes. Toutes les considérations de nature topologique que nous ferons sur $Y(L)$ resteront valables sur $Y'(k_\infty)$ comme elles seront conservées par les isomorphismes linéaires $\mathcal{L}$ et ϕ. Nous notons l'image de π_1 en tant que sous-$k_\infty-$espace vectoriel de k_∞^{nm} de la manière suivante :

$$\Pi := \pi_1(k_\infty^{nm}) \simeq k_\infty^d.$$

2.2 Une conjecture

La conjecture de Manin-Mumford classique[3], traitant la situation d'une courbe elliptique plongée dans sa Jacobienne a été prouvée (voir [R1]) et ensuite généralisée (voir [R2]) dans la formulation qui suit :

Théorème 2.2.1. *Soit X une sous-variété algébrique d'une variété abélienne $\mathcal{A}$ définie sur un corps de nombres. Si X contient un ensemble Zariski-dense de points de torsion, alors X est la translatée d'une sous-variété abélienne de $\mathcal{A}$ par un point de torsion.*

La version faible montrée dans [PZ] est une conséquence du Théorème 2.2.1 et se formule de cette manière :

Théorème 2.2.2. *Sous les mêmes hypothèses que le Théorème 2.2.1, si X ne contient pas de translatées de sous-variétés abéliennes de $\mathcal{A}$ de dimension > 0 par un point de torsion, alors X ne contient qu'un nombre fini de points de torsion.*

Admettons en effet le Théorème 2.2.1 et que la sous-variété algébrique X de $\mathcal{A}$ ne contient pas de translatées de sous-variétés abéliennes de $\mathcal{A}$ de dimension > 0 par des points de torsion. Si X contenait un nombre infini de points de torsion elle contiendrait aussi la clôture de Zariski X' de ces derniers, de dimension > 0. La sous-variété algébrique X' de $\mathcal{A}$ contient donc un ensemble Zariski-dense de points de torsion. L'application du Théorème 2.2.1 à X' implique que X' est la translatée d'une sous-variété abélienne de $\mathcal{A}$ par un point de torsion et comme $\dim(X') > 0$ cela contredit l'hypothèse sur X.

Une formulation analogue de ce résultat a été montrée par T. Scanlon dans [Sc] pour les $T-$modules qui sont la puissance d'un module de Drinfeld, en utilisant la théorie des modèles et se basant sur un précédent résultat de L. Denis (voir [Den3]), où le même résultat est montré pour une puissance d'un module de Drinfeld, mais sous une hypothèse supplémentaire sur la nature de ce dernier qui sera explicitée plus loin (voir Hypothèse 3). Le résultat de Scanlon est le suivant.

3. D'un point de vue historique la toute première version de cette conjecture a été montrée par M. Laurent sur $\mathbb{G}_m^n$, voir [Lau2]

Théorème 2.2.3. *Soit $\mathcal{A} := (\mathbb{D}^m, \Phi)$ un $T-$module puissance d'un module de Drinfeld $(\mathbb{D}, \Phi)$ donné. Soit X une sous-variété algébrique irréductible de $\mathcal{A}$. Si $X(\mathcal{F})_{tors.}$ est Zariski-dense dans X, alors X est une translatée d'un sous-$T-$module de $\mathcal{A}$ par un point de torsion.*

Un $T-$module sous forme diagonale est, comme nous l'avons déjà remarqué, un $T-$module abélien et uniformisable de façon évidente. Il est donc naturel de se demander si un tel résultat peut être montré, avec l'utilisation des nouvelles techniques utilisées dans [PZ], pour un $T-$module $\mathcal{A}$ abélien et uniformisable quelconque. Nous allons voir ci-dessous que la réponse est négative, nous utiliserons pour cela la notion suivante :

Définition 2.2.4. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module de dimension m. On dit qu'il est **simple** s'il n'admet pas de sous-$T-$modules non triviaux (autrement dit, différents de lui-même ou de 0). Soit $a(T) \in A \setminus \mathbb{F}_q$. On dit un sous-groupe algébrique de $\mathcal{A}$ un **sous-**$a(T)-$**module** s'il est un sous-$\mathbb{F}_q[a(T)]-$module sous l'action de Φ.*

Nous considérons le $T-$module de dimension 2 défini par la puissance tensorielle $C^{\otimes 2} = (\mathbb{G}_a^2, \Phi)$ du module de Carlitz C, introduit par G. Anderson et D. Thakur dans [AT]. On suppose ici que $q = 2$. Ce $T-$module est alors sous la forme suivante :

$$\Phi(T)\begin{pmatrix} X \\ Y \end{pmatrix}(\tau) = \begin{pmatrix} T & 1 \\ 0 & T \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\tau.$$

On peut donc montrer que :

$$\Phi(T^2)\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} T^2X + X^2 \\ T^2Y + (T+T^2)X^2 + Y^2 \end{pmatrix}.$$

Le sous-groupe algébrique $0 \times \mathbb{G}_a$ de $C^{\otimes 2}$ en est alors sous-T^2-module, mais n'en est cependant pas un sous-$T-$module. En général la puissance tensorielle $C^{\otimes m}$ du module de Carlitz C est toujours un $T-$module simple (voir [Yu], Proposition 1.2), abélien et uniformisable, mais on peut montrer qu'elle possède parfois des sous-T^j-modules (j dépendant de m et de q) non triviaux et fournissent donc des contre-exemples à une éventuelle généralisation du Théorème 2.2.3 comme chacun de ces sous-T^j-modules est en général une sous-variété algébrique de $C^{\otimes m}$ contenant une infinité de points de torsion. Par exemple, $C^{\otimes 2}$ est un $T-$module simple qui contient la sous-variété algébrique $0 \times \mathbb{G}_a$, qui en est en particulier un sous-T^2-module et contient donc une infinité de points de torsion.

Nous allons alors étendre la classe de sous-modules algébriques dans $\mathcal{A}$ nécessaires dans le but de trouver une formulation possible de la Conjecture de Manin-Mumford dans le cas plus général d'un $T-$module abélien et uniformisable.

Remarque 2.2.5. *Quand on a un sous-T^j-module, c'est automatiquement un sous-$a(T^j)-$module pour tout $a \in A \setminus \mathbb{F}_q$, inversement il semble que la gradation par le degré des polynômes définissant le $T-$module ne permette pas de trouver un exemple de sous-$a(T)-$module ne provenant pas d'un sous-T^j-module pour un j bien choisi. Un cas fondamental illustrant ce phénomène est d'ailleurs celui d'une puissance pure d'un module de Drinfeld, cas que nous discutons ci-dessous.*

Théorème 2.2.6. *Soit $\mathbb{D}^m = (\mathbb{G}_a^m, \Phi^m)$ la puissance $m-$ième d'un module de Drinfeld $\mathbb{D} = (\mathbb{G}_a, \Phi)$ dont nous appelons $\mathcal{F}$ le corps des coefficients. Il existe une correspondance bijective entre la famille des sous-$T-$modules de $\mathbb{D}^m$ et la famille des sous-espaces vectoriels de $Lie(\mathbb{D}^m)$ qui sont $End_{\mathcal{F}}(\Phi)-$rationnels. Cette correspondance est donnée par la fonction exponentielle :*

$$\overline{e} : Lie(\mathbb{D}^m) \to \mathbb{D}^m;$$

$$V \mapsto \overline{e}(V).$$

De plus on a que la dimension d'un sous-$T-$module de $\mathbb{D}^m$ et d'un sous-espace vectoriel $End_{\mathcal{F}}(\Phi)-$rationnel de $Lie(\mathbb{D}^m)$ correspondants sont égaux.

Démonstration. Voir [T], Théorème à page 33. □

Soit donc $\mathcal{B}$ un sous-$a(T)-$module de $\mathbb{D}^m$. Supposons que le module de Drinfeld $\mathbb{D}$ soit de rang d. Nous définissons :

$$T' := a(T);$$

et :

$$\Psi(T') := \Phi(a(T));$$

$\mathcal{B}$ est donc un $T'-$module qui est la puissance $m-$ième d'un $\mathbb{F}_q[T']-$module de Drinfeld de rang $d\deg_T(a(T))$. Suite au Théorème 2.2.6 il est donc décrit entièrement par $s = m - \dim(\mathcal{B})$ équations linéaires sous la forme suivante :

$$\sum_{j=1}^{m} P_{ij}(\tau)X_j = 0;$$

où $P_{ij}(\tau) \in End_{\mathcal{F}}(\Psi)$ pour tout $i = 1, ..., s$ et tout $j = 1, ..., m$. Comme $\Phi(T) \in End_{\mathcal{F}}(\Psi)$ aussi (en effet, $\Phi(T) \circ \Psi(T') = \Phi(T) \circ \Phi(a(T)) = \Phi(a(T)) \circ \Phi(T) = \Psi(T') \circ \Phi(T)$) et que $End_{\mathcal{F}}(\Psi)$ est un anneau commutatif (puisque $\mathbb{D}$ est de caractéristique 0) on voit que $\mathcal{B}$ est en fait un sous-$T-$module de $\mathbb{D}^m$ puisqu'il est stabilisé par l'action de $\Phi(T)$.

Tout sous-$a(T)-$module de $\mathbb{D}^m$ (puissance $m-$ième d'un module de Drinfeld quelconque) est alors pour tout $a(T) \in A \setminus \mathbb{F}_q$ un $T-$module aussi. Il est donc raisonnable de formuler la Conjecture suivante.

Conjecture 5. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module abélien et uniformisable de dimension m. Il existe alors un nombre $j(\mathcal{A}) \in \mathbb{N} \setminus \{0\}$ ne dépendant que de $\mathcal{A}$ tel que pour tout $a(T) \in A \setminus \mathbb{F}_q$ on ait que tout sous-$a(T)-$module de $\mathcal{A}$ est un sous-$T^{j(\mathcal{A})}-$module.*

Si $\mathcal{A}$ est **absolument simple** (ce qui veut dire qui ne contient aucun sous-T^j-module non trivial pour tout $j \in \mathbb{N} \setminus \{0\}$) nous fixons $j(\mathcal{A}) = 1$.

Nous remarquons que l'étude que nous venons de faire des puissances d'un module de Drinfeld choisi fournit un exemple d'une classe de $T-$modules $\mathcal{A}$ tels que pour tout $i \in \mathbb{N} \setminus \{0\}$ on ait que $j(\mathcal{A}^i) = j(\mathcal{A})$. On peut se demander s'il s'agit d'un phénomène général (nous espérons revenir plus tard à cette question).

Nous présentons ici un exemple supplémentaire qui semble corroborer une telle Conjecture.

Soit $C^{\otimes 2} = (\mathbb{G}_a^2, \Phi)$ la puissance tensorielle carrée du module de Carlitz C, déjà introduite avant, où nous supposons toujours que $q = 2$. Nous avons montré précédemment que la différentielle de $\Phi(T^2)$ est alors $T^2 I_2$, où I_2 est la matrice identité sous la forme 2×2. Nous disons que tout polynôme $a(T) \in A$ est **pair** si et seulement s'il est sous la forme suivante :

$$a(T) = a_0 + a_1 T^2 + ... + a_r T^{2r}.$$

Il s'ensuit facilement que la différentielle de $\Phi(a(T))$ avec $a(T)$ polynôme pair est $a(T)I_2$. Or si $b(T) \in A \setminus \{0\}$ n'est pas pair il est nécessairement sous la forme suivante :

$$b(T) = Ta(T) + r(T);$$

où $a(T)$ et $r(T)$ sont des polynômes pairs. En remarquant que la différentielle de $\Phi(Ta(T)) = \Phi(T) \circ \Phi(a(T))$ est, suite aux propriétés de la fonction exponentielle et à la description de $\Phi(T)$ que nous avons fait avant, sous la forme suivante :

$$\begin{pmatrix} T & 1 \\ 0 & T \end{pmatrix} \begin{pmatrix} a(T) & 0 \\ 0 & a(T) \end{pmatrix};$$

auquelle on ajoute la différentielle de $r(T)$, qui est $r(T)I_2$, nous concluons que la différentielle de $b(T)$ est une matrice triangulaire supérieure dont les termes diagonaux sont égaux à $b(T)$. Comme $b(T)$ n'est pas pair (il est donc différent de 0) il s'ensuit que le seul sous-espace dans $Lie(C^{\otimes 2})$ stable sous l'action de cette matrice est $\mathcal{C} \times 0$. Nous supposons maintenant qu'il existe un sous-$b(T)-$module $\mathcal{B}$ de $C^{\otimes 2}$ différent de $\overline{e}(\mathcal{C} \times 0)$. Alors :

$$\Phi(b(T))(\mathcal{B}) \subseteq \mathcal{B};$$

ce qui implique que $Lie(\mathcal{B})$ est stable sous l'action de la différentielle de $\Phi(b(T))$, ce qui implique suite aux passages précédents que $Lie(\mathcal{B}) = \mathcal{C} \times 0$, ce qui implique finalement qu'un tel $\mathcal{B}$ différent de $\overline{e}(\mathcal{C} \times 0)$ ne peut pas exister. Nous venons donc de montrer que $\overline{e}(\mathcal{C} \times 0)$ est le seul sous-$b(T)-$module possible de $C^{\otimes 2}$ où $b(T)$ est n'importe quel polynôme pas pair de $A \setminus \{0\}$. Comme T n'est pas un polynôme pair dans $A \setminus \{0\}$ le seul sous-$T-$module pas trivial de $C^{\otimes 2}$ ne peut être que $\overline{e}(\mathcal{C} \times 0)$. Mais nous savons justement que $C^{\otimes 2}$ est un $T-$module simple, ce qui implique que $\overline{e}(\mathcal{C} \times 0)$ n'est pas stable sous l'action de T ou qu'il n'est pas une sous-variété algébrique dans $\mathbb{G}_a^2$. Or :

$$\Phi(T) \circ \overline{e}(\mathcal{C} \times 0) = \overline{e}(TI_2(\mathcal{C} \times 0)) \subset \overline{e}(\mathcal{C} \times 0);$$

ce qui implique que $\overline{e}(\mathcal{C} \times 0)$ est stable sous l'action de T. Il s'ensuit finalement qu'il ne peut pas être une variété algébrique dans $\mathbb{G}_a^2$. Donc il ne peut pas être un sous-$b(T)-$module non plus quelque soit $b(T) \in A \setminus \mathbb{F}_q$. Nous concluons que $C^{\otimes 2}$ n'admet pas de sous-$b(T)-$modules avec $b(T)$ pas pair. Les seuls sous-$a(T)-$modules possibles de $C^{\otimes 2}$ sont alors ceux tels que $a(T)$ soit pair.

Remarque 2.2.7. *Pour trouver des sous-T^j-modules, il ne suffit nullement d'avoir un sous-groupe dont l'espace tangent à l'origine soit stable sous la différentielle* *de $\Phi(T^j)$. En effet, soit $\mathcal{A}$ un $T-$module de dimension m. Soit a_0 sa différentielle sur $Lie(\mathcal{A})$, comme dans la Définition 2.1.1. Comme a_0 est de la forme TI_m+N, où N est une matrice nilpotente, si $n \in \mathbb{N} \setminus \{0\}$ est tel que $N^n = 0$, on a que $a_0^{p^n} = T^{p^n} I_m$. Il existera donc un $j \in \mathbb{N}\setminus\{0\}$ tel que la différentielle de $\Phi(T^j)$ est $T^j I_m$. Tout sous-espace vectoriel $H \subset Lie(\mathcal{A})$ est alors stable sous l'action de la différentielle de $\Phi(T^j)$. Si on regarde par exemple la puissance tensorielle $C^{\otimes 2}$ du module de Carlitz C (où $q = 2$), le sous-groupe algébrique $\mathbb{G}_a \times 0$ n'est pas un sous-T^2-module de $C^{\otimes 2}$. En effet, un tel sous-groupe n'est pas stabilisé par l'action de $\Phi(T^2)$ alors que tout sous-$\mathcal{C}-$espace de $Lie(C^{\otimes 2}) \simeq \mathcal{C}^2$ doit être stabilisé par l'action de la différentielle pour les raisons précédemment expliquées.*

Tout ceci nous suggère alors une formulation différente de la Conjecture de Manin-Mumford dans le cas d'un $T-$module $\mathcal{A}$, où on se propose de montrer que, à un nombre fini près, les points de torsion de $\mathcal{A}$ se partagent en un nombre fini de sous-$T^{j(\mathcal{A})}-$modules, ayant initialement fixé un nombre $j(\mathcal{A}) \in \mathbb{N} \setminus \{0\}$, ne dépendant que du choix de $\mathcal{A}$ qui ne sera donc pas forcément 1, à la différence de ce que conduirait à penser un analogue immédiat avec la formulation classique de cette conjecture.

Cependant une telle modification n'est pas encore suffisante pour nous mettre à l'abri de contre-exemples. En analysant en effet le cas d'un produit de modules de Drinfeld non isogènes on y trouve des mauvaises situations. Supposons encore que $q = 2$. Soit $C(T)(\tau) = T+\tau$ module de Carlitz $\mathbb{D}_1$, où τ est l'automorphisme de Frobenius sur $\overline{\mathbb{F}_2}$. Nous définissons le module de Drinfeld $\mathbb{D}_2$ suivant :

$$C_{(2)}(T)(\tau) := T + (T^{1/2} + T)\tau + \tau^2.$$

Il est obtenu en tant que racine carrée sur les coefficients de $C(T^2)(\tau)$. Le produit :

$$\Phi(T)\begin{pmatrix} X \\ Y \end{pmatrix} := \begin{pmatrix} C(T)(X) \\ C_{(2)}(T)(Y) \end{pmatrix};$$

est donc un $T-$module comme nous les avons définis dans la Définition 2.1.1 et parmi ses points de torsion nous avons tous les couples $(z, z^{1/2})$, où $z \in \mathbb{D}_{1tors.}$. La variété algébrique $X = Y^2$ contient alors tous ces points de torsion et, comme $C(T^j)(Y^2) \neq (C_{(2)}(T^j)(Y))^2$ quelque soit $j \in \mathbb{N} \setminus \{0\}$, elle n'est pas stabilisée par l'action de $\Phi(T^j)$. Elle n'est donc pas un sous-T^j-module de $(\mathbb{D}_1 \times \mathbb{D}_2, \Phi)$ quelque soit $j \in \mathbb{N}\setminus\{0\}$. Comme cette variété a $\mathcal{C}-$dimension 1, elle n'admet pas de sous-T^j-modules non triviaux non plus. On remarque que le même contre-exemple se répète de la même manière pour q quelconque, en remplaçant le module de Carlitz C par un module de Drinfeld générique $\mathbb{D}_1 = (\mathbb{G}_a, \Phi_1)$ et $C_{(2)}$ par le module de Drinfeld $\mathbb{D}_2 = (\mathbb{G}_a, \Phi_2)$ obtenu en tant que racine $1/q^s-$ième des coefficients de $\Phi_1(T^{q^s})$, ce qui définit toute une classe infinie de mauvais cas.

Nous considérons alors le $T-$module $\mathcal{A} := (\mathbb{D}_1 \times ... \times \mathbb{D}_m, \Phi)$, où les modules de Drinfeld $(\mathbb{D}_1, \Phi_1), ..., (\mathbb{D}_m, \Phi_m)$ ne sont pas isogènes deux à deux. D'après la Définition 2.1.1, nous remarquons que si la matrice coefficient a_d est inversible, tous ces modules de Drinfeld ont nécessairement le même rang d. Une situation comme celle des exemples précédents ne pourra donc pas se produire quelque soit Φ ou q puisque $\Phi_{(q^s)}$ (le module de Drinfeld qu'on obtient en changeant les coefficients de son itérée q^s-ième $\Phi(T^{q^s})$ avec leur racine q^s-ième) a pour degré $q^s d$. Les points de torsion de $\mathcal{A}$ ne seront donc pas contenus dans une variété algébrique comme celle qu'on avait dans l'exemple précédent. A priori aucune relation algébrique entre leurs composantes n'est soupçonnable.

Si on considère en revanche un produit de m modules de Drinfeld isogènes, comme ils ont même rang on obtient un $T-$module vérifiant la condition d'avoir coefficient dominant inversible. Il y a cette fois une relation entre les points de torsion des modules de Drinfeld. Supposons pour simplifier $m = 2$. Notre $T-$module est alors le produit $\mathbb{D}_1 \times \mathbb{D}_2$ de deux modules de Drinfeld $\mathbb{D}_1 = (\mathbb{G}_a, \Phi_1)$ et $\mathbb{D}_2 = (\mathbb{G}_a, \Phi_2)$ isogènes. Si $P(\tau) \in Hom_{\mathcal{F}}(\Phi_1, \Phi_2) \setminus \{0\}$ est une isogénie entre les deux modules de Drinfeld, Φ_2 sera alors "'racine $P(\tau)-$ième"' de Φ_1. Autrement dit, $\Phi_1(T)(\tau) \circ P(\tau) = P(\tau) \circ \Phi_2(T)(\tau)$ et les points de torsion de $\Phi_1(T) \times \Phi_2(T)$ contiennent tous ceux sous la forme $(P(\tau)(z), z)$, où z est point de torsion par rapport à Φ_2. La variété algébrique $X = P(\tau)(Y)$ qui contient tous ces points de torsion est alors facilement stabilisée par l'action de $\Phi_1(T) \times \Phi_2(T)$. Ce qui montre donc qu'un lien algébrique entre les points de torsion d'un $T-$module n'est pas forcément un obstacle à ce que celui-ci satisfasse cette première version de la Conjecture de Manin-Mumford dans le cas des $T-$modules.

Dans ces deux cas extrêmes où le $T-$module est un produit de modules de Drinfeld de même rang, rien ne semble donc s'opposer à ce qu'un résultat de type Manin-Mumford soit également vrai. Dans ces situations le coefficient dominant du $T-$module est inversible toutefois une telle hypothèse directe d'inversibilité de a_d nous ferait cependant perdre un nombre considérable de bon cas possibles, comme par exemple celui qu'on a déjà examiné avant d'une puissance tensorielle $C^{\otimes m} = (\mathbb{G}_a^m, \Phi)$ d'un module de Carlitz, qui est en général sous la forme suivante :

$$\Phi(T)(\tau) := \begin{pmatrix} T & 1 & 0 & \cdots & 0 \\ & T & 1 & \cdots & 0 \\ & & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ 0 & & & & T \end{pmatrix} + \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ \vdots & 0 & & 0 & 0 \\ & & & & \\ \vdots & 0 & & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} \tau;$$

donc ne satisfaisant pas une éventuelle hypothèse d'inversibilité du coefficient dominant. Nous allons donc demander qu'il existe un nombre $i \in \mathbb{N} \setminus \{0\}$ tel que le coefficient dominant a'_{id} de l'itéré $i-$ième $\Phi(T^i)(\tau)$ de $\Phi(T)(\tau)$ est inversible. Comme il est facile d'observer, ça ne change en rien le raisonnement qu'on vient de faire et nous permet toujours d'enlever les mauvais cas décrits ci-dessus. D'un autre côté, on voit par exemple dans la situation d'une puissance tensorielle du module de Carlitz, que celle-ci respecte une telle hypothèse.

Théorème 2.2.8. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ $T-$module défini sur le corps $\mathcal{F} \subset \overline{k}$, tel qu'il existe un nombre $i \in \mathbb{N} \setminus \{0\}$ tel que le coefficient dominant de $\Phi(T^i) \in \mathcal{F}^{m,m}\{\tau\}$ est une matrice inversible. Alors $\mathcal{A}$ est abélien.*

Démonstration. Suite à l'isomorphisme canonique :

$$Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a) \simeq \mathcal{F}\{\tau\}^m;$$

nous considérons un morphisme $f \in Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a)$ comme étant un élément $f(\tau) \in \mathcal{F}\{\tau\}^m$. Comme le coefficient dominant de $\Phi(T^i)$ est inversible et l'algèbre de Ore $\mathcal{F}\{\tau\}$ est un anneau (non commutatif) muni de l'algorithme de division à droite (voir [Goss], Proposition 1.6.2), il est possible de diviser à droite par $\Phi(T^i)$ chaque élément de $\mathcal{F}\{\tau\}^m$, compte tenu que les coefficients d'un tel objet sont des vecteurs dans $\mathcal{F}^m$ alors que ceux de $\Phi(T^i)$ sont des matrices dans $\mathcal{F}^{m,m}$. En effet, une matrice inversible dans $\mathcal{F}^{m,m}$ divise aussi (à droite) tout élément de $\mathcal{F}^m$, ce qui nous permet donc la division euclidienne en question. L'algèbre $\mathcal{F}\{\tau\}^m$ se partage alors en $mi\widetilde{d}$ (où $\widetilde{d}$ est le degré de $\Phi(T)$ en tant que polynôme additif en τ) classes de division modulo $\Phi(T^i)$, ce qui se traduit en disant que $Hom_{\mathcal{F}}(\mathcal{A}, \mathbb{G}_a) \simeq \mathcal{F}\{\tau\}^m$ est engendré par $mi\widetilde{d}$ éléments en tant que $\mathcal{F}[T]-$module, selon l'action décrite précédemment. $\square$

Nous allons donc reformuler la Conjecture de Manin-Mumford pour un $T-$module de la façon suivante.

Conjecture 6. *Soit $\mathcal{A} = (\mathbb{G}_a^n, \Phi)$ un $T-$module uniformisable de dimension m et rang d, tel qu'il existe $i \in \mathbb{N} \setminus \{0\}$ tel que la matrice coefficient dominant de l'itéré $\Phi(T^i)$ est inversible. Il existe alors $j(\mathcal{A}) \in \mathbb{N} \setminus \{0\}$ tel qu'on ait la propriété suivante. Soit X une sous-variété algébrique irréductible de $\mathcal{A}$, telle que $\dim_{\mathcal{C}}(X) > 0$, définie sur $\overline{k}$. Si X ne contient pas de translatés de sous-$T^{j(\mathcal{A})}-$modules de $\mathcal{A}$ de dimension > 0 par des points de torsion, alors X ne possède qu'un nombre fini de points de torsion de $\mathcal{A}$.*

Définition 2.2.9. *On convient d'appeler, dorénavant,* ***classe de torsion*** *toute translatée :*

$$\overline{x} + \mathcal{B};$$

d'un sous-$T-$module $\mathcal{B}$ de $\mathcal{A}$ par un point de torsion.

2.2.1 Un pas vers la Conjecture 5

En général les puissances tensorielles d'un module de Carlitz constituent une classe de $T-$modules dont l'étude semble davantage renforcer l'hypothèse avancée dans la Conjecture 5. Nous commençons ici à étudier le comportement de tels $T-$modules dans le but de développer les calculs nécessaires à prouver finalement une première version de cette Conjecture, restreinte au cas où les éléments $a(T) \in A \setminus \{0\}$ sont des puissances de T. Soit $m \in \mathbb{N} \setminus \{0\}$. Un calcul direct montre que l'action de $\Phi(T^h)$ sur $\mathbb{G}_a^m$ est, quelque soit $h = 1, ..., m$, étant donné $l = m - h$, de la forme suivante :

$$\Phi(T^h)\begin{pmatrix} X_1 \\ \cdots \\ X_m \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^{h}\binom{h}{i}T^{h-i}X_{i+1} \\ \sum_{i=0}^{h}\binom{h}{i}T^{h-i}X_{i+2} \\ \cdots \\ \sum_{i=0}^{h}\binom{h}{i}T^{h-i}X_{i+l} \\ \sum_{i=0}^{h-1}\binom{h}{i}T^{h-i}X_{i+l+1} + X_1^q \\ \sum_{i=0}^{h-2}\binom{h}{i}T^{h-i}X_{i+l+2} + f_1(X_1^q, X_2^q) \\ \cdots \\ T^hX_m + f_{h-1}(X_1^q, X_2^q, \cdots, X_h^q) \end{pmatrix};$$

où $f_1, ..., f_{h-1}$ sont des polynômes linéaires à coefficients dans A en $X_1, ..., X_h$. Notons que si $h = m$ la première composante du vecteur que nous venons d'écrire est de la forme $\sum_{i=0}^{m-1}\binom{m}{i}T^{m-i}X_{i+1}+X_1^q$. Si m est divisible par la caractéristique p du corps des fonctions k soit p^α la puissance maximale de p qui divise m. Nous avons donc que :

$$\Phi(T^{p^\beta})\begin{pmatrix}X_1\\ \cdots\\ X_m\end{pmatrix}=\begin{pmatrix}T^{p^\beta}X_1+X_{p^\beta+1}\\ T^{p^\beta}X_2+X_{p^\beta+2}\\ \cdots\\ T^{p^\beta}X_{p^\beta+1}+X_{2p^\beta+1}\\ \cdots\\ T^{p^\beta}X_{m-p^\beta+1}+X_1^q\\ \cdots\\ T^{p^\beta}X_m+f_{p^\beta-1}(X_1^q,\cdots,X_{p^\beta-1}^q)\end{pmatrix},\ \forall 1\leq\beta\leq\alpha.$$

Pour tout $1\leq\beta\leq\alpha$ nous avons que le sous-groupe algébrique :

$$\{(X_1,...,X_m)\in\mathbb{G}_a^m,\ \ X_{sp^\beta+1}=0,\ \ \forall s=0,...,m/p^\beta\}=(0\times\mathbb{G}_a^{p^\beta-1})^{m/p^\beta};$$

de $\mathbb{G}_a^m$ est donc stable sous l'action de T^{p^β}, mais pas sous celle de $T^{p^{\beta-1}}$ en général si $\beta>1$, et il est donc un sous-$T^{p^\beta}-$module de $C^{\otimes m}$ qui n'en est pas un sous-$T^{p^{\beta-1}}-$module. Nous remarquons par contre que dans le cas où $m=p^\alpha$ tout groupe algébrique de la forme $0^h\times\mathbb{G}_a^k$, où $m=h+k$, est un sous-T^p-module de $C^{\otimes m}$. D'un autre côté les calculs semblent indiquer que l'existence de sous-T^j-modules de $C^{\otimes m}$, où $j>m$, qui ne soient pas stables sous l'action de T^i pour au moins un nombre naturel $0<i\leq m$, est peu probable. D'un autre côté, nous pouvons remarquer aussi que si h n'est pas une puissance de p et p^β est la puissance maximale de p qui divise h, pour un nombre $\beta\in\mathbb{N}$ opportun, nous avons que :

$$p|\binom{h}{i},\ \ \forall i\neq sp^\beta,\ \ \forall s=0,...,h/p^\beta;$$

$$\binom{h}{sp^\beta}\equiv\binom{h/p^\beta}{s}\ \mathtt{mod}\ (p),\ \ \forall s=0,...,h/p^\beta.$$

Il s'ensuit que :

$$\Phi(T^h)\begin{pmatrix}X_1\\ \cdots\\ X_m\end{pmatrix}=\begin{pmatrix}T^hX_1+h/p^\beta T^{h-p^\beta}X_{p^\beta+1}+\cdots+h/p^\beta T^{p^\beta}X_{h-p^\beta+1}+X_{h+1}\\ \cdots\\ T^hX_2+h/p^\beta T^{h-p^\beta}X_{p^\beta+2}+\cdots+h/p^\beta T^{p^\beta}X_{h-p^\beta+2}+X_{h+2}\\ \cdots\\ T^hX_{h-p^\beta+1}+h/p^\beta T^{h-p^\beta}X_{h+1}+\cdots+h/p^\beta T^{p^\beta}X_m+X_1^q\\ \cdots\\ T^hX_m+f_{h-1}(X_1^q,\cdots,X_{h-1}^q)\end{pmatrix}.$$

Nous pouvons donc remarquer que tout sous-T^h-module de $C^{\otimes m}$ qui est un produit cartésien de puissances de 0 et de $\mathbb{G}_a$ est de la forme suivante :

$$\{(X_1,...,X_m)\in\mathbb{G}_a^m,\ \ X_1=X_{p^\beta+1}=\cdots=X_{h+1}=\cdots=X_{m-p^\beta+1}=0\};$$

et il est donc un sous-$T^{p^\beta}-$module aussi. Ce qui suggère finalement que $j(C^{\otimes m})=p^\alpha$. Le cas où $p\nmid m$ semble par contre suggérer l'absence de sous-T^j-modules de $C^{\otimes m}$ pour tout $j \in \mathbb{N}\setminus\{0\}$, ce qui nous conduit à supposer que dans une telle situation on ait que $j(C^{\otimes m}) = 1$. Il serait également intéressant d'établir dans ce cas que $j((C^{\otimes m})^h) = j(C^{\otimes m}) = 1$ pour tout $h \in \mathbb{N} \setminus \{0\}$, cas particulier de la question qu'on s'est posé à l'issue de l'exemple des puissances de modules de Drinfeld (voir après la Conjecture 5) puisqu'en particulier $(C^{\otimes m})^h$ n'est jamais simple pour $h > 1$.

Il est très intéressant de remarquer aussi que pour tout $a(T) \in A \setminus \{0\}$ et tout sous-T^j-module $\mathcal{B}$ de $C^{\otimes m}$ sous une des formes précédemment étudiées (produit cartésien de puissances de 0 et de $\mathbb{G}_a$), pour un certain $j \in \mathbb{N} \setminus \{0,1\}$ opportun, le sous-ensemble $\Phi(a(T))(\mathcal{B})$ de $\mathbb{G}_a^m$ reste un groupe algébrique et en particulier un sous-T^j-module de $C^{\otimes m}$. Ce qui nous donne une classe de sous-T^j-modules de $C^{\otimes m}$ issue des familles précédentes, qui n'est pas nécessairement constituée de produits cartésiens entre des puissances de 0 et des puissances de $\mathbb{G}_a$. Un exemple est donné dans le cas où $p = m = 2$ par :

$$\Phi(T)(0 \times \mathbb{G}_a) = \{(X,Y) \in \mathbb{G}_a^2, Y = TX\}.$$

Nous remarquons maintenant que tout sous-espace vectoriel H de $Lie(C^{\otimes m})$ stable sous l'action de la différentielle $d\Phi(a(T))$, pour un certain $a(T) \in A\setminus\{0\}$, est tel que $\overline{e}(H)$, qui n'est pas en général une sous-variété algébrique de $\mathbb{G}_a^m$ comme nous l'avons vu dans la Remarque 2.2.7, est stable sous l'action de $\Phi(a(T))$. Etant donné un sous-$a(T)-$module $\mathcal{B}$ de $C^{\otimes m}$, il est donc possible de vérifier s'il est aussi un sous-$b(T)-$module pour un $b(T) \in A \setminus \{0, a(T)\}$, c'est le cas si et seulement si $d\Phi(b(T))Lie(\mathcal{B}) \subseteq Lie(\mathcal{B})$. On a que :

$$d\Phi(T) = TI_m + N;$$

où $N \in \mathbb{F}_q^{m,m}$ est telle que $N^m = 0$. Le développement de la puissance du binôme :

$$d\Phi(T)^j = (TI_m + N)^j;$$

montre que pour tout $j > m$:

$$d\Phi(T^j)\begin{pmatrix} z_1 \\ \cdots \\ z_m \end{pmatrix} = d\Phi(T)^j\begin{pmatrix} z_1 \\ \cdots \\ z_m \end{pmatrix} = \begin{pmatrix} T^j z_1 + \binom{j}{1}T^{j-1}z_2 + \cdots + \binom{j}{m-1}T^{j-m+1}z_m \\ T^j z_2 + \binom{j}{1}T^{j-1}z_3 + \cdots + \binom{j}{m-2}T^{j-m+2}z_m \\ \cdots \\ T^j z_m \end{pmatrix}.$$

Un calcul rapide montre alors comment la condition suivante :

$$\binom{j}{i} \equiv \binom{m}{i} \ \mathtt{mod}\ (p), \ \ \forall i = 1, ..., m-1;$$

est suffisante pour que tout sous-T^j-module de $C^{\otimes m}$ soit aussi un sous-T^m-module.

Un tel exemple nous indique le résultat suivant.

Théorème 2.2.10. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module abélien et uniformisable défini sur un corps de fonctions $\mathcal{F}$ contenant k. Il existe alors $j(\mathcal{A}) \in \mathbb{N} \setminus \{0\}$, ne dépendant que de $\mathcal{A}$, tel que tout sous-T^j-module de $\mathcal{A}$ est un sous-$T^{j(\mathcal{A})}-$module, quelque soit $j \in \mathbb{N} \setminus \{0\}$.*

Démonstration. Suite à la Définition 2.1.1 nous savons qu'il existe un nombre entier $m(\mathcal{A}) \in \mathbb{N} \setminus \{0\}$, ne dépendant que de $\mathcal{A}$, tel que la différentielle de $\mathcal{A}$ est de la forme suivante :

$$d\Phi(T) = TI_m + N;$$

où $N \in \mathcal{F}^{m,m}$ est une matrice nilpotente d'ordre $m(\mathcal{A})$ (ce qui veut dire que $N^{m(\mathcal{A})} = 0$ et $N^{m(\mathcal{A})-1} \neq 0$). Soit donc $b(\mathcal{A}) \in \mathbb{N} \setminus \{0\}$ le plus petit entier naturel tel que :

$$m(\mathcal{A}) \leq p^{b(\mathcal{A})}.$$

Soit $\mathcal{B}$ un sous-T^n-module de $\mathcal{A}$, où $n \in \mathbb{N} \setminus \{0\}$ est tel que $n > p^{b(\mathcal{A})}$. Soit donc $n_1 := n - p^{b(\mathcal{A})}$. Il s'ensuit que :

$$d\Phi(T^n) = (TI_m + N)^n = T^{p^{b(\mathcal{A})}}(TI_m + N)^{n_1}.$$

Comme $\mathcal{B}$ est un sous-T^n-module de $\mathcal{A}$ il s'ensuit que $Lie(\mathcal{B})$ est stable sous l'action de la différentielle $d\Phi(T^n)$. Soient donc $f_1, ..., f_s$, pour un $s \in \mathbb{N} \setminus \{0\}$ opportun, des formes linéaires à m indéterminées et à coefficients dans $\mathcal{C}$ telles que :

$$Lie(\mathcal{B}) = \{\overline{z} \in Lie(\mathcal{A}) \simeq \mathcal{C}^m, \;\; f_1(\overline{z}) = \cdots = f_s(\overline{z}) = 0\}.$$

Soit $\overline{z} \in Lie(\mathcal{B})$. Comme :

$$d\Phi(T^n)(\overline{z}) = (TI_m + N)^{n_1}(T^{p^{b(\mathcal{A})}}\overline{z}) \in Lie(\mathcal{B});$$

et comme :

$$f_i(d\Phi(T^n)(\overline{z})) = 0, \;\; \forall i = 1, ..., s;$$

il s'ensuit que :

$$f_i(T^{p^{b(\mathcal{A})}}(TI_m + N)^{n_1}(\overline{z})) = T^{p^{b(\mathcal{A})}} f_i((TI_m + N)^{n_1}(\overline{z})) = 0, \;\; \forall i = 1, ..., s;$$

puisque $f_1, ..., f_s$ sont $\mathcal{C}-$linéaires et $T^{p^{b(\mathcal{A})}} \in \mathcal{C}$. Par conséquent :

$$d\Phi(T^{n_1})(Lie(\mathcal{B})) = (TI_m + N)^{n_1}(Lie(\mathcal{B})) \subseteq Lie(\mathcal{B}).$$

Il s'ensuit que $\mathcal{B}$ est stabilisé par l'action de $\Phi(T^{n_1})$ et donc qu'il est un sous-$T^{n_1}-$module de $\mathcal{A}$, puisqu'il est déjà par hypothèse un sous-groupe algébrique de $\mathbb{G}_a^m$. Si $n_1 > p^{b(\mathcal{A})}$ nous répétons le même raisonnement jusqu'à ce que nous trouvions un nombre entier $n' \in \mathbb{N} \setminus \{0\}$ tel que $n' \leq p^{b(\mathcal{A})}$ pour lequel on ait que $Lie(\mathcal{B})$ est un sous-$T^{n'}-$module de $\mathcal{A}$. Nous pouvons donc supposer sans perte de généralité que tout sous-T^n-module $\mathcal{B}$ de $\mathcal{A}$ pour un certain $n \in \mathbb{N} \setminus \{0\}$ soit tel que $n \leq p^{b(\mathcal{A})}$. L'ensemble suivant :

$$S := \{n \in \mathbb{N} \setminus \{0\}, \;\; \exists \mathcal{B} <_n \mathcal{A}\};$$

où nous indiquons avec la notation $\mathcal{B} <_n \mathcal{A}$ que $\mathcal{B}$ est sous-T^n-module de $\mathcal{A}$ avec n minimal, est donc fini. Nous souvenant du fait que si $\mathcal{B}$ est un sous-T^n-module de $\mathcal{A}$ alors il est aussi un sous-$T^{an}-$module pour tout $a \in \mathbb{N} \setminus \{0\}$, un choix possible de $j(\mathcal{A})$ est le suivant :

$$j(\mathcal{A}) = PPCM\{n \in S\}.$$

□

2.3 Points de torsion et variétés

Ici nous présentons la stratégie d'attaque à la Conjecture 6, fondée sur les idées contenues dans le travail de J. Pila et J. Wilkie [PW]. Essentiellement nous rapporterons la question dans le langage des variétés analytiques dans $\mathcal{C}^m$, périodiques par rapport à Λ et soumises à l'action de A par la multiplication usuelle. Tous les $T-$modules traités seront toujours supposés être abéliens et uniformisables.

La méthode suivie par J. Pila et U. Zannier dans [PZ] pour montrer la Conjecture de Manin-Mumford classique (sous une forme plus faible) se base sur un raisonnement par l'absurde. Soit $\mathcal{A}$ une variété abélienne et X une sous-variété algébrique de $\mathcal{A}$ ne contenant aucune translatée par un point de torsion d'une sous-variété abélienne non triviale de $\mathcal{A}$. Le Théorème principal contenu dans [PW] donne une majoration du nombre des points de $N-$torsion (où $N \in \mathbb{N} \setminus \{0\}$) de $\mathcal{A}$ contenus en X en fonction de leur ordre de torsion N. D'un autre côté un corollaire au résultat de D. Masser ([Mas2], Corollary page 156) donne une minoration du même nombre toujours en fonction de N et de manière que si les points de torsion de $\mathcal{A}$ contenus dans X sont infinis, en faisant tendre à l'infini leur ordre de torsion les deux inégalités deviennent incompatibles.

Nous souhaitons répéter un tel raisonnement dans le cadre des $T-$modules abéliens et uniformisables. Dans ce paragraphe nous nous occuperons de fournir une majoration du nombre des points de $a(T)-$torsion (où $a(T)$ est un élément dans $A\setminus\{0\}$) d'un $T-$module $\mathcal{A}$, contenus dans une sous-variété algébrique de ce dernier qui respecte les hypothèses de la Conjecture 6, en fonction de $|a(T)|_{1/T}$. Un tel résultat sera donc notre analogue (voir Théorème 2.3.8) au Théorème principal montré par J. Pila et J. Wilkie dans [PW] dans le cas des variétés abéliennes. Nous adapterons leur méthode à notre situation.

A toute variété abélienne de dimension m est associé un espace tangent isomorphe à $\mathbb{C}^m$ à travers un revêtement topologique induit par les fonctions abéliennes, qui projecte cet espace dans la variété, de façon analogue au comportement de la fonction exponentielle par rapport aux $T-$modules, comme expliqué avant. La méthode offerte par le travail de J. Pila et U. Zannier se base sur la correspondance biunivoque entre les sous-variétés abéliennes d'une variété abélienne fixée et leurs espaces tangents, qu'on sait être exactement les sous-espaces de l'espace tangent de la variété de départ, tels que le noyau du revêtement qu'on a décrit (qui est un réseau à $2m$ générateurs sur $\mathbb{R}$) les intersecte de manière à détérminer un réseau de rang maximal.

Malheureusement une telle construction ne reste pas valable dans le cas des $T-$modules. En effet la correspondance entre sous-variétés abéliennes et sous-espaces de l'espace tangent, est démontrée (de manière pas évidente) grâce aux conséquences du principe GAGA (dont il existe un analogue en Géométrie Rigide qui peut trouver application dans notre situation) et du Théorème de Chow, qui ne trouve au contraire pas d'application dans notre situation suite à la non-compacité des $T-$modules. Dans notre cas, nous développons l'étude qui suit.

Suite au Lemme 2.1.37 nous pouvons voir la fonction exponentielle en tant que morphisme de $A-$modules $L-$entier sous la forme suivante :

$$\overline{e} : Lie(\mathcal{A})(\mathcal{C}) \to \mathcal{A}(\mathcal{C}).$$

Comme déjà expliqué dans la Remarque 2.2.7, nous avons démontré qu'il existe $j \in \mathbb{N}\backslash\{0\}$ tel que la différentielle de $\Phi(T^j)$ est T^j. Quitte à étendre éventuellement le corps $\mathcal{F}$ des coefficients de Φ, on remplacera dorénavant T par T^j. L'expression "'$T-$module"' indiquera donc en effet un T^j-module. L'exponentielle sera alors telle que :

$$\overline{e}(T\overline{z}) = \Phi(T)(\overline{e}(\overline{z}));$$

pour tout $\overline{z} \in Lie(\mathcal{A})(\mathcal{C})$. Dans le Lemme 2.1.37 on a construit un isomorphisme :

$$\mathcal{A}(\mathcal{C}) \simeq (k_\infty/A)^d \bigoplus Lib;$$

en y associant les projections triviales π_1 et π_2 de $\mathcal{A}(\mathcal{C})$ sur ses parties que nous appelons respectivement **de torsion** et **libre**, quitte à composer la fonction exponentielle $\overline{e}$ par l'isomorphisme ϕ que nous avons introduit dans le Théorème 2.1.38. En restreignant ces isomorphismes et ces projections aux points $L-$rationnels de $\mathcal{A}$ nous obtenons que :

$$\mathcal{A}(L) \simeq (k_\infty/A)^d \bigoplus Lib(L).$$

On remarque que $\pi_2(\Lambda) = \overline{0}$, ce qui implique que $\Lambda \subset \pi_1(\phi(Lie(\mathcal{A})(L))) = \Pi$. En particulier, la partie de torsion de $Lie(\mathcal{A})(\mathcal{C})$ introduite dans le Lemme 2.1.37 coïncide exactement (point par point) avec Π. Nous identifierons souvent dorénavant Λ et $\pi_1(\phi(\Lambda)) = A^d$.

Lemme 2.3.1. *Toute classe de torsion $\overline{x} + \mathcal{B}$ relative à un $T-$module $\mathcal{A}$ de dimension m et réseau Λ, où $\overline{x}$ et $\mathcal{B}$ sont respectivement un point de torsion et un sous-$T-$module de $\mathcal{A}$, correspond à un sous-espace affine H de $\mathcal{C}^m$ de la façon qui suit*[4] *:*

$$\overline{e}(\overline{y} + H) = \overline{x} + \mathcal{B};$$

où $\overline{y} \in \overline{e}^{-1}(\overline{x})$ et $\overline{e}(H) = \mathcal{B}$. De plus, $\Lambda \cap H$ a un rang strictement inférieur à celui de Λ. Donc, non seulement $\dim_{\mathcal{C}}(H) < m$, mais $\dim_{k_\infty}(\phi(H(L)) \cap \Pi) < d$.

Démonstration. A chaque sous-$T-$module $\mathcal{B}$ de $\mathcal{A}$ on associe son (unique) espace tangent $H = \overline{e}^{-1}(\mathcal{B}) = Lie(\mathcal{B})$ comme expliqué dans la Remarque 2.1.18, se souvenant du fait que nous sommes en train de supposer l'exponentielle surjective. Si $\overline{x}$ est un point de torsion de $\mathcal{A}$ on choisit un élément $\overline{y} \in \overline{e}^{-1}(\overline{x})$ dans $Lie(\mathcal{A})$. La $\mathbb{F}_q-$additivité de la fonction exponentielle implique que :

$$\overline{e}(\overline{y} + H) = \overline{x} + \mathcal{B}.$$

Nous montrons maintenant la propriété des réseaux associés. On a que :

$$\rho(\Lambda \cap H) = \rho(\phi(\Lambda) \cap \phi(H(L))) \leq \rho(\Lambda);$$

4. Nous soulignons que la correspondance entre sous-$T-$modules de $\mathcal{A}$ et sous-espaces vectoriels de $Lie(\mathcal{A})$ induite par l'exponentielle n'est pas biunivoque. Si H est un sous-espace vectoriel de $Lie(\mathcal{A})$ invariant par l'action de la différentielle de Φ, $\overline{e}(H)$ n'est pas forcément un sous-$T-$module de $\mathcal{A}$. Il est en effet un groupe additif stable sous l'action de Φ, mais pas une sous-variété algébrique a priori.

de façon évidente puisque $\phi(\Lambda) \cap \phi(H(L)) \subset \phi(\Lambda)$. Si les deux rangs étaient égaux, les deux réseaux seraient engendrés par le même nombre de périodes, qui sont alors dans les deux cas une $k_\infty-$base de $\phi(H(L)) \cap \Pi$. S'il existait alors $\lambda \in \phi(\Lambda) \setminus \phi(H(L))$, il serait $A-$combinaison linéaire des périodes. Mais comme ces dernières sont encore une base de $\phi(H(L)) \cap \Pi$, on a forcément que $\lambda \in \phi(H(L)) \cap \Pi$ et, par conséquent, $\phi(\Lambda) = \phi(\Lambda) \cap \phi(H(L))$. S'agissant de $T-$modules à exponentielle surjective ils sont identifiés, à isomorphisme près, avec leur propre réseau, ce qui implique que $\mathcal{A} = \mathcal{B}$, donc une contradiction. $\square$

2.3.1 Majoration du nombre des points de torsion

Soit X une sous-variété algébrique du $T-$module $\mathcal{A}$, comme dans les hypothèses de la Conjecture 6. Soit donc :

$$Y = \overline{e}^{-1}(X);$$

comme introduit dans le Théorème 2.1.38. Grâce à ce Théorème nous savons que $Y'(k_\infty)$ est un sous-ensemble pas vide et $k_\infty-$entier de $k_\infty^{mn} = \phi(Lie(\mathcal{A})(L))$. Nous définissons aussi l'ensemble qui suit :

$$Z := Y'(k_\infty) \cap \Pi \subset k_\infty^d \times \{\overline{0}\}.$$

Nous remarquons que Z est un sous-ensemble $k_\infty-$entier dans k_∞^d puisqu'il est l'intersection de deux ensembles $k_\infty-$entiers.

On sait que :

$$\mathcal{A}(\mathcal{C})_{tors.} = \bigcup_{a(T)\in A\setminus\{0\}} \mathcal{A}(\mathcal{C})[a(T)] = \bigcup_{a(T)\in A\setminus\{0\}} \{\overline{x} \in \mathcal{A}(\mathcal{C}), \Phi(a(T))(\overline{x}) = 0\}.$$

Nous définissons alors, pour tout $a(T) \in A \setminus \{0\}$:

$$Y[a(T)] := \{\overline{y} \in Y, a(T)\overline{y} \in \Lambda\};$$

et :

$$Y_{tors.} := \overline{e}^{-1}(\mathcal{A}(\mathcal{C})_{tors.}) \cap Y = \bigcup_{a(T)\in A\setminus\{0\}} Y[a(T)] = \bigcup_{a(T)\in A\setminus\{0\}} \{\overline{y} \in Y, a(T)\overline{y} \in \Lambda\}.$$

Lemme 2.3.2. *Avec toutes les données précédentes nous définissons :*

$$\Lambda_Z := Z \cap \Lambda.$$

Alors Z/Λ_Z est un compact.

Démonstration. Nous remarquons que :

$$k_\infty/A \simeq \frac{1}{T}\mathbb{F}_q[[\frac{1}{T}]];$$

comme k_∞ est un corps local tout disque ouvert (et à la fois fermé) dans sa base topologique canonique est compact, donc en particulier celui-ci :

$$\{x \in k_\infty, v_{1/T}(x) > 0\} \simeq \frac{1}{T}\mathbb{F}_q[[\frac{1}{T}]].$$

L'espace topologique quotient k_∞/A est donc compact. En particulier, le produit $(k_\infty/A)^d$ sera compact lui aussi. L'isomorphisme décrit dans le Théorème 2.1.38 nous permet de voir Z/Λ_Z en tant que sous-ensemble de $(k_\infty/A)^d$. Comme la topologie induite sur k_∞^d par la valuation $1/T-$adique est métrique, un sous-ensemble de k_∞^d est fermé par rapport à celle-ci si et seulement s'il est séquentiellement fermé. Nous considérons une suite convergente dans k_∞^d contenue dans Z. Soit $\overline{z}_0$ la limite d'une telle suite. Sans perdre en généralité nous supposons que cette suite est contenue dans un ouvert borné V de Z où Z s'exprime en tant que lieu de zéros d'un nombre fini de fonctions $k_\infty-$entières $f_1, ..., f_r$. Nous supposons aussi à une translation près que $\overline{0} \in V$. Soit alors, pour tout $j = 1, ..., r$, $f_j(\overline{z}) = \sum_{i\geq 0}\sum_{\mu\in\Lambda_d(i)} a_\mu \overline{z}^\mu$ l'expression de $f_j : k_\infty^d \to k_\infty$ sur un disque ouvert B_R de $\overline{0} \in k_\infty^d$, de rayon $R > 0$ dont l'intersection avec Z contient V. Pour tout $\epsilon > 0$ il existe alors $\overline{z}_n$ faisant partie d'une telle suite, tel que $||\overline{z}_0 - \overline{z}_n||_\infty < \epsilon$ (nous rappelons que pour tout $\overline{z} = (z_1, ..., z_d) \in k_\infty^d$ où $d > 1$ nous avons défini $||\overline{z}||_\infty = \max_{i=1,...,d}\{|z_i|_{1/T}\}$). Nous appelons dorénavant $f := f_j$ comme ce raisonnement est le même quelque soit j entre 1 et r. Alors :

$$|f(\overline{z}_0) - f(\overline{z}_n)|_{1/T} = \left|\sum_{i\geq 1}\sum_{\mu\in\Lambda_d(i)} a_\mu(\overline{z}_0^\mu - \overline{z}_n^\mu)\right|_{1/T} \leq \max_{i\geq 1, \mu\in\Lambda_d(i)}\{|a_\mu|_{1/T}|\overline{z}_0^\mu - \overline{z}_n^\mu|_{1/T}\}.$$

Nous remarquons qu'une telle borne finie existe suite à l'hypothèse de convergence de la série. On a que :

$$|\overline{z}_0^\mu - \overline{z}_n^\mu|_{1/T} < \epsilon\left|\sum_{|\eta|+|\rho|=|\mu|-1} \overline{z}_0^\eta \overline{z}_n^\rho\right|_{1/T} < \epsilon R^{|\mu|-1};$$

quelque soit $\mu \in \mathbb{N}^d$, $|\mu| \geq 1$. L'hypothèse de convergence de f sur V implique que :

$$\lim_{|\mu|\to+\infty} a_\mu R^{|\mu|} = 0;$$

quitte à remplacer éventuellement R par n'importe quel nombre $0 < R' < R$. Par conséquent :

$$|f(\overline{z}_0) - f(\overline{z}_n)|_{1/T} < \epsilon \max\{|a_\mu| R^\mu\} < \epsilon M;$$

pour un certain $M > 0$ ne dépendant que de f. Donc, il existe $M > 0$ ne dépendant que de f tel que pour tout $\epsilon > 0$ on ait que :

$$|f(\overline{z}_0)|_{1/T} = |f(\overline{z}_0) - f(\overline{z}_n)|_{1/T} < \epsilon M;$$

ce qui prouve que $f(\overline{z}_0) = 0$. L'ensemble Z est alors fermé, ce qui implique que Z/Λ_Z est aussi fermé dans $(k_\infty/A)^d$ par rapport à la topologie quotient. Comme celui-ci est un compact nous avons ainsi la compacité de Z/Λ_Z. □

Soit $a(T) \in A \setminus \{0\}$ et S un sous-ensemble quelconque de $Lie(\mathcal{A})(\mathcal{C})$. On appelle :

$$S[a(T)] := \overline{e}^{-1}(\mathcal{A}[a(T)]) \cap S.$$

Nous nous rappelons d'avoir identifié précédemment Λ avec A^d dans k_∞^d par la projection :

$$\pi_1 \circ \phi : Lie(\mathcal{A})(\mathcal{C}) \twoheadrightarrow k_\infty^d.$$

Nous avons vu également que cette projection a pour image exactement la partie de torsion de $Lie(\mathcal{A}(\mathcal{C}))$ qui suit de la décomposition décrite dans le Lemme 2.1.37. Quitte à identifier pour simplifier la notation S et $\phi(S)$ on a par conséquent que :

$$\pi_1(S[a(T)]) = \{\overline{z} \in \pi_1(S)(k), a(T)\overline{z} \in A^d \simeq \Lambda\} =$$

$$= \{\overline{z} = (\frac{\alpha_1}{\beta_1}, ..., \frac{\alpha_d}{\beta_d}) \in \pi_1(S)(k), PPCM(\{\beta_i\}_{i=1,...,d})|a(T)\};$$

$$\pi_2(S[a(T)]) = \{\overline{z} \in \pi_2(S), a(T)\overline{z} = 0\} = \{\overline{0}\} \texttt{ ou } \emptyset.$$

On en déduit que :

$$S[a(T)] = \emptyset \texttt{ si } \overline{0} \notin \pi_2(S);$$

tandis que si $S[a(T)] \neq \emptyset$ (autrement dit, si $\overline{0} \in \pi_2(S[a(T)])$), il existe l'identification d'ensembles suivante :

$$S[a(T)] \simeq \{\overline{z} = (\frac{\alpha_1}{\beta_1}, ..., \frac{\alpha_d}{\beta_d}) \in \pi_1(S)(k), PPCM(\{\beta_i\}_{i=1,...,d})|a(T)\} \times \{\overline{0}\}.$$

Nous allons utiliser une telle description pour étudier le nombre des points de torsion dans X, en supposant que X ne contient pas de classes de torsion. Le Lemme 2.3.1 nous permet en effet de nous ramener à étudier ce problème dans $Lie(\mathcal{A})$ où l'ensemble correspondant à X est Y. Nous remarquons que nous pouvons supposer $\overline{0} \in X$ dorénavant, puisque le cas contraire nous amène à la situation triviale où $Y_{tors.} = \emptyset$.

Soit X une sous-variété algébrique du $T-$module $\mathcal{A}$ abélien et uniformisable comme dans les hypothèses de la Conjecture 6. Etudier les points de $a(T)-$torsion de $\mathcal{A}$ contenus dans X est alors équivalent à étudier l'ensemble $Y[a(T)] \subset Lie(\mathcal{A})$ et, suite à l'identification entre la partie de torsion de $Lie(\mathcal{A}(\mathcal{C}))$ et $\pi_1(\phi(Lie(\mathcal{A}(L)))) = k_\infty^d$ qui suit du Théorème 2.1.38 point 5, c'est équivalent aussi à étudier les points de $Y(L)[a(T)]$. Comme dans ce Théorème nous avons montré que :

$$Y(L)[a(T)] \simeq Y'(k_\infty)[a(T)] = \{\overline{z} = (\frac{\alpha_1}{\beta_1}, ..., \frac{\alpha_d}{\beta_d}) \in k^d, PPCM(\{\beta_i\}_{i=1,...,d})|a(T)\} \times \{\overline{0}\};$$

l'ensemble $Y(L)[a(T)]$ est finalement en correspondance biunivoque avec l'ensemble qui suit :

$$Z[a(T)] := \{\overline{z} = (\frac{\alpha_1}{\beta_1}, ..., \frac{\alpha_d}{\beta_d}) \in k^d, PPCM(\{\beta_i\}_{i=1,...,d})|a(T)\}.$$

En particulier, nous avons que :

$$Y'(k_\infty)[a(T)] = Z[a(T)] \times \{\overline{0}\}.$$

Nous définissons aussi l'ensemble suivant :

$$Z_{tors.} := \bigcup_{a(T) \in A \setminus \{0\}} Z[a(T)].$$

Remarque 2.3.3. *Soit X une sous-variété algébrique d'un $T-$module $\mathcal{A}$ abélien et uniformisable comme dans les hypothèses de la Conjecture 6. L'ensemble des points de $a(T)-$torsion de $\mathcal{A}$ qui sont contenus dans X est donc en correspondance biunivoque avec l'ensemble qui suit :*

$$Z(k,[a(T)]) := \{(\frac{\alpha_1}{\beta_1},...,\frac{\alpha_d}{\beta_d}) \in Z[a(T)], \forall i=1,...,d, |\alpha_i|_{1/T} \leq |a(T)|_{1/T}\}.$$

Démonstration. En effet, les points $(\alpha_1/\beta_1,...,\alpha_d/\beta_d)$ de $Z[a(T)]$ (qui sont $k-$rationnels) sont par définition de ce dernier tels que $\beta_i|a(T)$ pour tout $i=1,...,d$. Or, comme A est un anneau euclidien par rapport à la valuation $1/T-$adique, tout $\alpha_i \in A$ tel que $|\alpha_i|_{1/T} \geq |a(T)|_{1/T}$ s'exprime uniquement sous la forme $\alpha_i = k(T)a(T)+r(T)$, où $k(T) \in A \setminus \{0\}$ et $r(T) \in A$ tel que $|r(T)|_{1/T} < |a(T)|_{1/T}$. La division par l'élément $\beta_i|a(T)$ nous donne alors $\alpha_i/\beta_i = (k(T)a(T)/\beta_i) + (r(T)/\beta_i)$ qui est bien de la forme $r(T)/\beta_i + \lambda$ avec $\lambda \in A$ et $|r(T)|_{1/T} \leq |\beta_i|_{1/T} \leq |a(T)|_{1/T}$. Suite à l'identification de X par $Y/(\Lambda \cap Y)$ qui suit du Lemme 2.1.37 et à celle de $Y(L)[a(T)]$ par $Y'(k_\infty)[a(T)]$ qui suit du Théorème 2.1.38 point 5, nous pouvons identifier finalement les points de $a(T)-$torsion de X par les points de $Y'(k_\infty)[a(T)]/(A^d \times \{\overline{0}\})$. L'ensemble des points de $a(T)-$torsion de la sous-variété algébrique X de $\mathcal{A}(\mathcal{C})$ n'est donc pas identifié avec $Z[a(T)]$ mais avec $Z(k,[a(T)])$, ce qui nous permet de nous limiter à un sous-ensemble précis de $Z[a(T)]$, dont la compacité suit du Lemme 2.3.2. Nous supposerons ainsi $|\alpha_i|_{1/T} < |a(T)|_{1/T}$ sans aucune perte de généralité. $\square$

On définit par ailleurs, étant donné S ensemble quelconque dans $\pi_1(\phi(Lie(\mathcal{A})))$ et $a(T) \in A$ de degré δ_a en T :

$$S(k,a(T)) := \{\overline{z} \in S(k), \widetilde{H}(\overline{z}) \leq |a(T)|_{1/T}\};$$

où $\widetilde{H}$ est une fonction définie comme il suit :

$$\widetilde{H} : k^d \to q^{\mathbb{Z}};$$

$$(z_1,...,z_d) \mapsto \max_{i=1,...,d}\{H(z_i)\};$$

où H est la hauteur absolue définie sur les points $k-$rationnels de k_∞^d (dont la hauteur logarithmique introduite dans le premier chapitre en est le logarithme en base q, voir [BG]). Nous remarquons que :

$$Z(k,a(T)) \times \{\overline{0}\} \subset Y'(k_\infty)(k,a(T)).$$

Comme la définition de la hauteur absolue H sur k est telle que :

$$H(z^{-1}) = H(z);$$

pour tout point $z = \frac{\alpha}{\beta} \in k$, où $\alpha, \beta \in A \setminus \{0\}$ sont premiers entre eux, en définissant pour tout $\overline{z} = (z_1,...,z_d) \in k^d \setminus \{\overline{0}\}$ son élément **inverse** de la façon suivante :

$$\overline{z}^{-1} := (z_1^{-1},...,z_d^{-1});$$

nous remarquons que :

$$\widetilde{H}(\overline{z}^{-1}) = \widetilde{H}(\overline{z}); \tag{2.7}$$

pour tout $\overline{z} \in k^d \setminus \{\overline{0}\}$.

Remarque 2.3.4. *Nous avons :*

$$S(k, [a(T)]) \subset S(k, a(T));$$

pour tout sous-ensemble S de $\phi(Lie(\mathcal{A}(\mathcal{C})))$ et tout $a(T) \in A \setminus \{0\}$ comme décris avant.

Démonstration. En effet, quitte à idéntifier S par $\pi_1(S)$, si $\overline{z} \in S(k, a(T))$ alors $\overline{z} = (\frac{\alpha_1}{\beta_1}, ..., \frac{\alpha_d}{\beta_d})$, où $\beta_i \neq 0$, $PGCD(\alpha_i, \beta_i) = 1$, $\beta_i | a(T)$, pour tout $i = 1, ..., d$. Puisque nous avons montré dans la Remarque 2.3.3 qu'il est possible de supposer sans perte de généralité que $|\alpha_i|_{1/T} < |a(T)|_{1/T}$ pour tout $i = 1, ..., d$, il s'ensuit facilement que $\widetilde{H}(\frac{\alpha_1}{\beta_1}, ..., \frac{\alpha_d}{\beta_d}) \leq |a(T)|_{1/T}$. □

Définition 2.3.5. *Nous appelons :*

$$N(S, [a(T)]) := |S(k, [a(T)])| \ \ \texttt{et} \ \ N(S, a(T)) := |S(k, a(T))|.$$

Nous avons alors les inégalités suivantes :

$$N(Z, [a(T)]) \leq N(Z, a(T)) \leq N(Y'(k_\infty), a(T)).$$

Nous donnons maintenant la définition d'ensemble **semi-algébrique** dans le cas d'un corps complet non archimédien, en reprenant la définition donnée dans [Sh], page 51, 100 dans le cas du corps des nombres réels $\mathbb{R}$. Comme sur un corps non-archimédien la relation d'ordre donnée par la valuation n'est pas totale, on modifiera la définition usuelle (qui est essentiellement celle du lieu des solutions d'inégalités polynomiales) comme il suit, en remplaçant en particulier ce le lieu de solutions par l'intersection de la variété algébrique avec un polydisque générique.

Définition 2.3.6. *Soit K corps de valuation complet et $n \in \mathbb{N} \setminus \{0\}$. Un* ***ensemble semi-algébrique*** *dans K^n est l'intersection entre une variété algébrique dans K^n et un polydisque, qui est un produit cartésien de boules dans K à rayon éventuellement infini. Dans le cas où le rayon est infini pour toutes les boules on a le cas particulier où l'ensemble semi-algébrique est en effet une variété algébrique. Si S est sous-ensemble de K^n, on appelle ensemble semi-algébrique dans S toute intersection de S avec un ensemble semi-algébrique de K^n.*

Définition 2.3.7. *Soit Y' défini comme dans le Théorème 2.1.38 point 5. Si $\mathcal{A}$ et $\mathcal{B}$ sont deux $T-$modules, la notation $\mathcal{B} \leq \mathcal{A}$ indique que $\mathcal{B}$ est un sous-$T-$module de $\mathcal{A}$. La notation $\mathcal{B} < \mathcal{A}$ indique que cette inclusion est stricte. Pour tout sous-$T-$module strict $\mathcal{B} < \mathcal{A}$, nous définissons $H_{\mathcal{B}} := \phi(\overline{e}^{-1}(\mathcal{B})(L))$ et :*

$$S(\mathcal{A}) := \{\mathcal{B} < \mathcal{A}, \ \exists \overline{y} \in Y'(k_\infty)_{tors.}, \ \overline{y} + H_{\mathcal{B}} \subset Y'(k_\infty)\};$$

et, pour chaque $\mathcal{B} \in S(\mathcal{A})$:

$$Y'(k_\infty)_{tors.}(\mathcal{B}) := \{\overline{y} \in Y'(k_\infty)_{tors.}, \ \overline{y} + H_{\mathcal{B}} \subset Y'(k_\infty)\}.$$

1. *Nous appelons :*

$$Y'(k_\infty)^{tc} := \bigcup_{\mathcal{B} \in S(\mathcal{A})} \bigcup_{\overline{y} \in Y'(k_\infty)_{tors.}(\mathcal{B})} (\overline{y} + H_{\mathcal{B}}) \subset Y'(k_\infty).$$

2. *Nous appelons également* $Y'(k_\infty)^{ra}$ *l'union de toutes les sous-variétés algébriques connexes dans* $Y'(k_\infty)$ *de* $\dim_{k_\infty} > 0$.
3. *Nous appelons* $Y'(k_\infty)^{alg.}$, *ou* ***partie semi-algébrique*** *sur* k_∞ *de* $Y'(k_\infty)$, *l'union de tous les sous-ensembles semi-*$k_\infty-$*algébriques de* $Y'(k_\infty)$ *de* $k_\infty-$*dimension* > 0.

Nous remarquons que :

$$Y'(k_\infty)^{t.c.} \subset Y'(k_\infty)^{ra} \subset Y'(k_\infty)^{alg.}.$$

Il s'ensuit que l'hypothèse de la Conjecture 6 pour laquelle la sous-variété algébrique X de $\mathcal{A}$ ne contient pas de classes de torsion se traduit par la condition suivante :

$$Y'(k_\infty)^{t.c.} = \emptyset;$$

ce qui est impliqué par la condition suivante :

$$Y'(k_\infty)^{alg.} = \emptyset.$$

L'identification de ces deux ensembles fait partie des objectifs de nos projets de poursuite de ce travail (voir paragraphe 2.4) et constitue un point essentiel dans la stratégie que nous nous proposons de développer visant à prouver la Conjecture 6. Cette stratégie, qui est analogue dans le cas d'un $T-$module abélien et uniformisable à celle exploitée par J. Pila et U. Zannier dans [PZ] dans le cas des variétés abéliennes sur des corps des nombres, présente des difficultés importantes, que nous analyserons dans le paragraphe 2.4 à suivre. Nous nous proposons de montrer le Théorème suivant, analogue du résultat de J. Pila et J. Wilkie (voir [PW]) dans notre situation particulière, dont l'application à l'ensemble $Y'(k_\infty)$ que nous avons défini dans le Théorème 2.1.38 point 5 nous donnera le premier pas en direction d'une reconstruction de la preuve de J. Pila et U. Zannier que nous souhaitons appliquer à la Conjecture 6 :

Théorème 2.3.8. *Soit* $W \subset k_\infty^{nm}$ *un sous-ensemble* $k_\infty-$*entier de* k_∞^{nm} *tel qu'il est analytiquement paramétrisable sur* k_∞. *Pour tout nombre réel* $\epsilon > 0$, *il en existe un autre* $c = c(W, \epsilon) > 0$ *tel que, quelque soit* $a(T) \in A \setminus \{0\}$, *on a :*

$$N(W \setminus W^{alg.}, a(T)) \leq c|a(T)|_{1/T}^{\epsilon}.$$

Nous voulons appliquer le Théorème 2.3.8 à l'ensemble $B_1^{nm}(k_\infty) \cap Y'(k_\infty)$ que nous avons défini avant. Nous pouvons le faire suite au Théorème 2.1.43.

Comme nous le verrons plus loin on peut se ramener en effet à supposer sans perte de généralité que W soit compact et contenu dans le polydisque $B_1^{nm}(k_\infty)$. Dans tous les cas on peut répéter le même raisonnement localement pour toute translatée de $B_1^{nm}(k_\infty)$ qui intersecte $Y'(k_\infty)$ (en tenant compte que la dimension de chacun de ces espaces affinoïdes n'est pas toujours la même mais dans tous les cas $< nm$). Nous pourrons donc appliquer le Théorème 2.3.8 à l'ensemble $Y'(k_\infty)$ que nous avons construit précédemment. On commence, dans le but de prouver le Théorème 2.3.8, à montrer des résultats intermédiaires.

Lemme 2.3.9. *Soient* $h, d, \delta \in \mathbb{N}\setminus\{0\}$. *Soient* $D := D_d(\delta) := |\{\mu \in \mathbb{N}^d, \sum_{i=1}^d \mu_i \leq \delta\}|$ *et* $B := B(h, d, \delta) := \sum_{\beta=0}^b L_h(\beta)\beta + (D_d(\delta) - \sum_{\beta=0}^b L_h(\beta))(b+1)$, *où*

$L_h(\beta) := |\{\mu \in \mathbb{N}^h, \sum_{i=1}^h \mu_i = \beta\}|$ et b est l'unique nombre naturel (voir [P]) tel que $D_h(b) \leq D_d(\delta) \leq D_h(b+1)$. Soient :

$$\Phi_1, ..., \Phi_D : k_\infty^h \to k_\infty;$$

des fonctions analytiques. Pour tout sous-ensemble J compact et convexe de k_∞^h, il existe un nombre réel :

$$c = c(J, \Phi_1, ..., \Phi_D) > 0;$$

tel que, pour tout $U \subset k_\infty^h$ polydisque de rayon $r \leq 1$, et tous $\overline{z}_1, ..., \overline{z}_D \in J \cap U$:

$$|\det(\Phi_i(\overline{z}_j))|_{1/T} \leq cr^B.$$

Démonstration. Soit $\overline{z}_0 \in J \cap U$ différent de $\overline{z}_1, ..., \overline{z}_D$. Si $a, b \in \mathbb{N} \setminus \{0\}$, nous rappelons les notations introduites dans la Définition 2.1.20 :

$$\Lambda_a(b) := \{(\mu_1, ..., \mu_a) \in \mathbb{N}^a, \sum_{i=1}^a \mu_i = b\};$$

$$\Delta_a(b) := \bigcup_{i=1}^b \Lambda_a(i).$$

On appelle, alors, $D_a(b) := |\Delta_a(b)|$ et $L_a(b) := |\Lambda_a(b)|$. On sait (voir [P]) qu'il existe un unique $b \in \mathbb{N} \setminus \{0\}$ tel que :

$$D_h(b) \leq D_d(\delta) \leq D_h(b+1).$$

Comme les fonctions $\Phi_1, ..., \Phi_D$ sont pesudoanalytiques sur $B_1^h(k_\infty)$, il existe $\zeta \in B_{z_i, z_0} := B(z_0, |z_i - z_0|_{1/T})$ tel que, pour tout i, j entre 1 et D :

$$\Phi_i(\overline{z}_j) = \sum_{\mu \in \Delta_h(b)} \frac{\partial^\mu \Phi_i(\overline{z}_0)}{\partial \overline{z}^\mu} (\overline{z}_j - \overline{z}_0)^\mu + \sum_{\mu \in \Lambda_h(b+1)} \frac{\partial^\mu \Phi_i(\zeta)}{\partial \overline{z}^\mu} (\overline{z}_j - \overline{z}_0)^\mu.$$

Pour tout l entre 1 et D on considère les sous-matrices $l \times l$ dans $(\Phi_i(\overline{z}_j))_{i,j}$. Cette expression est donc une $k_\infty-$combinaison linéaire de $L_h(\beta)$ vecteurs de k_∞^l. En faisant varier i et j dans un sous-ensemble de l éléments de $\{1, ..., D\}$, on obtient une sous-matrice dans $k_\infty^{l \times l}$. Si $l > L_h(\beta)$, ses l colonnes seront forcément $k_\infty-$linéairement dépendantes. Et son déterminant sera 0. On peut donc calculer :

$$|\det(\Phi_i(\overline{z}_j))|_{1/T} = |\det(\sum_{\beta=0}^b (\sum_{\mu \in \Lambda_h(\beta)} \frac{\partial^\mu \Phi_i(\overline{z}_0)}{\partial \overline{z}^\mu} (\overline{z}_j - \overline{z}_0)^\mu) +$$

$$+ \sum_{\mu \in \Lambda_h(b+1)} \frac{\partial^\mu \Phi_i(\zeta)}{\partial \overline{z}^\mu} (\overline{z}_j - \overline{z}_0)^\mu)|_{1/T};$$

en développant par rapport aux lignes (ou colonnes) jusqu'aux sous-matrices jusqu'à l'ordre, respectivement, $L_h(\beta)$, pour $\beta = 0, ..., b+1$. Si on appelle, donc :

$$c = c(J, \Phi_1, ..., \Phi_D) := \max_{\overline{\zeta} \in J} \max_{i=1,...,D} \max_{\beta=0,...,b+1} \max_{\mu \in \Delta_h(b+1)} \{|\frac{\partial^\mu \Phi_i(\overline{\zeta})}{\partial \overline{z}^\mu}|_{1/T}\}; \quad (2.8)$$

sachant que $||\overline{z}_j - \overline{z}_0||_\infty \leq r$ pour tout $j = 1, ..., D$ il s'ensuit que :

$$|\det(\Phi_i(\overline{z}_j))|_{1/T} \leq cr^B;$$

où :

$$B = B(h, d, \delta) := \sum_{\beta=0}^{b} L_h(\beta)\beta + (D_d(\delta) - \sum_{\beta=0}^{b} L_h(\beta))(b+1).$$

□

Proposition 2.3.10. *Soient $h < d$ et $\delta \in \mathbb{N} \setminus \{0\}$. Il existe un nombre réel $\epsilon = \epsilon(h, d, \delta) > 0$ tel que, pour toute fonction analytique :*

$$\Phi : B_1^h(k_\infty) \to k_\infty^d;$$

si :

$$S := \Phi(B_1^h(k_\infty));$$

et $a(T) \in A$ tel que $|a(T)|_{1/T} \geq 1$, il existe un nombre réel $C = C(h, d, \delta, B_1^h(k_\infty), \Phi) > 0$, tel que l'ensemble $S(k, a(T))$ est contenu dans l'union d'au plus $C|a(T)|_{1/T}^{\epsilon}$ hypersurfaces dans k_∞^d de degré au plus δ. De plus, si δ tend vers $+\infty$, alors ϵ tend vers 0.

Démonstration. Nous appelons (en reprenant les notations introduites dans la preuve du Lemme 2.3.9) :

$$V = V(h, d, \delta) := \sum_{\beta=0}^{d} L_h(\beta)\beta;$$

$$\epsilon = \epsilon(h, d, \delta) := \frac{hV}{B}.$$

Quand h et d sont fixés on peut remarquer que si δ tend vers $+\infty$, alors ϵ tend vers 0. Soit $U \subset B_1^h(k_\infty)$ un polydisque de rayon $r \in q^{\mathbb{Z}}$ tel que $r \leq 1$. Soient $\overline{z}_1, ..., \overline{z}_D \in U \cap \Phi^{-1}(S(k, a(T)))$, où $D := D_d(\delta)$, pas forcément distincts. En exprimant :

$$\Phi := (\Phi_1, ..., \Phi_d);$$

avec :

$$\Phi_1, ..., \Phi_d : B_1^h(k_\infty) \to k_\infty;$$

fonctions analytiques, on restreint ces dernières à U. Pour tout $\mu \in \Delta_d(\delta)$, nous définissons (avec la notation de puissance symbolique déjà signalée dans la définition 2.1.20) :

$$\Phi_\mu := (\Phi_1, ..., \Phi_d)^\mu;$$

ce qui donne D fonctions analytiques :

$$\Phi_\mu : U \to k_\infty.$$

On remarque, alors, que tout polydisque dans k_∞^h, donc $B_1^h(k_\infty)$ en particulier, est convexe et compact pour la topologie $1/T-$adique dans k_∞^h. En effet, si $x, y \in B_1(k_\infty)$, le polydisque minimal $B_{x,y}$ contenant les deux est contenue dans $B_1(k_\infty)$ car étant données deux boules non disjointes, alors l'une d'elles est contenue dans l'autre. Par ailleurs, comme la valuation $1/T-$adique est une valuation discrète et que $\mathbb{F}_q \simeq \mathbb{F}_q[[1/T]]/(1/T)$ est un corps fini, k_∞ est un corps local et donc les boules dans ce dernier sont compactes. Comme un polydisque est un produit fini de compacts et convexes dans k_∞^h, il est forcément encore compact et convexe dans la topologie produit. Le polydisque $B_1^h(k_\infty)$ peut donc jouer le rôle de l'ensemble J dans le Lemme 2.3.9. En conséquence de ce dernier il existe $c(\{\Phi_\mu\}_{\mu\in\Delta_d(\delta)}) > 0$ tel que :

$$|\det(\Phi_\mu(\overline{z}_j))|_{1/T} \leq cr^B.$$

Or, comme $\overline{z}_1, ..., \overline{z}_D \in \Phi^{-1}(S(k, a(T)))$:

$$\det(a(T)\Phi_\mu(\overline{z}_j)) = a(T)^V \det(\Phi_\mu(\overline{z}_j)) \in A.$$

Si on choisit donc :

$$r < (c|a(T)|_{1/T}^V)^{-1/B};$$

on a :

$$|\det(\Phi_\mu(\overline{z}_j))|_{1/T} \leq cr^B < c((c|a(T)|_{1/T}^V)^{-1/B})^B = |a(T)|_{1/T}^{-V}.$$

Donc, $|a(T)^V \det(\Phi_\mu(\overline{z}_j))|_{1/T} < 1$ et cet élément est dans A. D'où :

$$\det(\Phi_\mu(\overline{z}_j)) = 0;$$

pour tous $\overline{z}_1, ..., \overline{z}_D \in U \cap \Phi^{-1}(S(k, a(T)))$. Nous montrons que cette annulation est équivalente à l'existence d'une hypersurface définie sur k_∞ de degré $\leq \delta$ dans k_∞^d qui contient les D points $\Phi(\overline{z}_j) \in k_\infty^d$, pour tout $j = 1, ..., D$. Si, en effet :

$$f(X_1, ..., X_d) = \sum_{\mu\in\Delta_d(\delta)} a_\mu (X_1, ..., X_d)^\mu = 0;$$

est l'équation d'une hypersurface (dont le degré est trivialement $\leq \delta$), qui est définie sur k_∞ et qui contient $\overline{P}_1 := \Phi(\overline{z}_1), ..., \overline{P}_D := \Phi(\overline{z}_D) \in k_\infty^d$, il s'ensuit que :

$$\sum_{\mu\in\Delta_d(\delta)} a_\mu \overline{P}_j^{\ \mu} = 0;$$

pour tout $j = 1, ..., D$. Ce qui donne une $k_\infty-$dépendance linéaire entre les lignes de la matrice suivante :

$$(\overline{P}_j^{\ \mu}) = (\Phi_\mu(\overline{z}_j));$$

pour tout $\mu \in \Delta_d(\delta)$, $j = 1, ..., D$. D'un autre côté, si nous supposons que :

$$\det(\overline{P}_j^{\ \mu}) = 0;$$

soit $l < D$ tel que le rang de la matrice :

$$(\overline{P}_j^{\ \mu})_{\mu\in\Delta_d(\delta), j\in\{1,...,D\}};$$

est l. Il existe donc un mineur $(A_{IJ})_{\mu\in I, j\in J}$ de la matrice $(\overline{P}_j^{\ \mu})$, où $I \subset \Delta_d(\delta)$ et $J \subset \{1, ..., D\}$ tel que $|I| = |J| = l$, de rang l. Puisque $l < D$ nous avons qu'il existe un $\mu^* \in \Delta_d(\delta) \setminus I$. Nous définissons :

$$f(X_1, ..., X_d) := \det \begin{pmatrix} A_{\mu J} \\ (X_1, ..., X_d)^\mu \end{pmatrix}_{\mu\in I\cup\{\mu^*\}}.$$

Nous voyons que $f(X_1, ..., X_d)$ est un polynôme défini sur k_∞ de degré $\leq \delta$. Il s'ensuit que :

$$f(\overline{P}_j) = \det \begin{pmatrix} A_{\mu J} \\ \overline{P}_j^{\ \mu} \end{pmatrix} = 0;$$

pour tout $\mu \in I \cup \{\mu^*\}$, $j = 1, ..., D$. En effet si $j \in J$ la matrice :

$$\begin{pmatrix} A_{\mu J} \\ \overline{P}_j^{\ \mu} \end{pmatrix} \in k_\infty^{l+1,l+1};$$

a deux lignes égales, alors que si $j \notin J$ le déterminant doit être 0 comme le rang de la matrice au départ est l. On en conclut que $\Phi(U) \cap S(k, a(T))$ est contenu, pour $r < (c|a(T)|_{1/T}^V)^{-1/B}$, dans une hypersurface de degré au plus δ. Nous choisissons donc r le plus grand élément dans $q^{\mathbb{Z}\setminus\mathbb{N}}$ à être $\leq (\frac{c}{2}|a(T)|_{1/T}^V)^{-1/B}$. Maintenant nous nous souvenons que la topologie $1/T-$adique fait de tout recouvrement par des boules d'un convexe de k_∞ une partition. Comme $r \in q^{\mathbb{Z}\setminus\mathbb{N}}$ il s'ensuit que $-\log r \in \mathbb{N} \setminus \{0\}$. Nous savons que :

$$B_1^1(k_\infty) = \{z \in k_\infty, v_{1/T}(z) \geq 0\} = \mathbb{F}_q[[1/T]];$$

$$B_r^1(k_\infty) = \{z \in k_\infty, v_{1/T}(z) \geq -\log r\} = (1/T^{-\log r})\mathbb{F}_q[[1/T]].$$

Il s'ensuit que :

$$|B_1^1(k_\infty)/B_r^1(k_\infty)| = q^{-\log r} = 1/r. \tag{2.9}$$

En particulier, le nombre de polydisques U de rayon r recouvrant $B_1^h(k_\infty)$ est :

$$|B_1^1(k_\infty)/B_r^1(k_\infty)|^h = r^{-h} \leq (\frac{c}{2}|a(T)|_{1/T}^V)^{h/B} = C|a(T)|_{1/T}^\epsilon;$$

où $C := (\frac{c}{2})^{h/B} > 0$. Ce qui prouve l'assertion. □

Nous nous proposons d'appliquer la Proposition 2.3.10 à l'ensemble $W \setminus W^{alg.}$ que nous avons introduit dans le Théorème 2.3.8, après en avoir donné une paramétrisation analytique. Par hypothèse nous avons un recouvrement analytique de W sur k_∞ dont l'intersection des images par $W \setminus W^{alg.}$ nous donne un recouvrement analytique de $W \setminus W^{alg.}$.

Nous allons maintenant prouver le Théorème 2.3.8 en appliquant la Proposition 2.3.10 au recouvrement analytique de $W \setminus W^{alg.}$ sur k_∞ que nous venons de construire.

Démonstration. On observe que :

$$W = W_1 \cup W_2;$$

où :

$$W_1 := W \cap B_1^{nm}(k_\infty);$$

et :

$$W_2 := W \setminus W_1.$$

Nous remarquons que $W_1 \neq \emptyset$ comme nous pouvons supposer sans perte de généralité que $\overline{0} \in X$ et donc que $\overline{0} \in W$, comme nous l'avons déjà précédemment remarqué. Comme W_1 et W_2 sont des sous-ensembles de W, si nous avons un recouvrement analytique de W d'ouverts homéomorphes à $B_1^{d(W)(k_\infty)}$, à plus forte raison ce sera le même pour W_1 et W_2. Nous avons que W_1 est un compact mais ca n'est pas le cas a priori pour W_2. Nous considérons la **fonction d'inversion** suivante :

$$(\cdot)^{-1} : W_2 \to k_\infty^{nm};$$
$$\overline{z} \mapsto \overline{z}^{-1};$$

où si $\overline{z}^{-1}$ est défini comme avant. Nous appelons W_2^{-1} l'image de W_2 par cette fonction. Nous remarquons qu'il s'agit d'une fonction bijective et analytique dans les deux sens entre W_2 et W_2^{-1}. La propriété (2.8) rend stable sous l'action de la fonction d'inversion l'ensemble des points $\overline{z} \in k_\infty^{nm}$ tels que $\widetilde{H}(\overline{z}) \leq |a(T)|_{1/T}$. Montrer le Théorème 2.3.8 pour W_2^{-1} est donc équivalent à le montrer pour W_2. Comme W_2^{-1} est un compact nous pouvons nous ramener à traiter deux compacts séparemment, à condition que le Théorème 2.3.8 sur W_1 et W_2 implique le même résultat pour W.

Soient donc $A, B, C \subset k_\infty^{nm}$ tels que $C = A \cup B$. On peut montrer que :

$$A^{alg.} \cup B^{alg.} \subset C^{alg.}.$$

Admettons que le Théorème 2.3.8 soit valable pour A et B. Alors, pour tout $\epsilon > 0$, ils existent $c_A(\epsilon), c_B(\epsilon) > 0$ tels que :

$$N(A \setminus A^{alg.}, |a(T)|_{1/T}) \leq c_A(\epsilon)|a(T)|_{1/T}^{\epsilon};$$

$$N(B \setminus B^{alg.}, |a(T)|_{1/T}) \leq c_B(\epsilon)|a(T)|_{1/T}^{\epsilon}.$$

Alors :

$$N(C \setminus C^{alg.}, |a(T)|_{1/T}) \leq N((A \cup B) \setminus (A^{alg.} \cup B^{alg.}), |a(T)|_{1/T}) \leq$$

$$\leq N(A \setminus A^{alg.}, |a(T)|_{1/T}) + N(B \setminus B^{alg.}, |a(T)|_{1/T}) \leq c_C(\epsilon)|a(T)|_{1/T}^{\epsilon}; \quad (2.10)$$

en définissant :

$$c_C(\epsilon) := c_A(\epsilon) + c_B(\epsilon).$$

Nous pouvons donc nous limiter à W_1 de W et supposer W compact sans perte de généralité.

Comme W est compact, on peut supposer que tout recouvrement analytique ouvert $\mathcal{R}$ de W conséquent du Corollaire 2.1.25 soit fini. Nous appelons donc $N_{\mathcal{R}}$ le nombre de fonctions analytiques sous la forme suivante :

$$\Phi_i : B_1^{d(W,\mathcal{R})(k_\infty)} \to W, \ \forall i = 1, ..., N_{\mathcal{R}};$$

telles que :

$$W \subseteq \bigcup_{i=1}^{N_{\mathcal{R}}} \Phi_i(B_1^{d(W,\mathcal{R})}(k_\infty)).$$

Pour tout $i = 1, ..., N_{\mathcal{R}}$ et pour tout $\delta > 0$ il existe $\epsilon(\delta) > 0$ et une constante $c(\Phi_i, \delta) > 0$ telle que $\Phi_i(B_1^{d(W,\mathcal{R})}(k_\infty))(k, a(T))$ est contenu dans l'union d'au plus $c(\Phi_i, \delta)|a(T)|_{1/T}^{\epsilon(\delta)}$ hypersurfaces de degré $\leq \delta$.

Maintenant, quelque soit le recouvrement analytique $\mathcal{R} := \{\Phi_1, ..., \Phi_{N_\mathcal{R}}\}$ de W nous définissons :

$$M_\mathcal{R}(\delta) := \max_{i=1,\ldots,N_\mathcal{R}} \{c(\Phi_i, \delta)\} \geq 0;$$

où $c(\Phi_i, \delta) > 0$ est la constante associée à chaque fonction analytique Φ_i de $\mathcal{R}$ et au choix de $\delta > 0$ qu'on fait initiallement, telle qu'elle est définie en (2.9). En appellant $\mathcal{H}(W)$ la famille de tous les recouvrements analytiques de W induits par le Corollaire 2.1.25 nous avons qu'il existe une constante $C(W, \delta) \geq 1$ ne dépendant que de W et de δ définie comme il suit :

$$C(W, \delta) := \inf_{\mathcal{R} \in \mathcal{H}(W)} \{M_\mathcal{R}\} + 1.$$

Une telle constante existe puisque tout sous-ensemble non vide de $\mathbb{R}$ qui admet un minorant (dans notre cas c'est 0) admet une borne inférieure (soit, le maximum des minorants). Elle est donc telle qu'il existe au moins un $\mathcal{R} = \{\Phi_1, ..., \Phi_{N_\mathcal{R}}\} \in \mathcal{H}(W)$ tel que la constante $c(\Phi_i, \delta)$ définie comme en (2.9) pour tout $i = 1, ..., N_\mathcal{R}$ soit telle que :

$$c(\Phi_i, \delta) \leq C(W, \delta);$$

pour tout $i = 1, ..., N_\mathcal{R}$. Nous choisissons donc un tel $\mathcal{R}$ en appellant $N := N_\mathcal{R}$ et $d(W) := d(W, \mathcal{R})$. Pour un tel $\mathcal{R}$ nous avons donc que $W(k, a(T)) \subseteq \bigcup_{i=1}^N \Phi_i(B_1^{d(W)}(k_\infty))(k, a(T))$ et par conséquent que $W(k, a(T))$ est contenu dans l'union d'au plus $K(W, \delta)|a(T)|_{1/T}^{\epsilon(\delta)}$ hypersurfaces de degré au plus δ, où $K(W, \delta) := NC(W, \delta)$.

Soit $\epsilon > 0$. Nous choisissons alors $\delta > 0$ assez grand afin que $\epsilon(\delta) \leq \epsilon/2$, suivant les notations de la Proposition 2.3.10. Nous avons que l'ensemble des hypersurfaces dans k_∞^{nm} à coefficients dans k_∞ et dont le degré est $\leq \delta$ est en correspondance biunivoque avec l'espace projectif $\mathbb{P}_{\nu(\delta)}(k_\infty)$, pour un certain nombre $\nu(\delta) \in \mathbb{N}$ ne dépendant que de δ. Nous définissons :

$$T := W \times \mathbb{P}_{\nu(\delta)}(k_\infty).$$

Comme k_∞ est un corps local les mêmes raisonnements qu'on fait en caractéristique 0 restent valables pour montrer que $\mathbb{P}_{\nu(\delta)}(k_\infty)$ et donc T est un compact. Si $t \in \mathbb{P}_{\nu(\delta)}(k_\infty)$ nous appelons H_t l'hypersurface qu'on lui associe. Soit :

$$S := \{(\overline{z}, t) \in T, \overline{z} \in H_t\}.$$

Pour tout $t \in \mathbb{P}_{\nu(\delta)}(k_\infty)$ nous appelons **fibre** de t dans un sous-ensemble T' de T l'ensemble suivant :

$$T'_t := \{\overline{z} \in W, (\overline{z}, t) \in T'\}.$$

Chaque fibre dans S est un ensemble entier puisqu'elle est l'intersection entre un ensemble entier et un ensemble algébrique. Nous nous proposons de montrer le Théorème 2.3.8 en le faisant descendre d'une autre assertion. Nous montrons en effet que pour tout $S' \subset S$ il existe une constante $C(S', \epsilon) > 0$, ne dépendant que de S' (et donc de W si $S' = S$) telle que $N(S'_t \setminus S'^{alg.}_t, a(T)) \leq c(S', \epsilon)|a(T)|_{1/T}^{\epsilon/2}$ pour tout $t \in S'$. Nous allons prouver cet énoncé par récurrence sur la dimension des fibres dans S en supposant pour simplifier que $S' = S$, la preuve étant la même dans tous les autres cas. Soit h la dimension de S_t pour un $t \in \mathbb{P}_{\nu(\delta)}(k_\infty)$ fixé. Si $h = 0$, S_t est un ensemble discret et compact, donc fini. Dans ce cas on a que $S_t^{alg.} = \emptyset$, ce qui prouve l'assertion avec $c(S_t, \epsilon) = |S_t|$, quelque soit la valeur de ϵ. Soit, donc, $h > 0$. Soit :

$$A := \{(\overline{z}, t) \in S, \dim_{\overline{z}}(W \cap H_t) \leq h - 1\};$$

$$B := \{(\overline{z}, t) \in S, \dim_{\overline{z}}(W \cap H_t) = h\}.$$

Il s'ensuit que :

$$S = A \cup B.$$

Pour tout $t \in \mathbb{P}_{\nu(\delta)}(k_\infty)$ nous avons que :

$$A_t^{alg.} \cup B_t^{alg.} \subset (A \cup B)_t^{alg.}.$$

Pour chaque $t \in \mathbb{P}_{\nu(\delta)}(k_\infty)$ nous avons que :

$$\dim(A_t) \leq h - 1.$$

L'hypothèse de récurrence implique que :

$$N(A_t \setminus A_t, a(T)) \leq c(A, \epsilon)|a(T)|_{1/T}^{\epsilon/2};$$

pour une constante $c(A, \epsilon) > 0$ opportune. L'intersection d'une hypersurface H_t de degré $\leq \delta$ telle qu'elle intersecte W en points où la dimension d'une telle intersection est localement $\leq h - 1$ contient donc au plus $c(A, \epsilon)|a(T)|_{1/T}^{\epsilon/2}$ points dans $W(k, a(T))$. D'un autre côté, nous avons que :

$$\dim(B_t) = h.$$

Si donc $\overline{z} \in W \cap H_t$, il existe un voisinage ouvert $U_{\overline{z}} \subset k_\infty^h$ de $\overline{z}$ tel que :

$$U_{\overline{z}} \subset W \cap H_t.$$

Donc en particulier $U_{\overline{z}} \subset H_t$. Comme H_t est un ensemble algébrique il s'ensuit que :

$$B_t{}^{alg.} = B_t.$$

Le Théorème est donc trivialement vrai pour B. Suite à (2.11) nous avons que pour tout $t \in \mathbb{P}_{\nu(\delta)}(k_\infty)$ nous avons l'estimation suivante :

$$N(W \cap H_t \setminus (W \cap H_t)^{alg.}, a(T)) \leq c(W, \epsilon)|a(T)|_{1/T}^{\epsilon/2};$$

pour une certaine constante $C(W, \epsilon) := C(S, \epsilon) > 0$. Nous remarquons maintenant que pour toute hypersurface H_t de degré $\leq \delta$ nous avons que :

$$(W \cap H_t)^{alg.} = W^{alg.} \cap H_t;$$

puisque H_t est un ensemble algébrique. Il s'ensuit que :

$$W \setminus W^{alg.} = \bigcup_{t \in \mathbb{P}_{\nu(\delta)}(k_\infty)} ((W \setminus W^{alg.}) \cap H_t) = \bigcup_{t \in \mathbb{P}_{\nu(\delta)}(k_\infty)} ((W \cap H_t) \setminus (W \cap H_t)^{alg.}).$$

La compacité de W et la Proposition 2.3.10 impliquent qu'il y a une constante $K(W,\epsilon)>0$ telle que $W(k,a(T))$ est contenu dans l'union d'au plus $K(W,\epsilon)|a(T)|_{1/T}^{\epsilon/2}$ hypersurfaces de degré $\leq\delta$. Soit $\mathcal{S}\subset\mathbb{P}_{\nu(\delta)}(k_\infty)$ un ensemble d'autant d'éléments qui représente une telle famille d'hypersurfaces. Il s'ensuit que :

$$N(W\setminus W^{alg.},a(T))\leq\sum_{t\in\mathcal{S}}N(S_t\setminus {S_t}^{alg.},a(T))\leq C(W,\epsilon)K(W,\epsilon)|a(T)|_{1/T}^{\epsilon}.$$

En appellant :

$$c(W,\epsilon):=C(W,\epsilon)K(W,\epsilon);$$

nous prouvons le Théorème 2.3.8.

□

2.4 Projets de poursuite du travail

La méthode de J. Pila et U. Zannier prévoit ici, comme l'on a anticipé dans l'Introduction, que l'on arrive à montrer deux autres résultats, afin qu'en les intégrant avec le Théorème 2.3.8 on arrive à prouver la Conjecture 6. Plus précisément,

1. Prouver que $Y'(k_\infty)^{alg.}=Y'(k_\infty)^{t.c.}$;
2. Prouver qu'il existe un réel $\rho>0$ ne dépendant que du choix de $\mathcal{A}$ tel que :

$$\forall a(T)\in A\setminus\{0\},\ \ \forall\overline{x}\in\mathcal{A}[a(T)]\setminus\{0\}, D:=[k(\overline{x}):k]\geq|a(T)|_{1/T}^{\rho}.$$

La méthode avec laquelle J. Pila et U. Zannier ont montré l'analogue du premier de ces deux points dans le cas d'une variété abélienne trouve ici un obstacle apparemment pas évident à surmonter et qui a en ce moment bloqué la démarche de la preuve : la nature non-archimediénne de la topologie $1/T-$adique, qui est une topologie totalement discontinue où les boules (à la fois ouvertes et fermées) ne s'intersectent qu'à condition d'être contenues les unes dans les autres. Toute technique de prolongement analytique dans le sens usuel (avec laquelle on peut prouver facilement que tout ensemble semi-algébrique dans un ensemble analytique est union d'ensembles algébriques) n'aboutira à aucun résultat. La structure particulière des méthodes rigides prévoit d'ailleurs que l'on travaille sur $\mathcal{C}$ et non pas sur k_∞, et n'est en tout cas appliquable que dans très peu de situations dont la nôtre ne fait malheureusement pas partie.

Le deuxième point prévoit que l'on arrive à montrer une minoration du degré des points non nuls de $a(T)-$torsion, quelque soit $a(T)\in A\setminus\{0\}$, de l'ordre $|a(T)|_{1/T}^{\rho}$, pour un nombre $\rho>0$ ne dépendant que du choix du $T-$module $\mathcal{A}$. Une telle minoration entrerait donc évidemment en contradition avec la majoration qui suit du premier point pour toute valeur de $|a(T)|_{1/T}$ (ou, de façon équivalente, de $\deg_T(a(T))$) assez grand. Une fois prouvés donc ces deux points, il s'ensuit facilement que si X ne contient aucune translatée d'un sous-T^j-module non-trivial de $\mathcal{A}$ par un point de torsion pour aucun $j\in\mathbb{N}\setminus\{0\}$, X ne contient qu'un nombre fini de points de torsion, ce qui prouverait la Conjecture 6. En effet, le premier point nous permetterait de confondre $Y'(k_\infty)^{t.c.}$ avec $Y'(k_\infty)^{alg.}$ nous donnant ainsi la même majoration du Théorème 2.3.8

pour l'ensemble des points de $a(T)-$torsion de $Y'(k_\infty) \setminus Y'(k_\infty)^{t.c.}$. Suite à l'identification $Y'(k_\infty)^{t.c.}$ et l'union des translatés des sous-T^j-modules de $\mathcal{A}$ (pour un $j \in \mathbb{N} \setminus \{0\}$ opportun que nous idéntifions avec T à une extension éventuelle du corps des coefficients de Φ près) par des points de torsion, les hypothèses de la Conjecture 6 qui impliquent que $Y'(k_\infty)^{t.c.} = \emptyset$ nous permettent de conclure que l'estimation du Théorème 2.3.8 est une majoration du nombre des points de $a(T)-$torsion de X où X ne contient pas de classes de torsion. D'un autre côté le deuxième point nous donnerait une minoration du nombre des points de $a(T)-$torsion de $Y'(k_\infty)$ qui serait nécessairement en contradition avec le caractère arbitraire de l'exposant ϵ apparaissant dans la majoration du même nombre qui suit du Théorème 2.3.8 grâce au premier point. Dans [PZ] le deuxième point point est une conséquence directe du résultat prouvé par D. Masser dans [Mas2], une minoration de type Lehmer de la hauteur quadratique de Néron-Tate sur une variété abélienne $\mathcal{A}$, de la forme :

$$\widehat{h}(\overline{x}) \geq CD^{-\lambda};$$

où $\lambda > 0$ ne dépend que de la dimension de la variété abélienne et $\overline{x} \in \mathcal{A}_{NT}$. En général nous ne disposons, suite aux résultats du type Northcott, que de minorations de l'ordre :

$$\widehat{h}(x) \geq Cq^{-D^\lambda};$$

pour un module de Drinfeld quelconque (voir Théorème 1.2.10) et donc, vraissemblablement, pour un $T-$module assez générique, comme celui que nous étudions. Le premier chapitre de cette thèse fournit une solution dans le cas de modules de Drinfeld diagonaux seulement et les résultats de S. Dion ([Dn], chapitre 3) permettraient sans doute de les établir également pour les T-modules CM vérifiant les hypothèses de la thèse de cette dernière, ce qui permettrait d'avoir entièrement un cas non traité par le théorème de T. Scanlon.

Il s'agit toutefois d'un problème très ouvert pour les $T-$modules génériques. A présent, la seule stratégie apparemment efficace pour l'attaquer semble être celle développée par J. P. Serre (voir [Se2], Théorème 2, page 34) dans le cadre de sa preuve d'une version légèrement plus faible de la Conjecture de Lang (voir [Wt] pour un énoncé de cette dernière) pour une variété abélienne définie sur un corps de nombres. Plus précisément, il montre l'analogue dans cette situation de l'hypothèse suivante.

Hypothèse 3. *Soit $\mathcal{A} = (\mathbb{G}_a^m, \Phi)$ un $T-$module de dimension m et rang d, défini sur le corps des coefficients K. Il existe $c \in \mathbb{N} \setminus \{0\}$ tel que pour toute couple (a, b) de polynômes de A premiers entre eux, il existe $\sigma \in G_K$ tel que $\forall \overline{x} \in \mathcal{A}[a]$, $\Phi(b^c)(\overline{x}) = \sigma(\overline{x})$.*

Une telle hypothèse, déja formulée par L. Denis dans [Den3] dans le cas d'un module de Drinfeld, n'a pas encore été montrée dans ce cas particulier, ni dans celui plus général d'un $T-$module. Dans le cas où elle est satisfaite, on obtient alors assez facilement la minoration cherchée du degré algébrique sur K d'un point pas nul de $a(T)-$torsion en rapport avec une puissance de $|a(T)|_{1/T}$, où $a \in$ Spec A. En effet, si on appelle $Orb(\overline{x})$ l'orbite de $\overline{x}$ sous l'action de G_K, on a que :

$$|Orb(\overline{x})| \geq |\{b(T)^c, b(T) \in (A/(a))^*\}|.$$

La raison de cela est la suivante. Si $b_1(T)$ et $b_2(T)$ sont premiers entre eux, le seul point à la fois de $b_1(T)-$torsion et de $b_2(T)-$torsion est $\overline{0}$. Par conséquent, si $\Phi(b_1(T)^c)(\overline{x}) = \Phi(b_2(T)^c)(\overline{x})$, il s'ensuit que $a(T)|(b_1(T)^c - b_2(T)^c)$, ce qui veut dire que $b_1(T)^c \equiv b_2(T)^c \bmod (a(T))$. On obtient alors :

$$|Orb(\overline{x})| \geq \frac{q^{\delta_a}-1}{|\{b(T) \in (A/(a))^*, b(T)^c = 1\}|} \geq \frac{q^{\delta_a}}{2c}.$$

Si $D := [K(\overline{x}) : K]$ on a que :

$$D \geq \frac{1}{2c}|a(T)|_{1/T}.$$

En conclusion, tout $T-$module qui respecte l'hypothèse 3 vérifie le point 2.

Il est intéressant de remarquer qu'une version assez plus simple de la Conjecture de Lang, la Conjecture de Mumford-Tate, bien que pas encore prouvée pour une variété abélienne telle qu'on les a toujours supposées, ni pour un $T-$module en général, a été prouvée par R. Pink dans le cas d'un module de Drinfeld pas CM, comme nous allons l'expliquer. Soit $l \in \text{Spec } A$. Etant donné Φ un module de Drinfeld avec corps des coefficients K, soit $\Phi[l]$ le $A-$module de ses points de $l-$torsion. Comme on suppose Φ de caractéristique 0, il est bien connu qu'on a l'isomorphisme de $A-$modules :

$$\Phi[l] \simeq (A/(l))^d;$$

où d est le rang de Φ. L'action du groupe de Galois absolu G_K sur cet ensemble admet alors une représentation de Galois :

$$\rho_{\Phi,l} : G_K \to Aut(\Phi[l]) \simeq GL_d(A/(l)).$$

Une telle représentation s'étend aux modules de Tate :

$$\overline{\rho}_{\Phi,l} : G_K \to Aut(T_l(\Phi)) \simeq GL_d(A_{(l)}).$$

Le Théorème de R. Pink qu'on vient d'indiquer est alors le suivant (voir [Pink] pour un énoncé plus détaillé).

Théorème 2.4.1. *Si Φ n'est pas CM, $\rho_{\Phi,l}$ a une image ouverte.*

Les propriétés topologiques classiques de la limite projective de groupes finis impliquent alors qu'il existera $n_0 \in \mathbb{N} \setminus \{0\}$ tel que pour tout $n \geq n_0$ on ait que ρ_{Φ,l^n} est surjective. Une minoration de la cardinalité de $GL_d(A/(l^n))$ nous permet alors de minorer la cardinalité du groupe de Galois $G(K(\Phi[l^n])/K)$ par une bonne puissance de $|l(T)^n|_{1/T}$, ce qui corrobore le fait que les points de torsion devraient être aussi de degré minoré par la quantité qu'on désire.

Bibliographie

[A] G. Anderson, *t-motives*, Duke Math. Journal, 53 (1986), 457-502

[AM] G. Anderson, D. W. Masser, *Lower bounds for heights on elliptic curves*, Math. Z., t. 174, 1980, p. 23-24

[Am-Dv] F. Amoroso, R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory 80 (2000), pages 260-272

[Ash] R. B. Ash, *A Course In Commutative Algebra*, librement accessible, http ://www.math.uiuc.edu/ r-ash/ComAlg.html

[AT] G. Anderson, D. Thakur, *Tensor powers of the Carlitz module and zeta values*, Annals of Mathematics (2), 132(1) : 159-191, 1990

[At-Mac] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969

[B] H. Bauchère, *Thèse de doctorat - en cours de rédaction*, Université de Caen - Basse Normandie

[B-M] M. F. Becker, S. MacLane, *The minimum number of generators for inseparable algebraic extensions*, Bull. Amer. Math. Soc., Volume 46, n.2 (1940), 182-186

[Ba] I. Barsotti, *Structure theorems for group-varieties*, Annali di Matematica Pura e Applicata, volume 38, n.1 (1955), 77-119

[BG] E. Bombieri, W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006

[BGR] S. Bosch, U. Güntzer, R. Remmert, *Non-Archimedean Analysis*, Springer-Verlag, (1984)

[BP] E. Bombieri, J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. 59 (1989), 337-357. MR 1016893

[Brown] M. L. Brown, *Singular moduli and supersingular moduli of Drinfeld Modules*, Inventiones Mathematicae, 110, 419-439 (1992)

[Cart] H. Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann Editeurs des Sciences et des Arts - Collection Enseignements des Sciences, sixième edition 1985, nouveau tirage 1995

[Col-Maz] R. F. Coleman, B. Mazur, *The Eigencurve*, In Galois representations in arithmetic algebraic geometry (Durban, 1996), volume 254 of London Math. Soc. Lecture Note Ser., pages 1-113. Cambridge Univ. Press, Cambridge, 1998, librement accessible, http ://math.berkeley.edu/ coleman/eigen/coleman-mazur.pdf

[CM] S. H. Chebolu, J. Minac, *Counting irreducible polynômials over finite fields using the Inclusion-Exclusion Principle*, 2010

[Dav] C. David, *Average distribution of supersingular Drinfeld modules*, Journal of Number Theory vol. 56, 366-380, 1996

[Dav-Pach] S. David, A. Pacheco, *Le problème de Lehmer abélien pour un module de Drinfeld*, Int. J. Number Theory 4, No.6, 1043-1067 (2008)

[Den1] L. Denis, *Hauteurs canoniques et modules de Drinfeld*, Math. Annalen 294, 213-223 (1992)

[Den2] L. Denis, *Problèmes diophantiens sur les t-modules*, Journal de Théorie des Nombres de Bordeaux, tome 7, n. 1, 97-110, 1995

[Den3] L. Denis, *Géométrie Diophantienne sur les Modules de Drinfeld*, Proceedings of the Workshop at the Ohio State University, June 17-26, 1991

[Dn] S. Dion, *Analyse diophantienne et modules de Drinfeld*, Thèse de Doctorat, USTL, 17 mai 2002

[Dob] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynômial*, Acta Arithmetica 34, n.4, 391-401 (1979)

[FJ] M. D. Fried, M. Jarden, *Field Arithmetic*, third edition, revised by M. Jarden, 2008, Springer-Verlag

[Ge] E. U. Gekeler, *Drinfeld-Moduln und modulare Formen uber rationalen Funktionkorpern*, Bonnern Mathematische Schriften 119, Bonn, 1979

[Gh] D. Ghioca, *The local Lehmer inequality for Drinfeld modules*, Journal of Number Theory 123 (2007) 426-455

[Goss] D. Goss, *Basic structures of function field arithmetic*, Springer, 1996

[Hart] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag New York Inc., 1977

[Hayes] D. Hayes, *Explicit class field theory for rational function fields*, Transaction of the American Mathematical Society, vol. 189, 1974

[HS] M. Hindry, J. Silverman, *On Lehmer's Conjecture for Elliptic Curves*, Séminaire de Théorie des Nombres, Paris (1988-1989), 103-116, Progress. in Math. 91, Birkhauser Boston, 1990

[I] J. Igusa, *An introduction to the theory of local Zeta functions*, American Mathematical Society, Providence, RI, and International Press, Cambridge, MA, 2000

[IR] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, second edition, Springer-Verlag, GTM, vol. 84 (second edition), 1990

[Jeong] S. Jeong, *Calculus in positive characteristic p*, Journal of Number Theory 131 (2011), 1089-1104

[Lau1] M. Laurent, *Minoration de la hauteur de Néron-Tate*, Seminar on number theory, Paris 1981-1982 (Prog. in Math. 38, 137-151) Birkhauser, 1983

[Lau2] M. Laurent, *Equations diophantiennes exponentielles*, Invent. Math. 78 (1984), 299-327

[Leh] D. H. Lehmer, *Factorisation of some cyclotomic functions*, Annals of Math., 34, (2) 1933, 461-479

[Mah] K. Mahler, *Analogue to Minkowski's geometry of numbers*, Annals of Math., vol. 42, n. 2, 1941, 488-522

[Mas1] D. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France, 117, 1989, 247-265

[Mas2] D. Masser, *Small values of the quadratic part of the Néron-Tate height on an abelian variety*, Compositio Mathematica 53 (1984) 153-170

[Mats] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 25 mai 1989

[Milne] J. S. Milne, *Fields and Galois Theory*, version 4.30, april 2012, librement accessible, www.jmilne.org/math/CourseNotes/FT.pdf

[P] J. Pila, *Integer points on the dilatation of a subanalytic surface*, Quart. J. Math. vol. 55 Part 2, Oxford University Press, 2004

[PW] J. Pila, J. Wilkie, *The rational points of a definable set*, Duke Mathematical Journal, vol. 133, n. 3, 2006

[PZ] J. Pila, U. Zannier, *Rational points in periodic analytic sets and the Manin-Mumford conjecture*, Comptes Rendus Mathematique, vol. 346, Issues 9-10, May 2008, pages 491-494

[Pink] R. Pink, *The Mumford-Tate Conjecture for Drinfeld modules*, Publ. Res. Inst. Math. Sci. Kyoto Univ. 33 (1997), 393-425

[Pn] B. Poonen, *Drinfeld modules with no supersingular primes*, Internat. Math. Res. Notices, 1998, vol. 3, 151-159

[R1] M. Raynaud, *Courbes sur une varieté abelienne et points de torsion*, Inventiones Mathematicae, 71 (1983), n. 1, 207-233

[R2] M. Raynaud, *Sous-varieté d'une variété abélienne et points de torsion*, Arithmetic and Geometry, vol. I, Birkhauser, 1983

[Rib] P. Ribenboim, *L'Arithmétique des Corps*, Hermann, Paris, 1972

[Sc] T. Scanlon, *Diophantine Geometry of a torsion of a Drinfeld Module*, Journal of Number Theory, vol. 97, n. 1, 10-25, 2002

[Se1] J. P. Serre, *Lectures on the Mordell-Weil Theorem*, Aspects of Mathematics, Viewer-Verlag, 1989

[Se2] J. P. Serre, *Oeuvres. Collected papers. IV.*, Springer-Verlag, Berlin, 2000. 1985-1998

[Se3] J. P. Serre, *Corps Locaux*, Troisième édition, Hermann, Paris 1968

[Sh] M. Shiota, *Geometry of Subanalitic and Semialgebraic Sets*, Birkhäuser, 1997

[Shaf] I. R. Shafarevich, *Basic Algebraic Geometry I*, Springer-Verlag, 1988

[T] A. Thiery, *Théorème de Lindemann-Weierstrass pour les modules de Drinfeld*, Comp. Math. 95 (1995), n.1, 1-42

[Teich] O. Teichmüller, *Differentialrechung bei Charaketrisik p*, J. Reine Angew. Math. 175 (1936) 89-99

[V] V. Villani, *Sulle varie nozioni di dimensione per un insieme analitico*, Annali della Scuola Normale Superiore di Pisa, Classe di Scienze, 3ème série, tome 17, n. 1-2 (1963), p. 141-173, librement accessible, http ://www.numdam.org

[V-F] J. Fresnel, M. van der Put, *Rigid analytic geometry and its applications*, Progress in Math., Birkhauser, 2004

[V-P] M. van der Put, P. Schneider, *Points and topology in rigid geometry*, Math. Ann. 302 (1995), no.1, 81-103

[Wt] J. P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, Journal für die Reine und Angewandte Mathematik 553 (2002) 1-16

[Yu] J. Yu, *Homomorphisms into Drinfeld modules*, The Annals of Mathematics, Second Series, vo. 145, no. 2 (mar. 1997), pp. 215-233

[Zariski-Samuel] O. Zariski, P. Samuel, *Commutative Algebra*, Vol. II, Nostrand, Princeton, 1960