

Numéro d'ordre : 3119

UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE
U.F.R. DE MATHÉMATIQUES

THÈSE

présentée pour obtenir

le grade de

DOCTEUR DE L'UNIVERSITÉ

discipline : Mathématiques

par

Sophie DION

Analyse diophantienne et modules de Drinfeld.

Soutenue le 17 mai 2002 devant la commission d'examen

Directeur :	Mr Laurent DENIS	Université de Lille I
Rapporteurs :	Mr Ernst-Ulrich GEKELER	Université de Saarbrücken, Allemagne
	Mr Patrice PHILIPPON	CNRS, Université de Paris VI
Membres :	Mr Sinnou DAVID	Université de Paris VI
	Mr Yves HELLEGOUARCH	Université de Caen
	Mr François RECHER	Université de Lille I
	Mr Jing YU	Academia Sinica, Taipei

à Tonton Claude

Remerciements

Ce travail a été long, parfois difficile, mais par dessus tout enrichissant. Je souhaite tout d'abord remercier Laurent DENIS qui l'a encadré avec la plus grande habileté. Les thèmes scientifiques vers lesquels il m'a dirigée, les sujets de recherche qu'il m'a proposés sont à l'origine de l'enthousiasme avec lequel j'ai pu aborder cette thèse. Passionné et passionnant, toujours disponible et disposé, il a su transmettre son goût pour le défi, sa curiosité mathématique et sa ténacité face à la difficulté. Sa rencontre a été pour moi une expérience scientifique et humaine sans égale.

François RECHER m'a également accompagnée durant ces quelques années. Son dévouement sans mesure, ses nombreux encouragements, mais aussi ses conseils mathématiques ont été autant de soutiens nécessaires à la réalisation de ce travail. Aujourd'hui, c'est un plaisir pour moi de le remercier chaleureusement.

Je tiens aussi à exprimer ma très grande reconnaissance à Ernst-Ulrich GEKELER et à Patrice PHILIPPON qui ont spontanément accepté d'être les rapporteurs de cette thèse. Le travail qu'ils ont fourni, le temps qu'ils y ont consacré sont considérables. Leurs très nombreuses remarques et suggestions ont apporté un autre regard à ce travail, et m'ont offert de nouvelles perspectives ; je les en remercie pleinement.

J'ai eu l'occasion de rencontrer Sinnou DAVID plusieurs fois. L'intérêt qu'il a porté à mes interrogations m'a beaucoup touchée et encouragée ; ses discussions mathématiques, toujours pleines d'attention, m'ont beaucoup apporté. C'est un plaisir et un honneur pour moi de pouvoir le compter parmi les membres de mon jury.

Yves HELLEGOUARCH et Jing YU ont accepté d'examiner cette thèse et de participer au jury de sa soutenance. Leurs remarques m'ont permis d'en améliorer considérablement la présentation. Je suis très honorée de l'intérêt qu'ils lui ont porté et les en remercie vivement.

Je remercie aussi l'ensemble du personnel du laboratoire de mathématiques de l'Université des Sciences et Technologies de Lille, et plus particulièrement les membres de l'équipe d'arithmétique et les doctorants.

Enfin, j'associe à ce travail tous ceux qui m'ont offert les possibilités de le réaliser, à savoir mes enseignants et plus particulièrement Thierry DUGARDIN et Gérard DEBEAUMARCHÉ, mais aussi mes parents, ma famille et mes amis.

Je n'oublie pas Augustin, sans lequel je n'aurais pas trouvé la foi nécessaire à l'achèvement de cette thèse.

Table des matières

Introduction	3
Partie I : Théorème de Brownawell-Waldschmidt en caractéristique finie	9
1 - Introduction	9
2 - Enoncés des lemmes	10
3 - Démonstration du théorème	15
4 - Conséquences	25
Partie II : Un théorème de transcendance en caractéristique positive	27
1 - Objectif et notations	27
2 - Fonctions modulaires	31
3 - Etude d'un nouveau polynôme modulaire	37
4 - Démonstration du théorème	45
5 - Conséquence	50
Partie III : Problème de Lehmer et T-modules de dimension 2	51
1 - Introduction	51
2 - Séparabilité	56
3 - Géométrie	65
4 - Lemme-clef de Dobrowolski	75
5 - Lemme de zéros	80
6 - Fonction auxiliaire	83
7 - Conclusion	91
8 - Cas particuliers	104
Annexe : un lemme de zéros	111
Références	115

Introduction

L'objet de ce travail consiste en l'examen de quelques problèmes diophantiens en caractéristique non nulle. Plus particulièrement, on s'est attaché à la résolution de problèmes de transcendance, d'indépendance algébrique et intéressé au problème de Lehmer. Le rôle des groupes algébriques classiques est ici tenu par les T -modules. La première démarche a été d'adapter les preuves de résultats connus dans $\mathbb{C}$ à ces objets. La démonstration du premier résultat, analogue du théorème de Brownawell-Waldschmidt, se déroule relativement bien, nonobstant quelques compléments sur les bases des réseaux. Mais on est très vite confronté à certains problèmes liés à la caractéristique positive. Par exemple, la preuve du résultat d'indépendance algébrique de valeurs de fonctions modulaires de Y. Nesterenko (voir [N1] ou [N2]), et plus particulièrement celle du lemme de zéros ne s'adaptent pas. En effet, les formes modulaires, considérées ici, vérifient elles aussi des équations différentielles, et l'on peut comme Y. Nesterenko construire un opérateur de dérivation sur une algèbre de polynômes. Cependant, à cause de la caractéristique positive, on ne peut rien dire sur les idéaux stables par cet opérateur. Néanmoins, la méthode des Stéphanos, jointe à des estimations de hauteurs de nouveaux polynômes modulaires semblables à celles de L.C. Hsia [Hs], conduit à un résultat de transcendance. Enfin, au cours de l'adaptation des preuves de F. Amoroso, S. David et M. Hindry (voir [AD] et [DH]), plusieurs difficultés, nées de la caractéristique positive, sont apparues ; elles ont rendu les résultats obtenus concernant le problème de Lehmer un peu moins généraux. Un premier obstacle tient à la structure même du T -module. En effet, dans le cadre des groupes multiplicatifs, ou des variétés abéliennes, les groupes sont stables sous l'action de $\mathbb{Z}$. Ici, l'action de $A = \mathbb{F}_q[T]$ est beaucoup plus forte, et les groupes (en particulier les stabilisateurs de variétés) ne sont pas stables par cette action. Cette difficulté a été surmontée en imposant aux T -modules certaines hypothèses galoisiennes. Enfin, la méthode utilisée dans [DH] utilise fondamentalement qu'une variété a autant de conjuguées que le degré sur $\mathbb{Q}$ de son corps de définition. Ce résultat ne tient plus en caractéristique positive à cause de phénomènes d'inséparabilité. Cependant, dans le cas de la dimension 2, on a su éviter les variétés « inséparables » et on a obtenu un résultat comparable à celui démontré par S. David et M. Hindry. Avant de présenter les résultats de ce travail, on fixe quelques notations.

Soit p un nombre premier et $q = p^r$ où r est un entier non nul. On désigne par $A = \mathbb{F}_q[T]$ l'anneau des polynômes à une indéterminée T à coefficients dans le corps fini $\mathbb{F}_q$, par $k = \mathbb{F}_q(T)$ son corps des fractions et par $k_\infty = \mathbb{F}_q((1/T))$ son complété pour la valuation $1/T$ -adique $v = -\deg$, avec la convention $\deg(0) = -\infty$. Cette valuation se prolonge de manière unique à k_∞ et à une clôture algébrique $\bar{k}_\infty$. On note $\mathcal{C}$ le complété de $\bar{k}_\infty$, auquel se prolonge encore la valuation précédente avec unicité ; ce corps est l'analogue du corps des complexes $\mathbb{C}$. On désigne enfin par $\bar{k}$ la clôture algébrique de k dans $\mathcal{C}$.

Pour tous entiers $n > 0$ et $d \geq 0$, par T -module de dimension n , de degré d et défini sur une extension finie E de k , on entend la donnée d'un couple $(\mathbb{G}_a^n, \Phi)$, où Φ est un

homomorphisme injectif d'anneaux

$$\Phi : \begin{cases} A & \longrightarrow & \text{End}_E(\mathbb{G}_a^n) \\ T & \longmapsto & \Phi_T = a_0\mathcal{F}^0 + \dots + a_d\mathcal{F}^d \end{cases}$$

où les a_i ($i = 0, \dots, d$) sont des matrices $n \times n$ à coefficients dans E avec $a_d \neq 0$, où T est la seule valeur propre de a_0 , et où $\mathcal{F}$ est l'endomorphisme de Frobenius relatif à q sur $\mathbb{G}_a^n$

$$\mathcal{F} : (x_1, \dots, x_n) \longmapsto (x_1^q, \dots, x_n^q).$$

Un sous- T -module $H \subset \mathbb{G}_a^n$ est un sous-groupe algébrique connexe, vérifiant $\Phi_T(H) \subset H$. Un T -module qui ne possède pas de sous- T -module non trivial sera dit simple.

Un morphisme $\Delta : (\mathbb{G}_a^n, \phi) \longrightarrow (\mathbb{G}_a^m, \psi)$ de T -modules, est un morphisme algébrique vérifiant

$$\Delta \circ \phi(T) = \psi(T) \circ \Delta.$$

Une isogénie est un morphisme surjectif de T -modules dont le noyau est fini.

Exemples :

- Les T -modules de dimension 1 sont aussi appelés modules de Drinfeld. Dans ce cas, on ne parlera plus de degré mais de rang du module. En particulier, le module de Carlitz donné par

$$C : T \longmapsto T\mathcal{F}^0 + \mathcal{F}^1,$$

est un module de Drinfeld de rang 1 défini sur k , et tous les modules de Drinfeld de rang 1 lui sont isomorphes sur $\mathcal{C}$.

- Etant donnés $\phi^{(1)}, \dots, \phi^{(n)}$ des modules de Drinfeld, on définit leur T -module produit par

$$\Phi : T \longmapsto \begin{pmatrix} \phi_T^{(1)} & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \phi_T^{(n)} \end{pmatrix}.$$

- Enfin, la puissance tensorielle de Carlitz $C^{\otimes n}$ est le T -module de dimension n suivant.

$$C^{\otimes n} : T \longmapsto \begin{pmatrix} T & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & T \end{pmatrix} \mathcal{F}^0 + \begin{pmatrix} 0 & \dots & \dots & 0 \\ \vdots & & & \vdots \\ 0 & & & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix} \mathcal{F}^1$$

Soit $\varphi : A \longrightarrow \text{End}_E(\mathbb{G}_a)$ un module de Drinfeld de rang $d \geq 1$ défini sur $\bar{k}$ et vérifiant

$$\varphi_T = T\mathcal{F}^0 + a_1\mathcal{F} + \dots + a_d\mathcal{F}^d.$$

Il existe alors une unique fonction exponentielle $e : \mathcal{C} \longrightarrow \mathcal{C}$ entière, $\mathbb{F}_q$ -linéaire et caractérisée par

$$e'(0) = 1 \quad \text{et} \quad \forall a \in A, \quad \forall z \in \mathcal{C}, \quad e(az) = \varphi_a(e(z)).$$

Le noyau de cette exponentielle noté Λ , est un A -module libre de rang d , appelé réseau des périodes associé à φ . On notera R_Λ l'anneau des multiplications de Λ défini par

$$R_\Lambda = \{\gamma \in \mathcal{C}, \gamma\Lambda \subset \Lambda\}.$$

C'est un A -module libre auquel on peut prolonger φ . Le corps des fractions de R_Λ sera noté k_Λ , c'est une extension finie de k , de degré au plus d . On dira que le module de Drinfeld φ est à multiplications complexes si k_Λ contient strictement k .

Dans une première partie, on s'intéresse à un résultat d'indépendance algébrique démontré simultanément par W.D. Brownawell [Br] et M. Waldschmidt [Wa] en 1971. Il s'agit du théorème suivant.

Théorème [Br] [Wa]. *Soient x_1 et x_2 (respectivement y_1 et y_2) des nombres complexes linéairement indépendants sur $\mathbb{Q}$ tels que $e^{x_1 y_2}$ et $e^{x_2 y_2}$ sont algébriques sur $\mathbb{Q}$. Alors deux au moins des nombres*

$$x_1, x_2, y_1, y_2, e^{x_1 y_1}, e^{x_2 y_1}$$

sont algébriquement indépendants.

On en montre ici un analogue pour les valeurs de la fonction exponentielle e associée à un module de Drinfeld φ de rang d , défini comme précédemment. Le résultat obtenu est le suivant.

Théorème A [D]. *Soient $\mu \geq 1$ et $\nu \geq 1$ deux entiers et $x_1, \dots, x_\mu \in \mathcal{C}$, k_Λ -linéairement indépendants, soient de même $y_1, \dots, y_\nu \in \mathcal{C}$, k -linéairement indépendants. On suppose que pour $i = 1, \dots, \mu$, $e(x_i y_\nu)$ est algébrique sur k . Si $\nu\mu \geq \nu + d\mu$ alors deux au moins des nombres $x_i, y_j, e(x_i y_j)$ (pour $i = 1, \dots, \mu$ et $j = 1, \dots, \nu$) sont algébriquement indépendants sur k .*

En caractéristique zéro, la proposition précédente répond à la conjecture de Schneider, à savoir que l'un des deux nombres e^e ou e^{e^2} est transcendant sur $\mathbb{Q}$. Ici, on a le corollaire suivant.

Corollaire. *On considère φ un module de Drinfeld de rang d défini sur $\bar{k}$. Soit $a \in R_\Lambda$ tel que $a \neq 0$, alors l'un au moins des nombres $e(e(a)), \dots, e((e(a))^{2d})$ est transcendant sur k .*

En particulier, avec l'exponentielle e_c associée au module de Carlitz, ce corollaire donne la proposition suivante.

Proposition. *L'un des deux nombres $e_c(e_c(1))$ et $e_c(e_c(1)^2)$ est transcendant sur k .*

Dans la seconde partie, on s'attache à démontrer un résultat de transcendance de valeurs de certaines fonctions modulaires. Soit $(\mathbb{G}_a, \Upsilon)$ un module de Drinfeld de rang 2 défini sur $\bar{k}$:

$$\Upsilon_T = T\mathcal{F}^0 + g\mathcal{F} + \Delta\mathcal{F}^2.$$

La quantité $j(\Upsilon) = \frac{g^{q+1}}{\Delta}$ ne dépend que de la classe d'isomorphisme de Υ . Elle est appelée invariant modulaire de Υ .

Pour $z \in \mathcal{C}$, on note $|z|_i = \inf_{x \in k_\infty} |z - x|$ sa partie imaginaire. Le demi-plan supérieur $\mathcal{C} \setminus k_\infty$ est noté Ω . Alors, un élément de $\mathcal{C}$ est dans Ω , si et seulement si sa partie imaginaire est non nulle. Ainsi, on a l'égalité

$$\Omega = \{z \in \mathcal{C}, |z|_i > 0\}.$$

Le groupe $GL_2(k_\infty)$ agit sur le demi-plan supérieur Ω par :

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k_\infty), \quad \forall z \in \Omega, \quad \gamma z = \frac{az + b}{cz + d}.$$

On associe à Υ son réseau des périodes $\Lambda = Aw_1 \oplus Aw_2$, que l'on normalise en $A \oplus Az$. Alors deux éléments z et z' définissent des modules de Drinfeld isomorphes si et seulement si ils sont conjugués par l'action de $\Gamma = GL_2(A)$. L'invariant modulaire j fournit ainsi une bijection entre $\mathcal{C}$ et le quotient $GL_2(A) \backslash \Omega$.

Soit l un entier et $f : \Omega \longrightarrow \mathcal{C}$ une fonction holomorphe vérifiant

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A), \quad f(\gamma z) = (cz + d)^l f(z).$$

En particulier, on a

$$\forall z \in \Omega, \quad \forall a \in A, \quad f(z + a) = f(z).$$

Ainsi, f peut être considérée comme une fonction définie sur $A \backslash \Omega$. D'après E.U. Gekeler (voir [Ge5]), cela implique qu'il existe une fonction f^* telle que

$$\forall z \in \Omega, \quad |z|_i > 1 \implies f^*(t(z)) = f(z),$$

où $t(z)$ est l'analogue du paramètre à l'infini $q = e^{2i\pi z}$. Si f^* admet un développement en série entière autour de 0, alors on dira que f est une forme modulaire de poids l .

On fait correspondre à tout $z \in \Omega$ le module de Drinfeld $\Upsilon^{(z)}$ associé au réseau $A \oplus Az$, et donc des nombres $g(z)$ et $\Delta(z)$. On définit de cette façon des formes modulaires de poids respectifs $q - 1$ et $q^2 - 1$, qui sont aussi des fonctions en la variable t . Dans la suite, on omettra les astérisques, ainsi g et Δ désigneront aussi bien des fonctions en z que des fonctions en t . On verra qu'il existe une constante $\tilde{\pi} \in \mathcal{C}$ telle que les fonctions $\bar{g} = \tilde{\pi}^{1-q}g$ et $\bar{\Delta} = \tilde{\pi}^{1-q^2}\Delta$ ont des développements en t à coefficients dans A . Ces deux fonctions sont les analogues des fonctions d'Eisenstein classiques E_4 et E_6 de poids 4 et 6.

Pour chaque q dans $\mathbb{C}$, tel que $0 < |q| < 1$, Y. Nesterenko ([N1] ou [N2]) a obtenu l'indépendance algébrique sur $\mathbb{Q}$, de trois au moins des nombres $q, E(q), E_4(q), E_6(q)$, où E désigne la fausse série d'Eisenstein de poids 2. Un corollaire remarquable est

l'indépendance algébrique des deux nombres π et e^π . Dans le cadre des modules de Drinfeld, en notant E l'analogue de la fausse série d'Eisenstein, on peut espérer le résultat similaire suivant.

Conjecture. *Soit $t \in \mathcal{C}$ tel que $0 < |t| < q^{-1/(q-1)}$, alors trois au moins des quatre nombres $t, E(t), \bar{g}(t)$ et $\bar{\Delta}(t)$ sont algébriquement indépendants sur k .*

L'obstruction majeure est l'adaptation du lemme de zéros de Y. Nesterenko. Une alternative serait de construire un opérateur sur $\mathcal{C}[X_1, X_2, X_3, X_4]$, en utilisant par exemple les dérivées divisées, ou encore l'action de A sur les formes modulaires. Mais on ne sait rien sur les idéaux stables par ces opérateurs. Une autre approche serait aussi de ne pas faire appel au lemme de zéros et, comme le fait P. Philippon (voir [P3]), d'utiliser une mesure d'indépendance algébrique. Cependant là encore, le polynôme construit à l'aide des équations différentielles vérifiées par les séries d'Eisenstein et utilisé pour obtenir cette mesure, peut être identiquement nul. On obtient néanmoins la réponse partielle suivante.

Théorème B. *Soit $t \in \mathcal{C}$ tel que $0 < |t| < q^{-1/(q-1)}$, alors l'un au moins des deux nombres $\bar{\Delta}(t)$ et $j(t)$ est transcendant sur k .*

En particulier, pour $t \in \mathcal{C}$ tel que $0 < |t| < q^{-1/(q-1)}$, ce théorème implique la transcendance de l'un au moins des deux nombres $\bar{g}(t)$ et $\bar{\Delta}(t)$.

Enfin, dans la dernière partie, on s'intéresse au problème de Lehmer pour certains T -modules de dimension 2. Dans le cas classique, l'objectif est de minorer la hauteur de Weil logarithmique et absolue d'un nombre algébrique α en fonction de son degré. Le résultat optimal espéré est la célèbre conjecture suivante.

Conjecture de Lehmer. *Il existe un nombre $c > 0$ tel que pour tout α dans $\mathbb{G}_m(\overline{\mathbb{Q}})$, qui n'est pas une racine de l'unité on ait*

$$h(\alpha) \geq \frac{c}{D},$$

où $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Des travaux ont déjà abouti dans ce sens ; la meilleure minoration connue à ce jour reste celle de E. Dobrowolski [Do] qui obtient le théorème suivant.

Théorème [Do]. *Il existe une constante $c > 0$ telle que pour tout α dans $\mathbb{G}_m(\overline{\mathbb{Q}})$, de degré D sur $\mathbb{Q}$ qui n'est pas une racine de l'unité on ait la minoration*

$$h(\alpha) \geq \frac{c}{D} \left(\frac{\log \log(3D)}{\log(3D)} \right)^3.$$

F. Amoroso, S. David et M. Hindry dans [AD] et [DH], ont étendu ce résultat à des points de $\mathbb{G}_m^N(\overline{\mathbb{Q}})$, et à des points algébriques de certaines variétés abéliennes définies sur un corps de nombres et admettant des multiplications complexes. Cependant, leurs preuves s'adaptent difficilement ici. Les T -modules pour lesquels on obtient un résultat analogue, doivent vérifier certaines hypothèses que l'on commence par énoncer.

Soit K une extension finie de k , et $(\mathbb{G}_a^n, \Phi)$ un T -module défini sur K . Si b est un élément non nul de A , un point $\mathbf{x}_0 \in \mathbb{G}_a^n$ est dit de b -torsion si $\Phi_b(\mathbf{x}_0) = 0$. On dira de plus, qu'il est de b -torsion primitive, si pour tout v dans A , on a l'équivalence suivante.

$$\Phi_v(\mathbf{x}_0) = 0 \quad \Longleftrightarrow \quad b|v.$$

Le T -module Φ devra d'une part vérifier les hypothèses galoisiennes naturelles suivantes.

- (Gal 1) *Il existe une constante $C(\Phi) > 0$ telle que pour tout $b \in A$ non nul, tout point de b -torsion primitive possède au moins $|b|^{C(\Phi)}$ conjugués sur K .*
- (Gal 2) *Soient b et v des éléments non nuls de A . Si v est premier à b , alors Φ_v permute les conjugués sur K de tout point de b -torsion primitive.*

D'autre part, l'action de A , beaucoup plus « forte » que celle de $\mathbb{Z}$, fait des T -modules des objets plus généraux que les variétés abéliennes. L'hypothèse suivante permet de surmonter cette difficulté.

- (H) *Soit H un sous-groupe algébrique connexe de $\mathbb{G}_a^n(\bar{k})$ tel qu'il existe un élément $a \in A$ avec $\deg a > 0$, vérifiant $\Phi_a(H) \subset H$. Alors H est un sous- T -module de $(\mathbb{G}_a^n, \Phi)$.*

Enfin, pour $\nu_0 \in A$ irréductible et unitaire, la propriété $(\mathcal{H}_{\nu_0})$ est la suivante.

$$(\mathcal{H}_{\nu_0}) \quad \Phi_{\nu_0}(X_1, \dots, X_n) \equiv (X_1^{q^{d \deg \nu_0}}, \dots, X_n^{q^{d \deg \nu_0}}) \pmod{\nu_0}$$

Elle est l'analogue du petit théorème de Fermat utilisé dans [AD] et [DH] pour démontrer le lemme de Dobrowolski. On va imposer à Φ de vérifier $(\mathcal{H}_{\nu_0})$ pour « beaucoup » de ν_0 , ce qui signifie encore que l'ensemble

$$H_m(\Phi) = \{\nu_0 \in A, \text{ irréductible, unitaire, } (\mathcal{H}_{\nu_0}) \text{ vérifiée, et } |\nu_0| \leq m\}$$

devra être suffisamment grand. Avec ces notations, on montre le théorème suivant.

Théorème C. *Soit $(\mathbb{G}_a^2, \Phi)$ un T -module de degré d , défini sur k et pour lequel la matrice dominante a_d est inversible. On suppose que pour ce T -module, les hypothèses (H), (Gal 1) et (Gal 2) sont vérifiées et que :*

$$\exists t \geq 1, \quad \exists C > 0, \quad \forall m \in \mathbb{N}, \quad \text{card}(H_m(\Phi)) \geq C \frac{m^{1/t}}{\log m}.$$

Alors il existe une constante $\kappa_0 > 0$, telle que pour tout $\alpha \in \mathbb{G}_a^2(\bar{k})$ séparable de degré D sur k qui n'est pas de torsion modulo les sous- T -modules de Φ , on ait la minoration

$$\hat{h}(\alpha) \geq \kappa_0 \frac{1}{D^{1/2}} \left(\frac{(\log \log(3D))^V}{(\log(3D))^U} \right),$$

où $U = dt^4(42d + 17) + 3$ et $V = dt(21d + 8) + 2$.

Ce théorème s'applique en particulier au produit $\varphi \times \varphi$ de modules de Carlitz, ou encore de certains modules de Drinfeld de rang 2, à multiplications complexes.

Partie I : Théorème de Brownawell-Waldschmidt en caractéristique finie

1 - Introduction

On rappelle tout d'abord les notations suivantes.

$$A := \mathbb{F}_q[T],$$

$$k := \mathbb{F}_q(T),$$

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

On désigne encore par $\mathcal{C}$ le complété pour la valuation $1/T$ -adique de la clôture algébrique $\bar{k}_\infty$ de k_∞ , et par $\bar{k}$ la clôture algébrique de k dans $\mathcal{C}$. On appelle T -module de dimension n , de degré d défini sur un sous-corps L de $\mathcal{C}$, tout couple $(\mathbb{G}_a^n, \Phi)$, où $\mathbb{G}_a^n$ désigne le groupe additif de dimension n et $\Phi: A \rightarrow L\{\mathcal{F}\}$ un homomorphisme injectif d'anneaux tel que l'on a

$$\Phi_T = a_0\mathcal{F}^0 + a_1\mathcal{F}^1 + \cdots + a_d\mathcal{F}^d$$

où $L\{\mathcal{F}\}$ est l'algèbre de Ore et les a_i sont dans $\mathcal{M}_n(L)$ avec $a_d \neq 0$, où T est la seule valeur propre de a_0 et où $\mathcal{F}$ est l'endomorphisme de Frobenius relatif à q sur $\mathbb{G}_a^n$. Un module de Drinfeld est un T -module de dimension 1 ; dans ce cas, au lieu de degré du module, on parlera de rang du module. On considère ici un module de Drinfeld φ de rang $d \geq 1$ défini sur la clôture algébrique $\bar{k}$ de k :

$$(1) \quad \varphi_T = T\mathcal{F}^0 + a_1\mathcal{F} + \cdots + a_d\mathcal{F}^d.$$

Il existe alors une unique fonction $e: \mathcal{C} \longrightarrow \mathcal{C}$ dite exponentielle attachée à φ , entière, $\mathbb{F}_q$ -linéaire et caractérisée par

$$(2) \quad e'(0) = 1 \quad \text{et} \quad \forall a \in A, \quad \forall z \in \mathcal{C}, \quad e(az) = \varphi_a(e(z)).$$

Le noyau de cette exponentielle est un A -module libre de rang d , c'est le réseau des périodes noté Λ . On notera R_Λ l'anneau des multiplications de Λ donné par :

$$(3) \quad R_\Lambda = \{\gamma \in \mathcal{C}, \gamma\Lambda \subset \Lambda\}.$$

C'est un A -module libre auquel on peut prolonger φ . Le corps des fractions de R_Λ sera noté k_Λ ; c'est une extension finie de k , de degré au plus d . Pour $\gamma \in R_\Lambda$, on écrit

$$(4) \quad \varphi_\gamma = \sum_{i=0}^{n_\gamma} a_i(\gamma)\mathcal{F}^i.$$

Des résultats concernant les petits degrés de transcendance des extensions de $\mathbb{Q}$ ont été réécrits en caractéristique finie. Certains cas de degré de transcendance au moins 2 (rappelés par R. Tubbs dans [Tu1] et [Tu2]) ont été démontrés dans ce cadre, notamment par L. Denis dans [De4], [De6] et [De7] et par A. Thiery dans [T1]. Notre but est d'obtenir l'analogie du théorème suivant prouvé indépendamment par W.D. Brownawell [Br] et M. Waldschmidt [Wa] en 1971.

Théorème 1 [Br] [Wa]. *Soient x_1 et x_2 (respectivement y_1 et y_2) des nombres complexes linéairement indépendants sur $\mathbb{Q}$ tels que $e^{x_1 y_2}$ et $e^{x_2 y_2}$ sont algébriques sur $\mathbb{Q}$, alors deux au moins des nombres*

$$x_1, x_2, y_1, y_2, e^{x_1 y_1}, e^{x_2 y_1}$$

sont algébriquement indépendants.

Ici, le rôle du groupe multiplicatif $\mathbb{G}_m(\overline{\mathbb{Q}})$ est tenu par un module de Drinfeld φ de rang d défini sur $\overline{k}$, et celui de l'exponentielle classique par l'exponentielle e associée à φ . En adoptant les notations précédentes, on obtient le résultat suivant.

Théorème A [D]. *Soient $\mu \geq 1$ et $\nu \geq 1$ deux entiers et $x_1, \dots, x_\mu \in \mathcal{C}$, k_Λ -linéairement indépendants, soient de même $y_1, \dots, y_\nu \in \mathcal{C}$, k -linéairement indépendants. On suppose que pour $i = 1, \dots, \mu$, $e(x_i y_\nu)$ est algébrique sur k . Si $\nu\mu \geq \nu + d\mu$ alors deux au moins des nombres $x_i, y_j, e(x_i y_j)$ (pour $i = 1, \dots, \mu$ et $j = 1, \dots, \nu$) sont algébriquement indépendants sur k .*

On commence, au paragraphe suivant, par citer quelques lemmes utilisés dans la démonstration du théorème A. Celle-ci est développée en troisième partie. On y construit une fonction auxiliaire s'annulant à un certain ordre en des points bien choisis, puis on applique un critère de transcendance à son premier coefficient de Taylor non nul. Dans une dernière partie, on donnera quelques conséquences du théorème A, notamment l'analogie de la conjecture de Schneider.

2 - Enoncés des lemmes

Soit $\alpha \in \mathcal{C}$ algébrique de degré δ_0 sur k , entier sur A , θ_1 un élément de $\mathcal{C}$ transcendant sur $k(\alpha)$ et $\theta_2 \in \mathcal{C}$ algébrique de degré δ sur $k[\alpha](\theta_1)$, entier sur $A[\alpha, \theta_1]$. Alors un élément x de $B = A[\alpha, \theta_1, \theta_2]$ s'écrit de manière unique sous la forme

$$(5) \quad x = \sum_{\substack{\mathbf{i} \in \mathbb{N}^4 \\ 0 \leq i_2 \leq \delta_0 - 1 \\ 0 \leq i_4 \leq \delta - 1}} a_i T^{i_1} \alpha^{i_2} \theta_1^{i_3} \theta_2^{i_4} = P(T, \alpha, \theta_1, \theta_2)$$

où $P \in \mathbb{F}_q[X_1, X_2, X_3, X_4]$. Pour une telle écriture de x , on note

$$(6) \quad \begin{aligned} \deg_T(x) &= \deg_{X_1}(P), \\ \deg_{\theta_1}(x) &= \deg_{X_3}(P). \end{aligned}$$

Propriétés : Ces degrés vérifient les quelques propriétés suivantes :

1) Soient x et y dans B , alors on a les majorations

$$\begin{aligned}\deg_T(x+y) &\leq \max\{\deg_T(x), \deg_T(y)\}, \\ \deg_{\theta_1}(x+y) &\leq \max\{\deg_{\theta_1}(x), \deg_{\theta_1}(y)\}.\end{aligned}$$

2) Pour tout $x \in A[\theta_1]$, et tout $y \in B$, on a les égalités

$$\begin{aligned}\deg_T(xy) &= \deg_T(x) + \deg_T(y), \\ \deg_{\theta_1}(xy) &= \deg_{\theta_1}(x) + \deg_{\theta_1}(y).\end{aligned}$$

3) Il existe $C_0 \in \mathbb{R}$ (respectivement $C'_0 \in \mathbb{R}$) ne dépendant que de α et θ_2 (respectivement α, θ_1 et θ_2) tel que pour tout $n \in \mathbb{N}$ et $x_1, x_2, \dots, x_n \in B$, on ait les majorations suivantes.

$$\begin{aligned}\deg_T(x_1 x_2 \cdots x_n) &\leq \deg_T(x_1) + \deg_T(x_2) + \cdots + \deg_T(x_n) + C_0(n-1), \\ \deg_{\theta_1}(x_1 x_2 \cdots x_n) &\leq \deg_{\theta_1}(x_1) + \deg_{\theta_1}(x_2) + \cdots + \deg_{\theta_1}(x_n) + C'_0(n-1).\end{aligned}$$

Preuve - 1) et 2) sont évidents. On montre l'assertion 3) tout d'abord pour le produit de deux éléments de B . Soient x et y deux éléments de B :

$$x = \sum_{\substack{\mathbf{i} \in \mathbb{N}^2 \\ 0 \leq i_1 \leq \delta_0 - 1 \\ 0 \leq i_2 \leq \delta - 1}} x_{\mathbf{i}} \alpha^{i_1} \theta_2^{i_2} \quad \text{et} \quad y = \sum_{\substack{\mathbf{j} \in \mathbb{N}^2 \\ 0 \leq j_1 \leq \delta_0 - 1 \\ 0 \leq j_2 \leq \delta - 1}} y_{\mathbf{j}} \alpha^{j_1} \theta_2^{j_2}$$

où les $x_{\mathbf{i}}$ et les $y_{\mathbf{j}}$ sont dans $A[\theta_1]$. Alors, leur produit s'écrit

$$xy = \sum_{\substack{\mathbf{i}, \mathbf{j} \in \mathbb{N}^2 \\ 0 \leq i_1, j_1 \leq \delta_0 - 1 \\ 0 \leq i_2, j_2 \leq \delta - 1}} x_{\mathbf{i}} y_{\mathbf{j}} \alpha^{i_1 + j_1} \theta_2^{i_2 + j_2}.$$

On pose $C_0 = \max_{\substack{0 \leq l \leq 2(\delta_0 - 1) \\ 0 \leq l' \leq 2(\delta - 1)}} \{\deg_T(\alpha^l \theta_2^{l'})\}$ et $C'_0 = \max_{\substack{0 \leq l \leq 2(\delta_0 - 1) \\ 0 \leq l' \leq 2(\delta - 1)}} \{\deg_{\theta_1}(\alpha^l \theta_2^{l'})\}$. Alors, on a les majorations suivantes.

$$\begin{aligned}\deg_T(xy) &\leq \deg_T(x) + \deg_T(y) + C_0 \\ \deg_{\theta_1}(xy) &\leq \deg_{\theta_1}(x) + \deg_{\theta_1}(y) + C'_0\end{aligned}$$

Par récurrence, on montre facilement le résultat annoncé pour le produit de n éléments de B . □

Avec ces notations, on montre le lemme de Siegel suivant.

Lemme 1. Soient n et m deux entiers tels que $n > \delta_0 \delta m$, soient aussi $M_1 > 0$ et $M_2 > 0$ des réels. On se donne des éléments $(a_{i,j})_{\{1 \leq i \leq n, 1 \leq j \leq m\}}$ de B tels que $\deg_T(a_{i,j}) < M_1$, $\deg_{\theta_1}(a_{i,j}) < M_2$. Alors il existe $x_i \in A[\theta_1]$ pour $i = 1, \dots, n$ non tous nuls vérifiant

$$\begin{aligned}\forall j \in \{1, \dots, m\} \quad \sum_{i=1}^n a_{i,j} x_i &= 0, \\ \deg_T(x_i) &\leq \frac{\sqrt{\delta_0 \delta m}}{\sqrt{n} - \sqrt{\delta_0 \delta m}} M_1 + 1 \quad \text{et} \quad \deg_{\theta_1}(x_i) \leq \frac{\sqrt{\delta_0 \delta m}}{\sqrt{n} - \sqrt{\delta_0 \delta m}} M_2 + 1.\end{aligned}$$

Preuve - Soient X et Y deux entiers strictement positifs. On considère l'ensemble suivant.

$$E = \{(x_1, \dots, x_n) \in (A[\theta_1])^n \mid \deg_T(x_i) \leq X, \deg_{\theta_1}(x_i) \leq Y\}$$

On a d'une part l'égalité $\text{card } E = q^{n(X+1)(Y+1)}$. D'autre part, si l'on note

$$F = \{(y_1, \dots, y_m) \in B^m \mid \deg_T(y_i) \leq X + M_1, \deg_{\theta_1}(y_i) \leq Y + M_2\},$$

alors on a l'égalité $\text{card } F = q^{m\delta_0\delta(X+[M_1]+1)(Y+[M_2]+1)}$. On définit l'application linéaire de E dans F suivante

$$(x_1, \dots, x_n) \longmapsto \left(\sum_{i=1}^n a_{i,1}x_i, \dots, \sum_{i=1}^n a_{i,m}x_i \right).$$

Pour qu'il existe deux éléments de E ayant la même image par cette application, il suffit d'avoir l'inégalité $\text{card } E > \text{card } F$, c'est-à-dire

$$n(X+1)(Y+1) > m\delta_0\delta(X+M_1+1)(Y+M_2+1).$$

Ceci est vérifié par exemple pour

$$X = \frac{\sqrt{\delta_0\delta m}}{\sqrt{n} - \sqrt{\delta_0\delta m}}M_1 + 1 \quad \text{et} \quad Y = \frac{\sqrt{\delta_0\delta m}}{\sqrt{n} - \sqrt{\delta_0\delta m}}M_2 + 1.$$

Ainsi, la différence de ces deux éléments donne la réponse à notre problème. $\square$

On rappelle le lemme élémentaire suivant. Sa preuve se fait simplement, par récurrence sur le degré de $b \in A$.

Lemme 2. *Soit φ un module de Drinfeld de rang d , alors pour tout b dans A , φ_b est un polynôme de degré $d \deg b$ en $\mathcal{F}$:*

$$\varphi_b = b\mathcal{F}^0 + a_1(b)\mathcal{F}^1 + \dots + a_{d \deg b}(b)\mathcal{F}^{d \deg b}.$$

Le résultat suivant est dû à L. Denis (cf lemme 1 de [De3]).

Lemme 3 [De3]. *Soient $G_1, \dots, G_m$ des T -modules simples deux-à-deux non isogènes. Alors, tout sous- T -module H de $G = G_1^{n_1} \times \dots \times G_m^{n_m}$ est un produit $H_1 \times \dots \times H_m$ où chaque H_i désigne un sous- T -module de $G_i^{n_i}$.*

On utilisera un lemme de zéros dû à J. Yu, dans lequel interviennent les notations suivantes. On se donne un module de Drinfeld φ et on considère un T -module Φ de dimension $\mu + 1$ vérifiant l'égalité

$$(7) \quad \Phi_T = \begin{pmatrix} T & 0 & \dots & 0 \\ 0 & \varphi_T & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \varphi_T \end{pmatrix}.$$

Grâce au lemme précédent, on montre que les sous- T -modules de Φ sont de la forme $G = G_1 \times G_2$ où G_1 et G_2 sont respectivement des sous- T -modules du T -module trivial de dimension 1 et de φ^μ . Soient $x_1, \dots, x_\mu \in \mathcal{C}$, on considère l'application suivante.

$$(8) \quad \varepsilon : \begin{cases} \mathcal{C} & \longrightarrow \mathcal{C}^{\mu+1}, \\ z & \longmapsto (z, e(x_1 z), \dots, e(x_\mu z)), \end{cases}$$

où e désigne l'exponentielle attachée au module de Drinfeld φ . C'est un homomorphisme à un paramètre associé à Φ , c'est-à-dire que l'on a

$$(9) \quad \forall a \in R_\Lambda, \quad \varepsilon(az) = \Phi_a(\varepsilon(z)).$$

Soit $P \in \mathcal{C}[X_0, \dots, X_\mu]$, on dira que P s'annule à un ordre $\geq m$ en un point $\gamma \in \mathcal{C}^{\mu+1}$ le long de ε , si $P(\gamma + \varepsilon(z))$ n'a que des termes d'ordre $\geq m$ dans son développement de Taylor autour de 0. Soient $\omega_1, \dots, \omega_r$ des éléments de $\mathcal{C}^{\mu+1}$, on définit

$$(10) \quad \Gamma(s_1, \dots, s_r) = \{\Phi_{a_1}(\omega_1) + \dots + \Phi_{a_r}(\omega_r), \ a_i \in A, \ \deg(a_i) \leq s_i\}.$$

En reprenant la démonstration du lemme de zéros de L. Denis [De6] (théorème 1), et en y changeant $\Gamma(s)$ en $\Gamma(s_1, \dots, s_r)$, on obtient le lemme suivant.

Lemme 4. *Il existe une constante $c(\Phi)$ telle que si on a un polynôme $P(X_0, \dots, X_\mu)$ non nul en $\mu + 1$ variables de degré D_1 en X_0 et de degré total D_2 en $(X_1, \dots, X_\mu)$ qui s'annule sur $\Gamma(s_1 + \mu + 1, \dots, s_r + \mu + 1)$ à l'ordre supérieur ou égal à $(\mu + 1)M + 1$ le long de l'homomorphisme à un paramètre ε , alors il existe $G = G_1 \times G_2$ sous- T -module propre de Φ vérifiant la majoration*

$$\binom{M + r(G)}{r(G)} \text{card}(\Gamma(s_1, \dots, s_r) + G/G) \leq c(\Phi) D_1^{\text{codim} G_1} D_2^{\text{codim} G_2},$$

où $r(G)$ est la codimension analytique de l'image réciproque de G par ε .

On donne maintenant un lemme technique sur les réseaux, dont la preuve n'est autre qu'une méthode du pivot de Gauss adaptée.

Lemme 5. *Soit Γ_1 un A -module libre de rang d , dont une base est $(y_1, \dots, y_d)$. Soit Γ'_1 un sous- A -module de rang d' de Γ_1 . Alors, quitte à réordonner les y_i , on peut choisir une base $(z_1, \dots, z_{d'})$ de Γ'_1 telle que l'on ait l'égalité*

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_{d'} \end{pmatrix} = \begin{pmatrix} \alpha(1,1) & \alpha(1,2) & \dots & \alpha(1,d') & \dots & \alpha(1,d) \\ 0 & \alpha(2,2) & \dots & \alpha(2,d') & \dots & \alpha(2,d) \\ \vdots & \ddots & \ddots & \vdots & & \vdots \\ 0 & \dots & 0 & \alpha(d',d') & \dots & \alpha(d',d) \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{d'} \\ \vdots \\ y_d \end{pmatrix},$$

les $\alpha(i,j)$ étant dans A et vérifiant les inégalités

$$\deg(\alpha(i,j)) < \deg(\alpha(j,j)) \text{ pour } i = 1, \dots, j-1.$$

On peut voir la preuve du lemme de Schwarz-Jensen suivant dans [Y1] (lemme 2.3).

Lemme 6 [Y1]. Soient $f : \mathcal{C} \rightarrow \mathcal{C}$ une fonction entière, σ_r le nombre de zéros de f comptés avec multiplicité dans $\{z \in \mathcal{C}, \deg(z) \leq r\}$ et soit :

$$M(f, r) = \sup\{\deg(f(z)), \deg(z) \leq r\}.$$

Si $R > r$, alors on a la majoration $M(f, r) \leq M(f, R) - \sigma_r(R - r)$.

Soit $k \hookrightarrow E$ une extension finie de degré $\mathcal{D}$. On rappelle la notion de hauteur projective d'un élément $\alpha = (\alpha_0, \dots, \alpha_m)$ de $\mathbb{P}^m(E)$:

$$h(\alpha) = \frac{1}{\mathcal{D}} \sum_{\omega \in M_E} d_\omega \max_{0 \leq i \leq m} (-\omega(\alpha_i)),$$

où M_E désigne l'ensemble de toutes les places de E et d_ω le degré résiduel sur $\mathbb{F}_q$ en la place ω normalisée par $\omega(E) = \mathbb{Z} \cup \{+\infty\}$. Si $f(X_1, \dots, X_l) \in \bar{k}[X_1, \dots, X_l]$, $f(X) = \sum a_\lambda X^\lambda$ alors on appelle hauteur de f

$$h(f) = h(1, a_\lambda).$$

La proposition 3 de [T1] est démontrée pour $\psi \in \bar{k}_\infty$. Cependant, on a encore le résultat pour ψ appartenant à $\mathcal{C}$.

Lemme 7. Soient $\psi \in \mathcal{C}$ et $(P_n)_{n \in \mathbb{N}}$ une suite de polynômes non nuls de $A[X]$. On note $\delta_n = \deg_X(P_n)$, h_n la hauteur de P_n et $s_n = v(P_n(\psi)) = -\deg(P_n(\psi))$. On suppose qu'il existe un entier n_0 vérifiant

$$\forall n \geq n_0, \quad s_n \geq \max(h_n \delta_n + h_n \delta_{n+1} + h_{n+1} \delta_n, h_n \delta_n + h_n \delta_{n-1} + h_{n-1} \delta_n).$$

On suppose aussi que $\lim_{n \rightarrow \infty} \left(\frac{s_n}{\delta_n} - h_n \right) = +\infty$. Alors, on a

$$\forall n \geq n_0, \quad P_n(\psi) = 0.$$

3 - Démonstration du théorème

On se place sous les hypothèses du théorème A. Dans toute la suite $\log$ désignera le logarithme en base q , t_0 sera un entier arbitrairement grand et les constantes $C_i > 0$ ne dépendront pas de t_0 . Soit k_1 une extension finie de k contenant $e(x_1 y_\nu), \dots, e(x_\mu y_\nu)$, ainsi que les coefficients $a_i(\gamma)$ de φ_γ pour $\gamma \in R_\Lambda$ (voir (4)). Soit k_s la sous-extension séparable maximale de k_1 (c'est-à-dire la plus grande extension séparable de k contenue dans k_1) et p^{s_1} le degré d'inséparabilité de k_1 sur k . On sait alors qu'il existe $\alpha \in k_s$ entier sur A tel que $k_s = k[\alpha]$. On note δ_0 son degré. On choisit Δ_0 un dénominateur commun aux $e(x_i y_\nu)$ pour $i = 1, \dots, \mu$ c'est-à-dire un élément Δ_0 non nul de A tel que l'on ait

$$(11) \quad \forall i = 1, \dots, \mu, \quad \Delta_0 (e(x_i y_\nu))^{p^{s_1}} \in A[\alpha].$$

On peut alors trouver $\Delta \in A$ tel que $\Delta^{p^{s_1}}$ soit un multiple de Δ_0 . Ainsi, on aura

$$(12) \quad \forall i = 1, \dots, \mu, \quad (\Delta e(x_i y_\nu))^{p^{s_1}} \in A[\alpha].$$

De plus, comme A. Thiery dans [T2], on peut trouver $\lambda \in A$ tel que, quitte à changer Λ en $\frac{\Lambda}{\lambda}$, on ait

$$\forall \gamma \in R_\Lambda, \quad \text{si} \quad \varphi(\gamma) = \sum_{i=0}^{n_\gamma} a_i(\gamma) \mathcal{F}^i \quad \text{alors} \quad (a_i(\gamma))^{p^{s_1}} \in A[\alpha].$$

Pour commencer la preuve, on suppose le théorème A faux. Soit $L = k_1(x_i, y_j, e(x_i y_j))$ pour $i = 1, \dots, \mu$ et $j = 1, \dots, \nu$. Le degré de transcendance de L sur k est donc au plus 1, et d'après l'analogie du théorème d'Hermite-Lindemann en caractéristique finie, c'est exactement 1 car l'un au moins des nombres $e(x_1 y_1), x_1$ et y_1 est transcendant sur k .

On peut donc écrire $L_s = k_s(\theta_1, \theta_2)$ où θ_1 est transcendant sur k_s , θ_2 est algébrique de degré δ , séparable sur $k_s(\theta_1)$, entier sur $A[\alpha, \theta_1]$, et L_s est la sous-extension séparable maximale de L (c'est-à-dire la plus grande extension séparable de $k_s(\theta_1)$ contenue dans L). On pose p^{s_2} le degré d'inséparabilité de L sur $k_s(\theta_1)$. Soit $s = \max\{s_1, s_2\}$, alors les éléments de L élevés à la puissance q^s sont dans L_s . A. Thiery dans [T2] conserve ces puissances tout au long de sa preuve. Cependant ici, pour alléger la démonstration, quitte à élever les fonctions à la puissance q^s , on supposera que tous les nombres sont dans L_s et que les $\Delta e(x_i y_\nu)$ et les $\varphi_i(\gamma)$ sont dans $A[\alpha]$.

Soit $x \in k_s(\theta_1, \theta_2)$, il s'écrit :

$$(13) \quad x = \sum_{i=0}^{\delta-1} \frac{P_i(T, \alpha, \theta_1)}{P_\delta(T, \alpha, \theta_1)} \theta_2^i.$$

On en déduit alors des expressions pour $x_1, \dots, x_\mu, y_1, \dots, y_\nu$, ainsi que pour les $e(x_i y_j)$ pour $i = 1, \dots, \mu$ et $j = 1, \dots, \nu - 1$. On prendra $P_\delta(T, \alpha, \theta_1) \in A[\alpha, \theta_1]$ un de leurs dénominateurs communs, ainsi par exemple, on aura

$$x_1 P_\delta(T, \alpha, \theta_1) \in A[\alpha, \theta_1, \theta_2].$$

On notera T'_1 et T'_2 les maxima respectifs des degrés en T et en θ_1 de tous ces nombres multipliés par $P_\delta(T, \alpha, \theta_1)$.

3.1. Construction d'une fonction auxiliaire

Soit t_0 un entier arbitrairement grand, on définit les paramètres suivants.

$$(14) \quad \begin{aligned} m_0 &= \left\lceil t_0^{\frac{\nu}{\mu}+d} (\log t_0)^{-\frac{1}{\nu}} \right\rceil, \\ t_1 &= t_0 (\log t_0)^{-\frac{1}{d\nu}}, \\ t_2 &= t_0 (\log t_0)^{\frac{\nu-1}{d\nu}}. \end{aligned}$$

Grâce au lemme 1, on construit une fonction F entière s'annulant au moins à l'ordre m_0 en $a_1 y_1 + \dots + a_\nu y_\nu$ où les a_i sont dans A et vérifient les égalités

$$(15) \quad |a_i| < t_1 \text{ si } i = 1, \dots, \nu - 1 \quad \text{et} \quad |a_\nu| < t_2.$$

On cherche plus particulièrement, parmi les fonctions F de la forme

$$(16) \quad F(z) = P_{t_0}(z, e(x_1 z), \dots, e(x_\mu z)),$$

$$(17) \quad F(z) = \sum_{\chi \in \mathbb{N}^{\mu+1}} p_\chi z^{\chi_0} e(x_1 z)^{\chi_1} \dots e(x_\mu z)^{\chi_\mu},$$

où $P_{t_0}(X_0, \dots, X_\mu) = \sum_{\chi \in \mathbb{N}^{\mu+1}} p_\chi X_0^{\chi_0} \dots X_\mu^{\chi_\mu}$ est un polynôme en $\mu + 1$ variables vérifiant

$$\begin{aligned} \deg_{X_0}(P_{t_0}) &\leq m_0, \\ \deg_{X_i}(P_{t_0}) &\leq (\mathcal{K} t_0)^{\frac{\nu}{\mu}} \text{ si } i = 1, \dots, \mu, \end{aligned}$$

où la constante $\mathcal{K}$ sera définie ultérieurement.

Soit $\mathcal{Y} = \sum_{i=1}^{\nu} a_i y_i$ où les a_i sont dans A . Alors, on a les égalités

$$\begin{aligned} F(\mathcal{Y} + z) &= \sum_{\chi} p_\chi \left(\sum_{i=1}^{\nu} a_i y_i + z \right)^{\chi_0} \left(e \left(\sum_{i=1}^{\nu} a_i x_1 y_i + x_1 z \right) \right)^{\chi_1} \dots \left(e \left(\sum_{i=1}^{\nu} a_i x_\mu y_i + x_\mu z \right) \right)^{\chi_\mu}, \\ &= \sum_{n \in \mathbb{N}} \left(\sum_{\chi} p_\chi \alpha_{n,\chi}(a_1, \dots, a_\nu) \right) z^n. \end{aligned}$$

On est donc amené à résoudre le système suivant

$$(18) \quad \sum_{\chi} p_\chi \alpha_{n,\chi}(a_1, \dots, a_\nu) = 0$$

pour $n \leq m_0 - 1$, $|a_i| < t_1$ si $i = 1, \dots, \nu - 1$ et $|a_\nu| < t_2$. Ainsi, on a les inégalités

$$\begin{aligned} \text{Nombre d'équations : } \mathcal{E} &< m_0 (q^\nu t_1^{\nu-1} t_2) = q^\nu m_0 t_0^\nu. \\ \text{Nombre d'inconnues : } \mathcal{I} &\geq m_0 ((\mathcal{K} t_0)^{\frac{\nu}{\mu}})^\mu. \end{aligned}$$

On choisit donc $\mathcal{K}$ de manière à avoir $\mathcal{I} > \delta_0 \delta \mathcal{E}$: par exemple $\mathcal{K} = q(\delta_0 \delta + 1)$.

Soit $D_0 = 1$. Pour $i \geq 1$, on notera $D_i = [i](D_{i-1})^q$ où $[i] = T^{q^i} - T$. Comme les coefficients du module de Drinfeld φ sont dans $A[\alpha]$, la suite D_h est une suite de dénominateurs pour la fonction e . On peut montrer que si $e = \sum_{m=0}^{+\infty} e_m \mathcal{F}^m$ alors on a

$$(19) \quad \begin{aligned} 1) & \quad D_h \in A \\ 2) & \quad (D_h e_m) \in A[\alpha] \text{ pour } m = 0, \dots, h \\ 3) & \quad q^{h_1} + \dots + q^{h_i} \leq q^N \Rightarrow D_{h_1} \dots D_{h_i} | D_N. \end{aligned}$$

La preuve de 2) se fait par récurrence comme dans [B1] lemme 8.2, en utilisant l'équation fonctionnelle de e .

Pour être dans les conditions du lemme de Siegel cité, il faut se ramener à un système à coefficients dans $B = A[\alpha, \theta_1, \theta_2]$. Par le lemme 2, on a que pour a_l dans A , $e(a_l x_i y_j)$ est un polynôme en $e(x_i y_j)$ de degré $q^{\deg a_l}$. De plus, les x_i apparaissent avec un degré total au plus m_0 (ordre d'annulation de F) et les y_j avec un degré total au plus m_0 (car $\deg_{X_0} P_{t_0} \leq m_0$). On doit donc multiplier les équations du système par $P_\delta(T, \alpha, \theta_1)$ à la puissance

$$(20) \quad \left[\mu(\mathcal{K}t_0)^{\frac{\nu}{\mu}} t_0^d (\log t_0)^{-\frac{1}{\nu}} \right] + 1 + m_0 + m_0 \leq C_1 m_0.$$

La présence des $e(x_i y_\nu)$ conduit aussi à multiplier les équations par Δ à la puissance

$$(21) \quad \left[\mu(\mathcal{K}t_0)^{\frac{\nu}{\mu}} t_0^d (\log t_0)^{\frac{\nu-1}{\nu}} \right] \leq C_2 \left[t_0^{\frac{\nu}{\mu} + d} (\log t_0)^{\frac{\nu-1}{\nu}} \right]$$

et celle des coefficients e_i , à multiplier les équations par $D_{[\log m_0]+1}$; on aura alors

$$(22) \quad \deg(D_{[\log m_0]+1} e_{[\log m_0]+1}) \leq C_3 m_0 \log m_0.$$

On multiplie toutes les équations par ces dénominateurs et, grâce au lemme 1, on trouve une solution non triviale du nouveau système vérifiant

$$(23) \quad \deg_T(p_\chi) \leq \frac{\sqrt{\delta_0 \delta \mathcal{E}}}{\sqrt{\mathcal{I}} - \sqrt{\delta_0 \delta \mathcal{E}}} M_1 + 1,$$

$$(24) \quad \deg_{\theta_1}(p_\chi) \leq \frac{\sqrt{\delta_0 \delta \mathcal{E}}}{\sqrt{\mathcal{I}} - \sqrt{\delta_0 \delta \mathcal{E}}} M_2 + 1,$$

où M_1 et M_2 sont respectivement des majorants des degrés en T et en θ_1 des coefficients du nouveau système, c'est-à-dire des $\alpha_{n,\chi}(a_1, \dots, a_\nu)$ multipliés par des dénominateurs.

On définit les nombres T_1 et T_2 par

$$(25) \quad \begin{aligned} T_1 &= \max_{1 \leq i \leq \mu} \{T'_1, \deg_T(\Delta e(x_i y_\nu)), \deg_T(\Delta), \deg_T(P_\delta(T, \alpha, \theta_1))\}, \\ T_2 &= \max\{T'_2, \deg_{\theta_1}(P_\delta(T, \alpha, \theta_1))\}. \end{aligned}$$

On a alors la majoration suivante.

$$\begin{aligned}
M_1 \leq & T_1 C_1 m_0 \\
& + T_1 C_2 [t_0^{\frac{\nu}{\mu} + d} (\log t_0)^{\frac{\nu-1}{\nu}}] \\
& + C_3 m_0 \log m_0 \\
& + m_0 T_1 \\
& + m_0 (2T_1 + \log(t_0 (\log t_0)^{\frac{\nu-1}{d\nu}})) \\
& + T_1 \mu (\mathcal{K} t_0)^{\frac{\nu}{\mu}} (t_0 (\log t_0)^{\frac{\nu-1}{d\nu}})^d \\
& + C_0 (m_0 + \mu (\mathcal{K} t_0)^{\frac{\nu}{\mu}} (t_0 (\log t_0)^{\frac{\nu-1}{d\nu}})^d - 1)
\end{aligned}$$

et donc il existe $C_4 > 0$ vérifiant

$$(26) \quad M_1 \leq C_4 m_0 \log m_0.$$

On procède de même pour M_2 .

$$\begin{aligned}
M_2 \leq & T_2 C_1 m_0 \\
& + m_0 T_2 \\
& + m_0 T_2 \\
& + T_2 \mu (\mathcal{K} t_0)^{\frac{\nu}{\mu}} (t_0 (\log t_0)^{-\frac{1}{d\nu}})^d \\
& + C'_0 (m_0 + \mu (\mathcal{K} t_0)^{\frac{\nu}{\mu}} (t_0 (\log t_0)^{-\frac{1}{d\nu}})^d - 1)
\end{aligned}$$

Comme précédemment, on obtient l'existence d'une constante $C_5 > 0$ pour laquelle on a la majoration

$$(27) \quad M_2 \leq C_5 m_0.$$

Conclusion 1. *Pour $t_0 \in \mathbb{N}$, on a construit une fonction*

$$F(z) = P_{t_0}(z, e(x_1 z), \dots, e(x_\mu z))$$

telle que $P_{t_0} \in A[\theta_1][X_0, X_1, \dots, X_\mu]$, avec $P_{t_0} \neq 0$ et

$$\deg_{X_0}(P_{t_0}) \leq m_0 \quad \text{et} \quad \text{si} \quad i \neq 0 \quad \deg_{X_i}(P_{t_0}) \leq (\mathcal{K} t_0)^{\frac{\nu}{\mu}},$$

les coefficients p_χ de P_{t_0} vérifiant

$$\deg_T(p_\chi) \leq C_6 m_0 \log m_0 \quad \text{et} \quad \deg_{\theta_1}(p_\chi) \leq C_7 m_0,$$

et F s'annulant au moins à l'ordre m_0 en les nombres $a_1 y_1 + \dots + a_\nu y_\nu$ où les a_i sont dans A et vérifient

$$|a_i| < t_1 \quad \text{si} \quad i = 1, \dots, \nu - 1 \quad \text{et} \quad |a_\nu| < t_2.$$

3.2. Utilisation du lemme de zéros

Dans ce paragraphe, grâce au lemme 4, on trouve une majoration de l'ordre d'annulation de F en les points $a_1 y_1 + \dots + a_\nu y_\nu$ introduits précédemment. Soit

$$(28) \quad \Gamma_1(r_1, r_2) = \left\{ \sum_{i=1}^{\nu} a_i y_i \mid a_i \in A, \deg(a_i) \leq r_1 \text{ si } i = 1, \dots, \nu - 1 \text{ et } \deg(a_\nu) \leq r_2 \right\},$$

où $r_1 = [\log t_1] - 1$ et $r_2 = [\log t_2] - 1$.

Soit Φ le T -module de dimension $\mu + 1$ introduit en (7) au paragraphe 2, vérifiant

$$\Phi_T = \begin{pmatrix} T & 0 & \dots & 0 \\ 0 & \varphi_T & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \varphi_T \end{pmatrix}.$$

On note alors

$$(29) \quad \Gamma(r_1, r_2) = \{\varepsilon(\mathcal{A}) \mid \mathcal{A} \in \Gamma_1(r_1, r_2)\}$$

où ε est l'homomorphisme à un paramètre défini au point (8).

Par construction de F , P_{t_0} s'annule au moins à l'ordre m_0 le long de ε sur $\Gamma(r_1, r_2)$. On applique alors le lemme 4. Si P s'annule à l'ordre au moins $(\mu + 1)M + 1$ le long de ε sur $\Gamma(r_1, r_2)$, alors il existe G sous T -module propre de $\mathbb{G}_a \times \varphi^\mu$ qui, d'après le lemme 3, s'écrit $G = G_1 \times G_2$, et tel que l'on ait les inégalités

$$\binom{M + r(G)}{r(G)} \text{card}(\Gamma(r_1 - \mu - 1, r_2 - \mu - 1) + G/G) \leq c(\Phi) m_0^{\text{codim} G_1} (\mu(\mathcal{K}t_0)^\frac{\nu}{\mu})^{\text{codim} G_2},$$

$$\binom{M + r(G)}{r(G)} \frac{\text{card}(\Gamma(r_1 - \mu - 1, r_2 - \mu - 1))}{\text{card}(\Gamma(r_1 - \mu - 1, r_2 - \mu - 1) \cap G)} \leq c(\Phi) m_0^{\text{codim} G_1} (\mu(\mathcal{K}t_0)^\frac{\nu}{\mu})^{\text{codim} G_2}.$$

$$\begin{aligned} \text{Or, on a } \text{card}(\Gamma(r_1 - \mu - 1, r_2 - \mu - 1)) &= \text{card}(\Gamma_1(r_1 - \mu - 1, r_2 - \mu - 1)) \\ &= q^{((r_1 - \mu)(\nu - 1) + (r_2 - \mu))} \\ &\geq C_8 t_1^{\nu - 1} t_2 = C_8 t_0^\nu. \end{aligned}$$

De plus, $r(G) = \dim \mathcal{C} - \dim \varepsilon^{-1}(G) = \dim \mathcal{C} - \dim(\varepsilon(\mathcal{C}) \cap G) = 0$ ou 1 donc on a

$$\binom{M + r(G)}{r(G)} \geq \frac{M^{r(G)}}{r(G)!} = M^{r(G)}.$$

Dans tous les cas, on a donc la majoration suivante

$$(30) \quad M^{r(G)} t_0^\nu \leq c'(\Phi) \text{card}(\Gamma(r_1 - \mu - 1, r_2 - \mu - 1) \cap G) m_0^{\text{codim} G_1} t_0^\frac{\nu}{\mu} \text{codim} G_2.$$

On regarde alors les différentes possibilités pour G .

Premier cas : $G = \{0\} \times G_2$.

Comme $G_1 = \{0\}$ on a $\text{codim} G_1 = 1$, de plus $\varepsilon(\mathcal{C}) \cap G = \{0\}$ ainsi $r(G) = 1$ et l'ensemble $\Gamma(r_1 - \mu - 1, r_2 - \mu - 1) \cap G = \{0\}$ est de cardinal 1.

D'autre part, on a toujours $\text{codim} G_2 \leq \mu$, donc $M t_0^\nu \leq c'(\Phi) \times 1 \times m_0 t_0^\nu$. Finalement, on obtient

$$\exists C_9 > 0, \quad M \leq C_9 m_0.$$

Deuxième cas : $G = \mathbb{G}_a \times G_2$

On a ici $\text{codim} G_1 = 0$ et $\text{codim} G_2 \leq \mu$. Comme $G_1 = \mathbb{G}_a$ nécessairement, $G_2 \neq \varphi^\mu$ et donc, comme l'écrit A. Thiery dans [T2], G_2 a au moins une équation du type

$$\varphi_{u_1} X_1 + \cdots + \varphi_{u_\mu} X_\mu = 0$$

avec $(u_1, \dots, u_\mu) \in R_\Lambda^\mu \setminus \{(0, \dots, 0)\}$.

Soit $\mathcal{A} = \sum_{j=1}^{\nu} a_j y_j \in \Gamma_1(r_1 - \mu - 1, r_2 - \mu - 1)$ tel que $\varepsilon(\mathcal{A}) \in G$. On a donc l'égalité

$$\varphi_{u_1}(e(x_1 \mathcal{A})) + \cdots + \varphi_{u_\mu}(e(x_\mu \mathcal{A})) = e((u_1 x_1 + \cdots + u_\mu x_\mu) \mathcal{A}) = 0.$$

Or, par hypothèse, les nombres $x_1, \dots, x_\mu$ sont linéairement indépendants sur k_Λ , donc le nombre $u_1 x_1 + \cdots + u_\mu x_\mu$ n'est pas nul. Ainsi, on a

$$\mathcal{A} = \sum_{j=1}^{\nu} a_j y_j \in (u_1 x_1 + \cdots + u_\mu x_\mu)^{-1} \Lambda.$$

Le réseau $\Lambda' = (u_1 x_1 + \cdots + u_\mu x_\mu)^{-1} \Lambda$ est aussi de rang d . De plus $y_1, \dots, y_\nu$ sont linéairement indépendants sur k et engendrent sur A un module Γ_1 de rang $\nu \geq \frac{\nu}{\mu} + d$. Le réseau $\Gamma'_1 = \Lambda' \cap \Gamma_1$ est de rang $d' \leq d$, sous- A -module de Γ_1 , donc, d'après le lemme 5, on peut en choisir une base $(z_1, \dots, z_{d'})$ telle que, quitte à réordonner les y_i on ait la relation

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_{d'} \end{pmatrix} = \begin{pmatrix} \alpha(1,1) & \alpha(1,2) & \dots & \alpha(1,d') & \dots & \alpha(1,\nu) \\ 0 & \alpha(2,2) & \dots & \alpha(2,d') & \dots & \alpha(2,\nu) \\ \vdots & \ddots & \ddots & \vdots & & \vdots \\ 0 & \dots & 0 & \alpha(d',d') & \dots & \alpha(d',\nu) \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{d'} \\ \vdots \\ y_\nu \end{pmatrix}$$

les $\alpha(i,j)$ étant dans A et vérifiant

$$(31) \quad \deg(\alpha(i,j)) < \deg(\alpha(j,j)) \text{ pour } i = 1, \dots, j-1.$$

Finalement, si $\mathcal{A} = b_1 z_1 + \cdots + b_{d'} z_{d'} \in \Gamma_1(r_1 - \mu - 1, r_2 - \mu - 1) \cap \Lambda'$, on montre par récurrence sur n que $\deg(b_n) \leq r_2$. Pour cela, on regarde les coordonnées de $\mathcal{A}$ dans la base $(y_1, \dots, y_\nu)$.

- La première coordonnée (celle en y_1) de $\mathcal{A}$ est $a_1 = \alpha(1,1)b_1$.

Or, $\deg(a_1) \leq r_2$, donc $\deg(\alpha(1,1)b_1) \leq r_2$ et comme $\alpha(1,1) \in A$, alors $\deg(b_1) \leq r_2$.

- La seconde coordonnée (celle en y_2) est $a_2 = \alpha(1,2)b_1 + \alpha(2,2)b_2$.

Comme précédemment, on obtient la majoration $\deg(\alpha(1,2)b_1 + \alpha(2,2)b_2) \leq r_2$.

Si $\deg(\alpha(1,2)b_1) \neq \deg(\alpha(2,2)b_2)$, alors

$$\deg(\alpha(1,2)b_1 + \alpha(2,2)b_2) = \max\{\deg(\alpha(1,2)b_1), \deg(\alpha(2,2)b_2)\}$$

et donc, on a bien $\deg(b_2) \leq r_2$.

Sinon, $\deg(\alpha(1,2)b_1) = \deg(\alpha(2,2)b_2)$ et comme $\deg(\alpha(1,2)) < \deg(\alpha(2,2))$ on a toujours $\deg(b_2) < \deg(b_1) \leq r_2$.

- Soit $n \in \{1, \dots, \nu\}$. On suppose que pour $i = 1, \dots, n-1$, $\deg(b_i) \leq r_2$.
En considérant la coordonnée en y_n de $\mathcal{A}$, on obtient la majoration

$$\deg(\alpha(1, n)b_1 + \dots + \alpha(n-1, n)b_{n-1} + \alpha(n, n)b_n) \leq r_2.$$

Si $\deg(\alpha(1, n)b_1 + \dots + \alpha(n-1, n)b_{n-1}) \neq \deg(\alpha(n, n)b_n)$ alors on a $\deg(\alpha(n, n)b_n) \leq r_2$ et donc $\deg(b_n) \leq r_2$.

Sinon,

$$\deg(\alpha(n, n)b_n) = \deg(\alpha(1, n)b_1 + \dots + \alpha(n-1, n)b_{n-1})$$

$$\deg(\alpha(n, n)b_n) \leq \max_{i=1, \dots, n-1} \{\deg(\alpha(i, n)b_i)\}$$

$$\deg(\alpha(n, n)b_n) \leq r_2 + \max_{i=1, \dots, n-1} \{\deg(\alpha(i, n))\}$$

d'où $\deg(b_n) \leq r_2$.

Ce résultat démontré, on peut maintenant majorer convenablement le cardinal de l'ensemble $\Gamma(r_1 - \mu - 1, r_2 - \mu - 1) \cap G$.

$$\begin{aligned} \Gamma(r_1 - \mu - 1, r_2 - \mu - 1) \cap G &\subseteq \varepsilon(\Gamma_1(r_1 - \mu - 1, r_2 - \mu - 1) \cap \Lambda') \\ &\subseteq \varepsilon(\Gamma_1(r_1, r_2) \cap \Lambda') \\ &\subseteq \varepsilon(\Gamma_1(r_1, r_2) \cap \Gamma'_1) \end{aligned}$$

Or, tout élément $\mathcal{A}$ de $\Gamma_1(r_1, r_2) \cap \Gamma'_1$ est de la forme $\mathcal{A} = \sum_{j=1}^{d'} b_j z_j$ avec $\deg(b_j) \leq r_2$.

On a donc

$$\begin{aligned} \text{card}(\Gamma(r_1 - \mu - 1, r_2 - \mu - 1) \cap G) &\leq \text{card}(\Gamma_1(r_1, r_2) \cap \Gamma'_1), \\ &\leq q^{d'(r_2+1)}, \\ &\leq q^{d'} t_2^{d'}. \end{aligned}$$

Enfin, puisque $\varepsilon^{-1}(G) \subset (u_1 x_1 + \dots + u_\mu x_\mu)^{-1} \Lambda$, $\varepsilon^{-1}(G)$ est de dimension 0, et donc $r(G) = 1$. On a alors les majorations

$$\exists C_{10} > 0, \quad M t_0^\nu \leq C_{10} t_0^\nu t_2^d,$$

$$(32) \quad \exists C_{10} > 0, \quad M \leq C_{10} t_0^d (\log t_0)^{\frac{\nu-1}{\nu}}.$$

Comme on est au moins dans un de ces cas, la condition la moins forte sera vérifiée, à savoir

$$(33) \quad \exists C_{11} > 0, \quad M \leq C_{11} m_0.$$

Conclusion 2. Si la fonction F s'annule à l'ordre $\geq (\mu + 1)M + 1$ sur $\Gamma_1(r_1, r_2)$, alors

$$M \leq C_{11} m_0.$$

3.3. Majoration du degré de $F(z)$

On utilise le lemme 6 pour majorer $\deg(F(z))$ avec $\deg(z) \leq r$ où r va être défini. On a clairement

$$\frac{\mu}{\nu + d\mu} < \frac{\mu(\nu + d)}{d(\nu + d\mu)}.$$

On choisit donc des réels positifs B et B_0 vérifiant les encadrements

$$(34) \quad \frac{\mu}{\nu + d\mu} < B_0 < B < \frac{\mu(\nu + d)}{d(\nu + d\mu)}.$$

Soit s_0 le plus grand entier tel que F s'annule à l'ordre $s_0 - 1$ sur $\Gamma_1(r_1, r_2)$. On a évidemment $s_0 \geq m_0$ et, par la deuxième étape $s_0 \leq (\mu + 1)C_{11}m_0 + 2$. On applique le lemme 6 avec $r = B_0 \log m_0$ et $R = B \log m_0$.

Si $\mathcal{A} \in \Gamma_1(r_1, r_2)$, alors $\deg(\mathcal{A}) \leq r_2 + \max_{i=1, \dots, \nu} \{\deg(y_i)\}$, c'est-à-dire

$$\begin{aligned} \deg(\mathcal{A}) &\leq \log(t_0(\log t_0)^{\frac{\nu-1}{d\nu}}) + \max_{i=1, \dots, \nu} \{\deg(y_i)\} \\ &\leq B_0 \log(m_0), \end{aligned}$$

pour t_0 assez grand (car $B_0 > \frac{\mu}{\nu + d\mu}$).

Alors, pour t_0 assez grand, F s'annule au moins $C_{12}s_0t_0^\nu$ fois dans $\{z \in \mathcal{C}, \deg(z) \leq r\}$, ainsi on a la minoration

$$(35) \quad \sigma_r \geq C_{12}s_0t_0^\nu.$$

De plus, e est une fonction entière d'ordre inférieur à d , donc il existe une constante $C > 0$ pour laquelle on a l'implication

$$(36) \quad \deg(z) \leq r \implies \deg(e(z)) \leq Cq^{dr}.$$

Si $\deg(z) \leq R$, alors $\deg(x_iz) \leq R + \deg(x_i)$ et donc $\deg(e(x_iz)) \leq C'q^{dR} = C''m_0^{dB}$. De plus, les coefficients p_χ de P_{t_0} vérifient les estimations données dans la conclusion 1

$$\deg_T(p_\chi) \leq C_6m_0 \log m_0 \quad \text{et} \quad \deg_{\theta_1}(p_\chi) \leq C_7m_0.$$

Et donc, on obtient

$$\deg(p_\chi) \leq C_6m_0 \log m_0 + \max_{l=0, \dots, [C_7m_0]} \{\deg(\theta_1^l)\}.$$

Alors, pour $z \in \mathcal{C}$ vérifiant $\deg z \leq r$, le lemme 6 donne la majoration

$$\deg(F(z)) \leq C'_{12}(m_0 \log m_0 + \mu m_0^{dB}(\mathcal{K}t_0)^{\frac{\nu}{\mu}} + Bm_0 \log m_0) - C_{12}(B - B_0)s_0t_0^\nu \log m_0.$$

Finalement, B et B_0 ont été choisis de sorte que l'on ait

$$(37) \quad \exists C_{13} > 0, \quad \forall z \in B(0, r) \quad \deg(F(z)) \leq -C_{13}s_0t_0^\nu \log m_0.$$

Conclusion 3. Si $r = B_0 \log m_0$, on a

$$\forall z \in \mathcal{C} \text{ tel que } \deg z \leq r, \quad \deg(F(z)) \leq -C_{13}s_0 t_0^\nu \log m_0.$$

3.4. Critère de transcendance

Par définition de l'entier s_0 introduit à l'étape précédente, on sait que F ne s'annule pas à l'ordre s_0 sur $\Gamma_1(r_1, r_2)$. Donc il existe $\mathcal{Y} = \sum_{i=1}^{\nu} a_i y_i \in \Gamma_1(r_1, r_2)$ tel que le coefficient de Taylor de $F(z + \mathcal{Y})$ à l'ordre s_0 soit non nul. On note ce coefficient

$$(38) \quad X_{t_0} = \sum_{\chi} p_{\chi} \alpha_{s_0, \chi}(a_1, \dots, a_{\nu}).$$

Sachant que $s_0 \leq (\mu + 1)C_{11}m_0 + 2$, on le multiplie correctement par des dénominateurs, afin d'obtenir un élément de $A[\alpha, \theta_1, \theta_2]$.

$$(39) \quad Y_{t_0} = P_{\delta}(T, \alpha, \theta_1)^{C'_1 m_0} \Delta^{C'_2 [t_0^{\frac{\nu}{\mu} + d} (\log t_0)^{\frac{\nu-1}{\nu}}]} D_{[\log((\mu+1)C_{11}m_0+2)]+1} X_{t_0} \in A[\alpha, \theta_1, \theta_2].$$

Ainsi, Y_{t_0} a une écriture de la forme

$$(40) \quad Y_{t_0} = \sum_{\substack{0 \leq i \leq \delta_0 - 1 \\ 0 \leq j \leq \delta - 1}} Q_{i,j}(T, \theta_1) \alpha^i \theta_2^j,$$

avec $\deg_T(Y_{t_0}) \leq C_{14}m_0 \log m_0$ et $\deg_{\theta_1}(Y_{t_0}) \leq C_{15}m_0$.

Il est clair que l'extension $k(\theta_1) \hookrightarrow k_s(\theta_1)[\theta_2]$ est finie et séparable. De plus, comme $k(\theta_1)$ et k_s sont linéairement disjoints sur k , elle est de degré $\delta_0 \delta$, et la famille

$$\{(\alpha^i \theta_2^j), 0 \leq i \leq \delta_0 - 1, 0 \leq j \leq \delta - 1\}$$

est une base de $k_s(\theta_1, \theta_2)$ en tant que $k(\theta_1)$ -espace vectoriel. Si on note $\mathcal{N} = \mathcal{N}_{k_s(\theta_1, \theta_2)/k(\theta_1)}$ l'application norme de $k_s(\theta_1, \theta_2)$ sur $k(\theta_1)$, alors $\mathcal{N}(Y_{t_0})$ est le déterminant de l'application linéaire

$$\begin{aligned} k_s(\theta_1, \theta_2) &\longrightarrow k_s(\theta_1, \theta_2), \\ z &\longmapsto zY_{t_0}. \end{aligned}$$

Si on écrit la matrice de cet endomorphisme dans la base précédente, comme α et θ_2 sont entiers, on obtient que $\mathcal{N}(Y_{t_0}) \in \mathbb{F}_q[T, \theta_1]$ ainsi que les majorations suivantes

$$(41) \quad \deg_T(\mathcal{N}(Y_{t_0})) \leq \delta_0 \delta (C_0 + \max_{\substack{0 \leq i \leq \delta_0 - 1 \\ 0 \leq j \leq \delta - 1}} \{\deg_T(Q_{i,j}(T, \theta_1))\}),$$

$$(42) \quad \deg_{\theta_1} \mathcal{N}(Y_{t_0}) \leq \delta_0 \delta (C'_0 + \max_{\substack{0 \leq i \leq \delta_0 - 1 \\ 0 \leq j \leq \delta - 1}} \{\deg_{\theta_1}(Q_{i,j}(T, \theta_1))\}),$$

où $C_0 = \max_{\substack{0 \leq l \leq 2(\delta_0 - 1) \\ 0 \leq l' \leq 2(\delta - 1)}} \{\deg_T(\alpha^l \theta_2^{l'})\}$ et $C'_0 = \max_{\substack{0 \leq l \leq 2(\delta_0 - 1) \\ 0 \leq l' \leq 2(\delta - 1)}} \{\deg_{\theta_1}(\alpha^l \theta_2^{l'})\}.$

Il existe donc $\mathcal{P}_{t_0} \in A[X]$ tel que $\mathcal{P}_{t_0}(\theta_1) = \mathcal{N}(Y_{t_0})$. Ce polynôme vérifie notamment

$$(43) \quad \begin{aligned} h_{t_0} &= h(\mathcal{P}_{t_0}) \leq C_{16}m_0 \log m_0, \\ \delta_{t_0} &= \deg(\mathcal{P}_{t_0}) \leq C_{17}m_0. \end{aligned}$$

On pose $s_{t_0} = -\deg(\mathcal{P}_{t_0}(\theta_1)) = -\deg(\mathcal{N}(Y_{t_0}))$.

Si on écrit $F(z + \mathcal{Y}) = \sum_{m=0}^{\infty} f_m z^m$, les inégalités de Cauchy dans le cas non archimédien (voir [BGR]), donnent

$$(44) \quad \forall \rho \in \mathbb{R}, \quad \sup\{\deg(F(z + \mathcal{Y})), \deg(z) \leq \rho\} = \sup\{\deg(f_m) + m\rho, m \geq 0\}.$$

Avec $\rho = r = B_0 \log m_0 > 0$, puisque $\deg \mathcal{Y} \leq r$ et d'après la majoration (37) on obtient

$$(45) \quad \begin{aligned} \deg(X_{t_0}) &= \deg(f_{s_0}) \leq \sup\{\deg(F(z + \mathcal{Y})), \deg(z) \leq r\}, \\ &\leq \sup\{\deg(F(z)), \deg(z) \leq r\}, \\ &\leq -C_{13}s_0 t_0^\nu \log m_0. \end{aligned}$$

En tenant compte des dénominateurs, on montre facilement que l'on a

$$\deg(\mathcal{N}(Y_{t_0})) \leq \deg(X_{t_0}) + C_{18}m_0 \log(m_0).$$

On obtient alors la majoration suivante

$$(46) \quad \exists C_{19} > 0, \quad s_{t_0} = -\deg(\mathcal{N}(Y_{t_0})) \geq C_{19}s_0 t_0^\nu \log m_0.$$

Finalement, on obtient la minoration

$$(47) \quad \frac{s_{t_0}}{\delta_{t_0}} - h_{t_0} \geq \frac{C_{18}s_0 t_0^\nu \log m_0}{C_{17}m_0} - C_{16}m_0 \log m_0.$$

En supposant que $\mu\nu \geq \nu + d\mu$, on se place dans les hypothèses du lemme 7 et donc pour t_0 assez grand $\mathcal{P}_{t_0}(\theta_1) = 0$ ce qui contredit la transcendance de θ_1 . $\square$

4 - Conséquences

On a tout d'abord un analogue du théorème de Brownawell-Waldschmidt. On considère l'exponentielle de Carlitz e_c associée au module de Carlitz $C_T = T\mathcal{F}^0 + \mathcal{F}$. On rappelle qu'elle est définie par

$$e_c = \sum_{h \geq 0} \frac{\mathcal{F}^h}{D_h}$$

où $D_0 = 1$ et $D_h = (T^{q^h} - T)(D_{h-1})^q$. Alors, ici $d = 1$ et le théorème A donne le corollaire suivant.

Corollaire 1. *Soient x_1, x_2 (resp. y_1, y_2) $\in \mathcal{C}$, A -linéairement indépendants. On suppose que $e_c(x_1 y_2)$ et $e_c(x_2 y_2)$ sont algébriques sur k , alors deux au moins des nombres $x_i, y_j, e_c(x_i y_j)$ (pour $i, j = 1$ ou 2) sont algébriquement indépendants sur k .*

Ce résultat, en caractéristique 0, contient la conjecture de Schneider, à savoir que :

$$e^e \text{ ou } e^{e^2} \text{ est transcendant sur } \mathbb{Q}.$$

En caractéristique finie, on en a aussi un analogue.

Corollaire 2. *On considère φ un module de Drinfeld de rang d défini sur $\bar{k}$. Soit $a \in R_\Lambda$ non nul, alors l'un au moins des nombres $e(e(a)), \dots, e((e(a))^{2d})$ est transcendant sur k .*

Preuve - On pose $x_1 = 1, x_2 = e(a), y_1 = a, y_2 = e(a), \dots, y_{2d} = (e(a))^{2d-1}$. D'après le théorème d'Hermite-Lindemann, comme $a \in R_\Lambda \subset \bar{k}$ alors $e(a) \notin \bar{k}$, et donc x_1 et x_2 sont linéairement indépendants sur k_Λ et les y_i le sont sur k . Si les nombres $e(e(a)^{2d-1})$ et $e((e(a))^{2d})$ étaient algébriques alors, avec $\mu = 2, \nu = 2d$, on se trouverait dans les conditions du théorème A et donc deux au moins des nombres suivants seraient algébriquement indépendants :

$$1, \quad a, \quad e(a), \quad e(ae(a)) = \varphi_a(e(e(a))), \quad e(e(a)^n), \quad \text{pour } n = 1, \dots, 2d. \quad \square$$

On retrouve en particulier, avec l'exponentielle de Carlitz, la proposition suivante.

Proposition. *L'un des deux nombres $e_c(e_c(1))$ et $e_c(e_c(1)^2)$ est transcendant sur k .*

Partie II : Un théorème de transcendance en caractéristique positive

1 - Objectifs et notations

1.1. Présentation du problème

Dans les cas complexes et p -adiques, les Stéphanos [BS et al.] ont obtenu un résultat de transcendance concernant l'invariant modulaire J attaché aux courbes elliptiques, et ont ainsi répondu à la conjecture de Mahler-Manin.

Proposition 1 [BS et al.]. *Si $q \in \mathbb{C}$ (resp. $q \in \mathbb{C}_p$) est algébrique sur $\mathbb{Q}$, et vérifie $0 < |q| < 1$ (resp. $0 < |q|_p < 1$), alors $J(q)$ est transcendant.*

On rappelle les notations données dans l'introduction. On désigne par $A = \mathbb{F}_q[T]$ l'anneau des polynômes à une indéterminée T à coefficients dans le corps fini $\mathbb{F}_q$, par $k = \mathbb{F}_q(T)$ son corps des fractions et par $k_\infty = \mathbb{F}_q((1/T))$ son complété pour la valuation $1/T$ -adique $v = -\deg$. Cette valuation se prolonge de manière unique à k_∞ et à une clôture algébrique $\bar{k}_\infty$. On note enfin $\mathcal{C}$ le complété de $\bar{k}_\infty$, sur lequel se prolonge encore la valuation précédente, et $\bar{k}$ la clôture algébrique de k dans $\mathcal{C}$.

Dans ce contexte, les courbes elliptiques ont un analogue : les modules de Drinfeld de rang 2, auxquels on associe également un invariant modulaire j . C'est dans ce cadre que M. Ably, L. Denis et F. Recher ont montré l'analogue suivant de la proposition précédente (voir [ADR]).

Proposition 2 [ADR]. *Soit $t \in \mathcal{C}$ tel que $0 < |t| < q^{-1/(q-1)}$, alors l'un au moins des deux nombres t et $j(t)$ est transcendant sur k .*

Pour chaque q dans $\mathbb{C}$, tel que $0 < |q| < 1$, Y. Nesterenko ([N1] ou [N2]) a obtenu l'indépendance algébrique sur $\mathbb{Q}$, de trois au moins des nombres $q, E(q), E_4(q), E_6(q)$, où E_4 et E_6 sont les séries d'Eisenstein de poids 4 et 6, et où E est la fausse série d'Eisenstein de poids 2. Un corollaire remarquable est l'indépendance algébrique des deux nombres π et e^π . Dans le cadre de la caractéristique finie, on peut espérer le résultat similaire suivant.

Conjecture 1. *Soit $t \in \mathcal{C}$ tel que $0 < |t| < q^{-1/(q-1)}$, alors trois au moins des quatre nombres $t, E(t), \bar{g}(t)$ et $\bar{\Delta}(t)$ sont algébriquement indépendants sur k ,*

où E est l'analogue de la fausse série d'Eisenstein, et $\bar{g}$ et $\bar{\Delta}$ sont des formes modulaires définies par E.U. Gekeler dans [Ge5], dont on redonnera les définitions dans la suite. Ici, on obtient la réponse partielle suivante.

Théorème B. *Soit $t \in \mathcal{C}$ tel que $0 < |t| < q^{-1/(q-1)}$, alors l'un au moins des deux nombres $\bar{\Delta}(t)$ et $j(t)$ est transcendant sur k .*

Le lemme de zéros de Y. Nesterenko ne s'adapte pas ici. Les formes modulaires classiques vérifient certaines équations différentielles. Y. Nesterenko les utilise pour créer un opérateur de dérivation par lequel il cherche les idéaux stables de $\mathbb{C}[X_1, X_2, X_3, X_4]$. Ici, il existe aussi des équations différentielles vérifiées par les formes modulaires (voir [Ge5]), qui fournissent un opérateur sur $\mathcal{C}[X_1, X_2, X_3, X_4]$. Cependant, il semble inespéré d'obtenir des informations suffisamment restrictives sur les idéaux stables par cet opérateur, ceci à cause de la caractéristique p . Une alternative serait de construire un opérateur sur $\mathcal{C}[X_1, X_2, X_3, X_4]$, en utilisant par exemple les dérivées divisées, ou encore l'action de l'application $z \mapsto az$ sur les formes modulaires. La difficulté est alors non seulement de trouver un opérateur D cohérent - c'est-à-dire tel que pour tout polynôme P de $\mathcal{C}[X_1, X_2, X_3, X_4]$, $D\left(P(t, E(t), \bar{g}(t), \bar{\Delta}(t))\right)$ soit encore un polynôme $\mathcal{D}P$ calculé en les fonctions $t, E(t), \bar{g}(t), \bar{\Delta}(t)$ - mais aussi d'obtenir suffisamment d'informations concernant les idéaux stables par cet opérateur. Une autre approche serait de ne pas faire appel au lemme de zéros et, comme le fait P. Philippon (voir [P3]), d'utiliser une mesure d'indépendance algébrique. Cependant la méthode employée pour obtenir cette mesure ne s'adapte pas ici ; en effet, le polynôme construit à l'aide des équations différentielles vérifiées par les séries d'Eisenstein, peut dans ce cas s'annuler identiquement.

On commence par rappeler quelques définitions, et par faire le lien entre ce résultat et les travaux d'Alain Thiery [T1]. Soit L un sous-corps de $\mathcal{C}$. Par module de Drinfeld de rang d défini sur L , on entend la donnée d'un homomorphisme injectif d'anneaux $\Upsilon: A \rightarrow L\{\mathcal{F}\}$ tel que

$$(1) \quad \Upsilon_T = T\mathcal{F}^0 + a_1\mathcal{F}^1 + \cdots + a_d\mathcal{F}^d$$

où $\mathcal{F}$ désigne l'endomorphisme Frobenius relatif à q sur le groupe additif $\mathbb{G}_a$, $L\{\mathcal{F}\}$ l'algèbre de Ore sur L , et où les a_i sont dans L avec $a_d \neq 0$. Pour un tel objet, on sait qu'il existe une unique fonction $e_\Upsilon: \mathcal{C} \rightarrow \mathcal{C}$ dite exponentielle attachée à Υ , entière et vérifiant

$$(2) \quad \begin{cases} e_\Upsilon(0) = 0, & e'_\Upsilon(0) = 1, \\ \forall a \in A, \forall z \in \mathcal{C}, & e_\Upsilon(az) = \Upsilon_a(e_\Upsilon(z)). \end{cases}$$

Le noyau de cette exponentielle est un A -module libre de rang d , c'est le réseau des périodes noté Λ . Réciproquement, pour un A -module libre Λ de rang d donné, il existe un unique module de Drinfeld de rang d , dont le réseau des périodes est exactement Λ . On a de plus le développement suivant donné par la dérivée logarithmique de e_Υ .

$$(3) \quad e_\Upsilon(z)^{-1} = \sum_{\lambda \in \Lambda} \frac{1}{z + \lambda}.$$

On appelle isogénie entre deux modules de Drinfeld Υ et Υ' , tout homomorphisme algébrique f non nul de $\mathbb{G}_a$ vérifiant les relations

$$\forall a \in A, \quad \Upsilon_a \circ f = f \circ \Upsilon'_a.$$

Si f est inversible, c'est-à-dire si c'est une homothétie, on dira que Υ et Υ' sont isomorphes. Par exemple, les modules de Drinfeld de rang 1 sont tous isomorphes au module de Carlitz défini par l'égalité

$$(4) \quad C_T = T\mathcal{F}^0 + \mathcal{F}.$$

Sa fonction exponentielle associée est donnée par

$$e_c(z) = \sum_{h \geq 0} \frac{z^{q^h}}{D_h}$$

où les D_h sont définis ainsi

$$(5) \quad D_0 = 1, \quad D_i = [i][i-1]^q \dots [1]^{q^{i-1}} \quad \text{où} \quad [i] = T^{q^i} - T \quad \text{pour } i \in \mathbb{N} \setminus \{0\}.$$

On rappelle encore qu'il existe un élément $\pi \in k_\infty$ transcendant sur k , pour lequel on a l'égalité $\ker(e_c) = \tilde{\pi}A$ où l'on a noté $\tilde{\pi} = (T - T^q)^{1/(q-1)}\pi$. On note pour tout élément z de $\mathcal{C} \setminus k_\infty$,

$$(6) \quad t = t(z) = \frac{1}{e_c(\tilde{\pi}z)}.$$

On peut maintenant énoncer brièvement les résultats d'A. Thiery.

1.2. Indépendance algébrique des périodes et quasi-périodes

Pour faciliter la lecture de ce paragraphe, on rappelle le célèbre théorème de G.V. Chudnovsky (voir [Ch]).

Proposition 3 [Ch]. *Soit $\wp$ la fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques et ζ la fonction de Weierstrass associée à $\wp$. On se donne une période λ de $\wp$ et w un point de $\wp$ qui ne soit pas un pôle, tels que λ et w soient linéairement indépendants sur $\mathbb{Q}$. Alors, les deux nombres*

$$\frac{2\zeta(\lambda/2)}{\lambda} \quad \text{et} \quad \zeta(w) - \frac{2\zeta(\lambda/2)}{\lambda}w$$

sont algébriquement indépendants sur $\mathbb{Q}$.

Une conséquence est que le nombre w/π est transcendant sur $\mathbb{Q}$. On verra, dans une dernière partie, l'analogie de ce résultat pour les modules de Drinfeld.

On considère ici un module de Drinfeld Υ de rang 2, défini sur une extension finie L de k . On note Λ_Υ son réseau des périodes. Une bidérivation associée à Υ , est une application $\eta : A \longrightarrow L\{\mathcal{F}\} \circ \mathcal{F}$ qui est $\mathbb{F}_q$ -linéaire, et qui vérifie les égalités

$$\forall a, b \in A, \quad \eta_{ab} = a\eta_b + \eta_a \circ \Upsilon_b.$$

D'après [Ge6], il existe une unique fonction entière $F_\eta \in L\{\{\mathcal{F}\}\} \circ \mathcal{F}$ telle que l'on ait

$$\forall a \in A, \forall z \in \mathcal{C}, \quad F_\eta(az) - aF_\eta(z) = \eta_a \circ e_\Upsilon(z).$$

Avec ces notations, en prenant $L = k$, le résultat obtenu par A. Thiery [T1] est le suivant.

Proposition 4 [T1]. *Soient λ et w des éléments non nuls de Λ_Υ pour lesquels le nombre $F_\eta(w) - \frac{F_\eta(\lambda)}{\lambda}w$ est non nul. Alors les deux nombres*

$$F_\eta(w) - \frac{F_\eta(\lambda)}{\lambda}w \quad \text{et} \quad \frac{F_\eta(\lambda)}{\lambda}$$

sont algébriquement indépendants sur k .

On rappelle encore que, si Υ vérifie une égalité de la forme $\Upsilon_T(X) = TX + gX^q - X^{q^2}$, alors on a la relation de Legendre suivante démontrée par G.W. Anderson (voir [Ge7])

$$\left(F_\eta(w_1)w_2 - F_\eta(w_2)w_1\right)^{q-1} = \tilde{\pi}^{q-1},$$

où (w_1, w_2) désigne une base du réseau Λ_Υ , et où $\eta : T \mapsto \eta_T = \mathcal{F}$. Ainsi, la proposition 4 donne

$$\left(\frac{\tilde{\pi}}{w_2}\right)^{q-1} = \left(F_\eta(w_1) - \frac{F_\eta(w_2)}{w_2}w_1\right)^{q-1} \notin \bar{k}.$$

On fixe maintenant $t \in \mathcal{C}$, tel que $|t| < q^{-\frac{1}{q-1}}$. Soit $z \in \mathcal{C} \setminus k_\infty$ tel que $t = t(z)$. On considère le module de Drinfeld $\Upsilon^{(z)}$ de réseau des périodes $A \oplus zA$:

$$\Upsilon_T^{(z)}(X) = TX + g(z)X^q + \Delta(z)X^{q^2}.$$

On note $j(z) = g(z)^{q+1}/\Delta(z)$ son invariant modulaire, et on suppose que $j(z)^{1/(q+1)}$ est dans k . Soit $\mu \in \mathcal{C}$ pour lequel on a $\mu^{q^2-1} = -\frac{1}{\Delta(z)}$, alors le module de Drinfeld Υ associé au réseau $\frac{1}{\mu}A \oplus \frac{z}{\mu}A$ vérifie

$$\Upsilon_T(X) = TX + \mu^{q-1}g(z)X^q - X^{q^2}.$$

Puisque $(\mu^{q-1}g(z))^{q+1} = -j(z)$, alors Υ est défini sur k , et donc la période $\frac{\tilde{\pi}}{\mu}$ n'est pas algébrique sur k , ainsi on a

$$\frac{\Delta(z)}{\tilde{\pi}^{q^2-1}} = \overline{\Delta}(t) \notin \bar{k}.$$

Finalement, le résultat d'A. Thiery a la conséquence suivante

$$\text{Si } j(t)^{1/(q+1)} \in k, \text{ alors } \overline{\Delta}(t) \notin \bar{k}.$$

Cependant, on peut reprendre sa démonstration en substituant à l'extension L de k , le corps L' engendré sur L par les coefficients du module de Drinfeld Υ et de la bidérivation η . On obtiendrait alors le même résultat pour les modules de Drinfeld définis sur $\bar{k}$. Cela entraînerait clairement le théorème prouvé ici. La démonstration est malgré tout différente; ici on a recours aux corps de fonctions modulaires, tandis qu'A. Thiery fait essentiellement appel aux fonctions exponentielles et à leurs équations fonctionnelles.

On commence par donner quelques définitions et remarques sur les formes modulaires, puis sur les fonctions modulaires de niveau supérieur. Pour une étude plus approfondie, le lecteur pourra se référer à [Ge1] ou à [Ge3]. Le but du paragraphe 2 est essentiellement de placer les deux fonctions $z \mapsto j(az)$ et $z \mapsto \overline{\Delta}(az)$ dans une même extension finie de $k(j, \overline{\Delta})$, dont on maîtrise le degré sur $k(j, \overline{\Delta})$ quand a parcourt A . Au paragraphe suivant, on construit un nouveau polynôme modulaire $\overline{\Phi}_a(X, Y)$ dont on majore la hauteur. Pour cela, on suit en partie la démarche de L.C. Hsia qui donne dans [Hs] une estimation exacte de la hauteur du polynôme modulaire classique. La hauteur des nombres $j(az)$ est obtenue à l'aide de hauteurs différentielles dans [ADR], mais la méthode utilisée ne donne aucun résultat pour les nombres $\overline{\Delta}(az)$. C'est donc ce polynôme modulaire $\overline{\Phi}_a(X, Y)$ qui fournira la majoration de la hauteur des nombres $\overline{\Delta}(az)$. Enfin, la dernière partie est consacrée à la preuve du théorème annoncé. On y applique un lemme de Liouville aux nombres $j(az)$ et $\overline{\Delta}(az)$ pour a dans A , convenablement choisis.

2 - Fonctions modulaires

On définit le demi-plan supérieur Ω par

$$(7) \quad \Omega = \mathcal{C} \setminus k_\infty.$$

Pour $z \in \mathcal{C}$, on note $|z|_i = \inf_{x \in k_\infty} |z - x|$ sa partie imaginaire et $|z|_A = \inf_{a \in A} |z - a|$. Alors, un élément de $\mathcal{C}$ est dans Ω , si et seulement si sa partie imaginaire est non nulle. Soit $c > 0$, on définit l'ensemble suivant

$$(8) \quad \Omega_c = \{z \in \Omega, |z|_i > c\}.$$

Dans la suite, on considère des modules de Drinfeld de rang 2 définis sur $\bar{k}$:

$$(9) \quad \Upsilon_T = T\mathcal{F}^0 + g\mathcal{F} + \Delta\mathcal{F}^2.$$

On remarque que la quantité $j(\Upsilon) = g^{q+1}/\Delta$ ne dépend que de la classe d'isomorphisme de Υ . On l'appelle invariant modulaire de Υ .

Le groupe $GL_2(k_\infty)$ agit sur le demi-plan supérieur Ω par :

$$(10) \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k_\infty), \quad \forall z \in \Omega, \quad \gamma z = \frac{az + b}{cz + d}.$$

On associe à Υ son réseau des périodes $\Lambda = Aw_1 \oplus Aw_2$, que l'on normalise en $A \oplus Az$. Alors deux éléments z et z' définissent des modules de Drinfeld isomorphes si et seulement si ils sont conjugués par l'action de $\Gamma = GL_2(A)$. On obtient ainsi une bijection entre $\mathcal{C}$ et le quotient $GL_2(A) \backslash \Omega$ fournie par l'invariant modulaire j .

2.1. Formes modulaires

Soient m et l des entiers et $f : \Omega \longrightarrow \mathcal{C}$ une fonction holomorphe vérifiant

$$(11) \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A), \quad \forall z \in \Omega, \quad f(\gamma z) = (\det(\gamma))^{-m} (cz + d)^l f(z).$$

En particulier, on a

$$\forall z \in \Omega, \quad \forall a \in A, \quad f(z + a) = f(z).$$

Ainsi, f peut être considérée comme une fonction définie sur $A \backslash \Omega$. Or, d'après E.U. Gekeler (voir [Ge5]), pour tout $c > 1$, $z \longmapsto t(z)$ (voir (6)) définit un isomorphisme du quotient $A \backslash \Omega_c$ sur une boule épointée $B_r \setminus \{0\} = \{z \in \mathcal{C} \setminus \{0\}, |z| < r\}$. Par conséquent, il existe une fonction f^* telle que l'on ait

$$\forall z \in \Omega_1, \quad f^*(t(z)) = f(z).$$

On dira que f est une *forme modulaire de poids l et de type m* , si f^* admet un développement en série entière autour de 0. On notera M_l^m l'espace vectoriel sur $\mathcal{C}$ des formes modulaires de poids l et de type m , alors $\mathcal{M} = \bigoplus_{l,m} M_l^m$ et $\mathcal{M}^0 = \bigoplus_l M_l^0$ sont des

algèbres graduées.

On remarque que si $M_l^m \neq \{0\}$ alors $l \equiv 2m[q-1]$.

Exemple :

A chaque $z \in \Omega$, on associe le module de Drinfeld $\Upsilon^{(z)}$ associé au réseau $A \oplus Az$, et donc des nombres $g(z)$ et $\Delta(z)$. On définit ainsi des formes modulaires de type 0 et de poids respectifs $q-1$ et q^2-1 , qui sont donc aussi des fonctions en la variable t .

Dans la suite, on omettra les astérisques, ainsi g et Δ désigneront aussi bien des fonctions en z que des fonctions en la variable t . On notera encore $\overline{\Delta} = \tilde{\pi}^{1-q^2}\Delta$ et $\overline{g} = \tilde{\pi}^{1-q}g$, de sorte que les fonctions $\overline{g}$ et $\overline{\Delta}$ ont des développements en t à coefficients dans A . En effet, comme E.U. Gekeler dans [Ge5], on note B_0 l'ensemble des séries

$$f = \sum_{j \geq 0} m_j s^j \quad \text{où } s = t^{q-1}, \quad m_j \in A \quad \text{et} \quad \deg m_j \leq j.$$

Il est clair que B_0 est stable pour l'addition, la multiplication et que si $f = \sum_{j \geq 0} m_j s^j$ est un élément de B_0 vérifiant $m_0 \neq 0$, alors la fonction $1/f$ est aussi un élément de B_0 . Il est vu dans [Ge5] que la fonction $\overline{\Delta}(s)/s = \tilde{\pi}^{1-q^2}\Delta(s)/s$ est dans B_0 . Comme $\overline{\Delta} = -s + \dots$ alors $s/\overline{\Delta}(s)$ appartient à B_0 . D'autre part, la fonction $\overline{g}(s) = \tilde{\pi}^{1-q}g(s) = 1 + \dots$ est elle aussi dans B_0 et donc $sj(s) \in B_0$. Ainsi, on a les deux développements suivants

$$(12) \quad \overline{\Delta}(s) = \sum_{i \geq 1} \delta_i s^i = \sum_{i \geq 1} \delta_i t^{i(q-1)} \quad \text{avec} \quad \deg \delta_i \leq i-1,$$

$$(13) \quad j(s) = \sum_{i \geq -1} \gamma_i s^i = \sum_{i \geq -1} \gamma_i t^{i(q-1)} \quad \text{avec} \quad \deg \gamma_i \leq i+1.$$

Enfin, comme dans toute démonstration de transcendance, on doit s'assurer de l'indépendance algébrique de ces fonctions. On la montre facilement en utilisant leurs propriétés modulaires. On peut donc énoncer le lemme suivant.

Lemme 1. *Les fonctions Δ et j sont algébriquement indépendantes sur $\mathcal{C}$.*

Preuve - On suppose au contraire, que ces deux fonctions sont algébriquement dépendantes sur $\mathcal{C}$. Alors, puisque j est transcendante, on peut trouver une relation non triviale :

$$P_0(j)\Delta^n + \dots + P_{n-1}(j)\Delta + P_n(j) = 0.$$

Si on applique cette égalité en γz où $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(A)$, on obtient que pour tout z dans Ω , le polynôme

$$P_0(j(z))X^n + \dots + P_{n-1}(j(z))X + P_n(j(z))$$

est annulé par les $(cz+d)^{q^2-1}\Delta(z)$ qui sont en nombre infini. C'est donc le polynôme nul. Comme j est transcendante, on obtient une contradiction. $\square$

2.2. Fonctions modulaires de niveau a

Pour a dans $A \setminus \{0\}$, on introduit maintenant une famille de fonctions, dites *fonctions modulaires de niveau a* , contenant les formes modulaires que l'on vient de définir. Il s'agit de fonctions qui sont modulaires pour un certain sous-groupe Γ_a de Γ . Dans le cas classique, elles sont par exemples étudiées dans [L1] (Chapitre 6). Dans notre cadre, E.U. Gekeler les introduit dans [Ge1] ou dans [Ge3] (Chapitre VII). On note

$$(14) \quad t_a = t(az) = \frac{1}{e_c(\widetilde{\pi}az)} = \frac{1}{C_a(e_c(\widetilde{\pi}z))} = \frac{1}{C_a(1/t)}.$$

Soit $a \in A$ unitaire et Γ_a le sous-groupe de $\Gamma = GL_2(A)$ suivant

$$(15) \quad \Gamma_a = \left\{ \gamma \in \Gamma, \quad \gamma \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{a} \right\}.$$

Ce groupe est appelé sous-groupe de congruence de niveau a de Γ .

Soit $f : \Omega \longrightarrow \mathcal{C}$ une fonction méromorphe et stable par Γ_a . En particulier, pour tout élément z de $\mathcal{C}$, elle vérifie $f(z + a) = f(z)$. Puisque pour tout $c > 1$, $z \longmapsto t(z)$ définit un isomorphisme de $A \setminus \Omega_c$ sur une boule époutée $B_r \setminus \{0\}$, alors pour tout $c > 1$, l'application

$$(16) \quad z \longmapsto t_{1/a} = t_{1/a}(z) = \frac{1}{e_c(\widetilde{\pi}z/a)}$$

définit un isomorphisme du quotient $a.A \setminus \Omega_c$ sur $B_r \setminus \{0\}$. Comme précédemment, on peut trouver une fonction f^* telle que $f^*(t_{1/a}) = f(z)$. Si f^* possède un développement en série de Laurent en 0, et s'il en est de même pour les $(f \circ \gamma)^*$ où γ parcourt Γ , on dira que f est une fonction modulaire de niveau a sur Ω .

On donne quelques exemples intervenant ultérieurement. Le suivant est classique, sa preuve se déroule très naturellement à l'image de celle donnée dans [L1] dans le cadre de la caractéristique nulle.

Lemme 2. *Soit $\alpha \in M_2(A)$ de déterminant a . Alors, $j \circ \alpha$ est une fonction modulaire de niveau a .*

Preuve - Soit $\beta = I + a.M \in \Gamma_a$. La matrice $\beta' = \alpha\beta\alpha^{-1} = I + \alpha M(a\alpha^{-1})$ est de déterminant 1 et à coefficients dans A , ainsi β' est dans $\bar{\Gamma} = SL_2(A)$ et donc on a

$$j \circ \alpha \circ \beta = j \circ \beta' \circ \alpha = j \circ \alpha.$$

D'autre part, si $\gamma \in \Gamma$ alors $\beta'' = \gamma\beta\gamma^{-1} = I + a\gamma M\gamma^{-1} \in \Gamma_a$, ainsi on a

$$j \circ \alpha \circ \gamma \circ \beta = j \circ \alpha \circ \beta'' \circ \gamma = j \circ \alpha \circ \gamma.$$

Les autres propriétés concernant les développements en $t_{1/a}$ de $j \circ \alpha$ et des fonctions $j \circ \alpha \circ \gamma$ pour γ dans Γ , découlent facilement du développement en t de la fonction j . Ainsi, $j \circ \alpha$ est bien une fonction modulaire de niveau a . $\square$

Soit $a \in A$. Comme dans le cas classique, le groupe $\Gamma = GL_2(A)$ agit par multiplication à droite, et par multiplication à gauche sur l'ensemble

$$(17) \quad \Delta_a^* = \left\{ \alpha = \begin{bmatrix} a_0 & b_0 \\ c_0 & d_0 \end{bmatrix} \in M_2(A), (a_0, b_0, c_0, d_0) = 1, \exists \mu \in \mathbb{F}_q^*, \det(\alpha) = \mu a \right\}.$$

On a le système de représentants pour l'action à gauche suivant, que l'on note $\Delta_a^*(\Gamma)$,

$$(18) \quad \Delta_a^*(\Gamma) = \left\{ \alpha = \begin{bmatrix} a_0 & b_0 \\ 0 & d_0 \end{bmatrix} \in \Delta_a^*, a_0 \text{ unitaire, } a_0 d_0 = a, \deg b_0 < \deg d_0 \right\}.$$

On notera $\psi(a)$ son cardinal. S. Bae, en appendice de [Ba], démontre l'égalité suivante

$$(19) \quad \psi(a) = |a| \prod_{b|a} \left(1 + \frac{1}{|b|} \right).$$

On a alors la majoration suivante (voir lemme 7 de [ADR])

$$(20) \quad \exists C > 0, \quad \psi(a) \leq C|a| \log \log |a| + C,$$

où C est une constante ne dépendant que de q .

On définit maintenant la fonction h_α pour $\alpha = \begin{bmatrix} a_0 & b_0 \\ 0 & d_0 \end{bmatrix} \in \Delta_a^*(\Gamma)$ par

$$(21) \quad h_\alpha(z) = a_0^{q^2-1} \frac{\Delta \circ \alpha(z)}{\Delta(z)}.$$

Avec ces notations, on a le lemme suivant.

Lemme 3. *Soit $\alpha \in \Delta_a^*(\Gamma)$. Alors, h_α est une fonction modulaire de niveau a .*

Preuve - Soit $\beta = I + a.M \in \Gamma_a$ et $\beta' = \alpha\beta\alpha^{-1}$. On écrit

$$\alpha = \begin{bmatrix} a_0 & b_0 \\ 0 & d_0 \end{bmatrix} \quad \beta = \begin{bmatrix} l & m \\ n & p \end{bmatrix} \quad \beta' = \begin{bmatrix} l' & m' \\ n' & p' \end{bmatrix}.$$

De l'égalité $\alpha\beta = \beta'\alpha$, on tire les relations $nd_0 = n'a_0$ et $d_0p = n'b_0 + p'd_0$. Comme Δ est une forme modulaire de poids $(q^2 - 1)$, on obtient sans difficulté l'égalité $h_\alpha \circ \beta = h_\alpha$. Les autres propriétés concernant les développements en $t_{1/a}$ de h_α et des fonctions $h_\alpha \circ \gamma$ pour γ dans Γ , découlent facilement du développement en t de la fonction Δ . On a donc bien que h_α est une fonction modulaire pour Γ_a . $\square$

On définit maintenant une famille de fonctions modulaires de niveau a , qui sont les analogues des fonctions de Weber classiques. On a vu précédemment, qu'à chaque z de Ω , on peut associer un module de Drinfeld $\Upsilon^{(z)}$ de rang 2; on note e_z son exponentielle. On considère alors les fonctions f_u définies sur Ω , par

$$(22) \quad \forall z \in \Omega, \quad f_u(z) = g(z)e_z^{q-1}(u).$$

Pour r et s dans A non divisibles par a , on note $u(z, r, s) = \frac{rz + s}{a}$, et on définit les fonctions suivantes.

$$(23) \quad \forall z \in \Omega, \quad f_{(r,s)}(z) = g(z)e_z^{q-1}(u(z, r, s)).$$

On a alors les propriétés élémentaires suivantes (c.f. [Ge3] chapitre VII).

Lemme 4 [Ge3].

- 1- $\forall \gamma \in \Gamma, \quad f_{(r,s)\gamma}(z) = f_{(r,s)}(\gamma z),$
- 2- Les fonctions $f_{(r,s)}$ sont modulaires de niveau a ,
- 3- $f_{(r,s)} = f_{(r',s')} \iff \exists c \in \mathbb{F}_q^*, \quad (r, s) \equiv c(r', s') \pmod{a}.$

2.3. Corps de fonctions modulaires de niveau a

L'objectif de ce paragraphe est de placer les deux fonctions $\overline{\Delta} \circ a : z \mapsto \overline{\Delta}(az) = \overline{\Delta}(t_a)$ et $j \circ a : z \mapsto j(az) = j(t_a)$ (voir page 32) dans une extension finie de $k(\overline{\Delta}, j)$ dont on maîtrise le degré en fonction de a . On sait déjà que la fonction $j \circ a$ est racine du polynôme modulaire classique (voir par exemple [Ba]) défini par

$$(24) \quad \prod_{\alpha \in \Delta_a^*(\Gamma)} (X - j \circ \alpha) \in k(j)[X].$$

Ainsi, la fonction $j \circ a$ est algébrique de degré inférieur à $\psi(a)$ sur $k(j)$. On pose

$$(25) \quad \alpha_a = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in \Delta_a^*(\Gamma).$$

Dans la suite, on montre que la fonction $h_{\alpha_a} = a^{q^2-1} \frac{\overline{\Delta} \circ a}{\overline{\Delta}}$ est un élément de $k(j, j \circ a)$. Pour cela, on utilise les résultats de E.U. Gekeler sur les corps de fonctions modulaires.

On note $F_a(\mathcal{C})$ le corps des fonctions modulaires de niveau a définies sur $\mathcal{C}$. On sait classiquement que $F_1(\mathcal{C}) = \mathcal{C}(j)$. Le groupe $\Gamma = GL_2(A)$ agit sur $F_a(\mathcal{C})$ par composition $f \mapsto f \circ \gamma$. Ainsi, d'après le lemme 4, il agit sur les fonctions de Weber par $f_{(r,s)} \mapsto f_{(r,s)\gamma}$. On définit

$$(26) \quad Z = \mathbb{F}_q^* \cdot I = \left\{ \begin{bmatrix} \mu & 0 \\ 0 & \mu \end{bmatrix}, \mu \in \mathbb{F}_q^* \right\}.$$

Puisque Γ_a et Z agissent trivialement sur $F_a(\mathcal{C})$, on peut définir une action du groupe fini $\Gamma/Z \cdot \Gamma_a$ sur $F_a(\mathcal{C})$. Plus précisément, E.U. Gekeler montre comme dans le cas classique la proposition suivante (proposition 3.4.1 de [Ge1]).

Proposition 5 [Ge1]. *Le corps $F_a(\mathcal{C})$ est le corps engendré sur $\mathcal{C}$ par les fonctions j et $f_{(r,s)}$ où $r, s \in A \setminus a.A$. De plus, l'extension $F_1(\mathcal{C}) = \mathcal{C}(j) \hookrightarrow F_a(\mathcal{C}) = \mathcal{C}(j, f_{(r,s)})_{r,s}$ est galoisienne et son groupe de galois est*

$$\Gamma/Z \cdot \Gamma_a \simeq \left\{ \gamma \in GL_2(A/a.A), \det(\gamma) \in \mathbb{F}_q^* \right\} / Z.$$

On considère le groupe de congruence suivant

$$(27) \quad \Gamma_0(a) = \left\{ \begin{bmatrix} a_0 & b_0 \\ c_0 & d_0 \end{bmatrix} \in \Gamma, \quad c_0 \equiv 0 \pmod{a} \right\}.$$

D'après les travaux de E.U. Gekeler (voir [Ge2]), le corps des fonctions modulaires pour $\Gamma_0(a)$ et définies sur $\mathcal{C}$ est le sous-corps $\mathcal{C}(j, j \circ a)$ de $F_a(\mathcal{C})$. Avec ces résultats, on peut démontrer la proposition suivante, qui répond à la question posée en début de paragraphe.

Proposition 6. *Le corps de fonctions $\mathcal{L}_a = k(\overline{\Delta}, j, j \circ a)$ est une extension finie de $k(\overline{\Delta}, j)$ de degré inférieur à $\psi(a)$, et qui contient la fonction $\overline{\Delta} \circ a$.*

Preuve - Tout d'abord, puisque l'on a l'égalité (14), la fonction

$$h_{\alpha_a} = a^{q^2-1} \frac{\overline{\Delta} \circ a}{\overline{\Delta}}$$

a un développement de Laurent en t à coefficients dans k . On montre alors que la fonction h_{α_a} est modulaire pour le groupe $\Gamma_0(a)$. Il suffit pour cela de voir qu'elle est fixée par le groupe $\Gamma_0(a)$.

Soit $\gamma = \begin{bmatrix} a_0 & b_0 \\ ac_0 & d_0 \end{bmatrix}$ une matrice à coefficients dans A de déterminant premier avec a .

On note γ' la matrice $\begin{bmatrix} a_0 & ab_0 \\ c_0 & d_0 \end{bmatrix}$ de sorte qu'on ait l'égalité

$$\alpha_a \circ \gamma = \gamma' \circ \alpha_a.$$

En utilisant les propriétés modulaires de $\overline{\Delta}$, on montre facilement que l'on a

$$\frac{\overline{\Delta} \circ \gamma' \circ \alpha_a}{\overline{\Delta} \circ \gamma} = \frac{\overline{\Delta} \circ \alpha_a}{\overline{\Delta}}.$$

Par conséquent, la fonction h_{α_a} est fixée par le groupe $\Gamma_0(a)$. Par suite, elle se trouve dans le corps $\mathcal{C}(j, j \circ a)$. Ainsi, il existe deux polynômes $P(X, Y)$ et $Q(X, Y)$ de $\mathcal{C}[X, Y]$, pour lesquels on a

$$h_{\alpha_a} = \frac{P(j, j \circ a)}{Q(j, j \circ a)}.$$

Or, les fonctions h_{α_a} , j et $j \circ a$ ont des développements de Laurent en t à coefficients dans k . Par conséquent, l'égalité

$$h_{\alpha_a}(t) \times Q(j(t), j \circ a(t)) - P(j(t), j \circ a(t)) = 0$$

est équivalente à un système linéaire (de rang fini) à coefficients dans k et dont les inconnues sont les coefficients des polynômes $P(X, Y)$ et $Q(X, Y)$. On sait que ce système a une solution non nulle à coordonnées dans $\mathcal{C}$, nécessairement il a en au moins une non nulle à coordonnées dans k . Par suite, on peut choisir les deux polynômes $P(X, Y)$ et $Q(X, Y)$ dans $k[X, Y]$. Ainsi, la fonction h_{α_a} est bien un élément du corps $k(j, j \circ a)$. Par définition de h_{α_a} , la fonction $\overline{\Delta} \circ a$ est bien un élément de $\mathcal{L}_a = k(\overline{\Delta}, j, j \circ a)$. Or, la fonction $j \circ a$ est algébrique de degré inférieur à $\psi(a)$ sur $k(j)$, la proposition 6 est donc établie. $\square$

3 - Etude d'un nouveau polynôme modulaire

Soit $k \hookrightarrow E$ une extension finie de degré $\mathcal{D}$. On rappelle la notion de hauteur projective d'un élément $\beta = (\beta_0, \dots, \beta_m)$ de $\mathbb{P}^m(E)$:

$$h(\beta) = \frac{1}{\mathcal{D}} \sum_{\omega \in M_E} d_\omega \max_{0 \leq i \leq m} (-\omega(\beta_i)),$$

où M_E désigne l'ensemble de toutes les places de E et d_ω le degré résiduel sur $\mathbb{F}_q$ en la place ω normalisée par $\omega(E) = \mathbb{Z} \cup \{+\infty\}$. Si $f(X_1, \dots, X_l) = \sum a_\lambda X^\lambda \in \bar{k}[X_1, \dots, X_l]$, alors on appelle hauteur du polynôme f

$$H(f) = h(1, a_\lambda).$$

On définit encore la mesure de Mahler d'un polynôme $P(X) = a_0 \prod_{j=1}^D (X - \xi_j) \in \mathcal{C}[X]$ par

$$m(P) = \deg a_0 + \sum_{j=1}^D \max\{0, \deg \xi_j\}.$$

La hauteur d'un polynôme à coefficients dans A est aussi sa mesure de Mahler et le maximum des degrés de ses coefficients. Ainsi, si

$$P(X) = a_0 X^D + \dots + a_{D-1} X + a_D = a_0 \prod_{j=1}^D (X - \xi_j) \in A[X],$$

alors on a les égalités suivantes.

$$\begin{aligned} H(P) &= m(P), \\ &= \deg a_0 + \sum_{j=1}^D \max\{0, \deg \xi_j\}, \\ &= \max_{i=0, \dots, D} \deg a_i. \end{aligned}$$

Dans cette partie, on construit un polynôme $\bar{\Phi}_a(X, Y)$ pour tout a de A non nul, dont on majore la hauteur. L'intérêt de ce polynôme est qu'il est annulé par le couple

$$\left(a^{q^2-1} \frac{\bar{\Delta} \circ a}{\bar{\Delta}}, j \right).$$

Ceci permettra dans le paragraphe 4, d'obtenir une majoration de la hauteur du nombre $\bar{\Delta}(t_a)$ supposé algébrique sur le corps k .

Soient $\alpha_1, \dots, \alpha_{\psi(a)}$ les éléments de l'ensemble $\Delta_a^*(\Gamma)$ défini en (18). On considère le polynôme suivant

$$(28) \quad \Phi_a(X) = \prod_{i=1}^{\psi(a)} (X - h_{\alpha_i}),$$

où les fonctions h_{α_i} sont définies en (21). On va montrer que c'est un polynôme modulaire, c'est-à-dire que ses coefficients sont des polynômes en la fonction j . Dans la suite les U_i désigneront les coefficients de ce polynôme :

$$(29) \quad \Phi_a(X) = \sum_{i=0}^{\psi(a)} U_i X^i.$$

3.1. Développement en $t_{1/a}$ de U_i

Dans ce paragraphe, on démontre la proposition suivante.

Proposition 7. *Il existe des éléments $u_{i,j}$ de $A[e_c(\tilde{\pi}/a)]$, tels que l'on ait*

$$U_i = \sum_{j \geq -(q-1)|a|\psi(a)} u_{i,j}(t_{1/a})^j.$$

Preuve - Les fonctions h_α n'ont pas nécessairement de développement en t mais elles en ont un en $t_{1/a}$. On étudie ces développements. On a vu d'une part, que la fonction $\frac{s}{\Delta}$ appartient à B_0 (voir page 32). D'autre part, on a les égalités

$$\begin{aligned} t(z) &= t(az/a) = \frac{1}{C_a(1/t_{1/a}(z))}, \\ &= \sum_{j \geq |a|} u_j t_{1/a}(z)^j \quad \text{où les } u_j \text{ sont dans } A. \end{aligned}$$

Ainsi, $\frac{s}{\Delta}$ a un développement en série entière en $t_{1/a}$ à coefficients dans A .

Soit $\alpha = \begin{bmatrix} a_0 & b_0 \\ 0 & d_0 \end{bmatrix}$ un élément de $\Delta_a^*(\Gamma)$, alors on a le développement qui suit.

$$\begin{aligned} t(\alpha(z)) &= \left(e_c \left(\frac{a_0 \tilde{\pi} z + \tilde{\pi} b_0}{d_0} \right) \right)^{-1} = t \left(\frac{a_0 z}{d_0} \right) \left(1 + e_c \left(\frac{\tilde{\pi} b_0}{d_0} \right) t \left(\frac{a_0 z}{d_0} \right) \right)^{-1}, \\ &= \sum_{n \geq 0} (-1)^n e_c \left(\frac{\tilde{\pi} b_0}{d_0} \right)^n t \left(\frac{a_0 z}{d_0} \right)^{n+1} = \sum_{n \geq 0} (-1)^n e_c \left(\frac{\tilde{\pi} b_0}{d_0} \right)^n \left(\frac{1}{C_{a_0^2}(1/t_{1/a})} \right)^{n+1}, \\ &= \sum_{j \geq |a_0|^2} P_{j,a_0} \left(e_c \left(\frac{\tilde{\pi} b_0}{d_0} \right) \right) t_{1/a}^j, \end{aligned}$$

où $P_{j,a_0} \in A[X]$. Ainsi, il est clair que $\overline{\Delta}(\alpha(z))$ a un développement en série entière en $t_{1/a}$, à coefficients dans $A[e_c(\tilde{\pi}/a)]$.

Enfin, on aura besoin du développement suivant.

$$\begin{aligned} 1/s(z) &= e(\tilde{\pi} a z/a)^{q-1} = C_a(1/t_{1/a})^{q-1}, \\ &= \left(\sum_{i=0}^{\deg a} l_i(a)/t_{1/a}^{q^i} \right)^{q-1} = \sum_{j=q-1}^{(q-1)|a|} r_j(a)/t_{1/a}^j \quad \text{où les } r_j(a) \text{ sont dans } A. \end{aligned}$$

Finalement, vu sa définition (21), la fonction h_α a un développement en série de Laurent du type

$$h_\alpha = \sum_{i \geq -(q-1)|a|} Q_i(\alpha)(t_{1/a})^i \quad \text{où les } Q_i(\alpha) \text{ sont dans } A[e_c(\tilde{\pi}/a)].$$

Comme $\text{card} \Delta_a^*(\Gamma) = \psi(a)$, la proposition 7 en découle facilement. $\square$

3.2. Propriétés modulaires du polynôme Φ_a

Dans ce paragraphe, on démontre que les coefficients U_i de $\Phi_a(X)$ (voir (29)) sont des polynômes en j dont on majore le degré. Plus précisément, on obtient la proposition suivante.

Proposition 8. *Soit $a \in A$ unitaire, alors il existe $\overline{\Phi}_a(X, Y) \in A[X, Y]$ de degré en Y inférieur à $\psi(a)$ tel que l'on ait*

$$\overline{\Phi}_a(X, j) = \prod_{i=1}^{\psi(a)} (X - h_{\alpha_i}).$$

Preuve - Avant de commencer la preuve, on donne quelques remarques concernant l'action de Γ sur les fonctions h_{α_i} . Le théorème 1.1 de S. Bae [Ba], dit que $GL_2(A)$ agit transitivement à droite sur les classes à gauches, ainsi on a

$$\forall \alpha \in \Delta_a^*(\Gamma), \quad \forall \gamma \in GL_2(A), \quad \exists \alpha' \in \Delta_a^*(\Gamma), \quad \exists \gamma' \in GL_2(A) \text{ tels que } \alpha\gamma = \gamma'\alpha'.$$

Une conséquence en est le lemme suivant.

Lemme 5. *Le groupe Γ permute transitivement les fonctions h_{α_i} .*

Preuve - Soit $\alpha \in \Delta_a^*(\Gamma)$ et $\gamma \in GL_2(A)$. On peut trouver $\alpha' \in \Delta_a^*(\Gamma)$ et $\gamma' \in GL_2(A)$ tels que $\alpha\gamma = \gamma'\alpha'$. Si on écrit :

$$\alpha = \begin{bmatrix} a_0 & b_0 \\ 0 & d_0 \end{bmatrix} \quad \alpha' = \begin{bmatrix} a'_0 & b'_0 \\ 0 & d'_0 \end{bmatrix} \quad \gamma = \begin{bmatrix} l & m \\ n & p \end{bmatrix} \quad \gamma' = \begin{bmatrix} l' & m' \\ n' & p' \end{bmatrix},$$

on obtient les égalités $nd_0 = a'_0n'$ et $d_0p = b'_0n' + p'd'_0$. Ainsi :

$$\begin{aligned} h_\alpha \circ \gamma(z) &= a_0^{q^2-1} \frac{\overline{\Delta} \circ \gamma' \alpha'(z)}{\overline{\Delta} \circ \gamma(z)} = \left(a_0 \frac{n'(a'_0z + b'_0)/d'_0 + p'}{nz + p} \right)^{q^2-1} \frac{\overline{\Delta} \circ \alpha'(z)}{\overline{\Delta}(z)}, \\ &= \left(a_0 \frac{d_0nz + d_0p}{d'_0nz + d'_0p} \right)^{q^2-1} \frac{\overline{\Delta} \circ \alpha'(z)}{\overline{\Delta}(z)} = \left(\frac{a_0d_0}{d'_0} \right)^{q^2-1} \frac{\overline{\Delta} \circ \alpha'(z)}{\overline{\Delta}(z)} = h_{\alpha'}(z), \end{aligned}$$

car on a $a'_0 = \frac{a}{d'_0} = \frac{a_0d_0}{d'_0}$, ce qui achève la preuve du lemme. $\square$

Preuve de la proposition 8 - D'une part, puisque les coefficients de Φ_a sont des fonctions symétriques en les h_{α_i} , il en résulte qu'ils sont stables par l'action de $GL_2(A)$. D'autre part, d'après la proposition 7, les coefficients U_i de Φ_a ont un développement de Laurent en $t_{1/a}$; comme ils sont modulaires, ces développements sont en fait en la variable t . Enfin, d'après ce qui précède, pour tout μ dans $\mathbb{F}_q^*$, les U_i sont stables par $z \mapsto \mu z$, donc aussi par $t \mapsto \mu t$. Ainsi, les U_i ont un développement en série de Laurent en la variable $s = t^{q-1}$. En outre, ils sont de la forme :

$$U_i = \sum_{j \geq -\psi(a)} v_{i,j} s^j,$$

où les $v_{i,j}$ sont a priori dans $A[e_c(\tilde{\pi}/a)]$. D'après [Ca], $\text{Aut}(k(e_c(\tilde{\pi}/a)), k)$ est composé d'automorphismes σ_r définis par $\sigma_r(e_c(\tilde{\pi}/a)) = e_c(r\tilde{\pi}/a)$, où $r \in A$ est premier avec a .

Or, les fonctions h_{α_i} sont permutées par ces automorphismes, donc les coefficients de $\Phi_a(X)$ sont stables par l'action de $\text{Aut}(k(e_c(\tilde{\pi}/a), k))$. Ainsi, ils sont dans $A((s))$. De plus, puisque les seules fonctions modulaires qui sont holomorphes sur Ω et à l'infini sont les constantes, comme dans [L1] (chapitre 5) on a le lemme suivant.

Lemme 6. *Soit f une fonction modulaire qui est holomorphe sur Ω . On suppose que f a un développement de la forme*

$$f = \sum_{i \geq -M} c_i s^i \quad c_{-M} \neq 0, \quad M \geq 0,$$

alors f est un polynôme en j de degré M et dont les coefficients sont dans le A -module engendré par les c_i .

On en conclut que chaque U_i est un polynôme en j de degré inférieur ou égal à $\psi(a)$, et à coefficients dans A , d'où la proposition annoncée. $\square$

3.3. Majoration de la hauteur du polynôme modulaire

Dans ce paragraphe, on donne une majoration de la hauteur du polynôme $\overline{\Phi}_a(X, Y)$. L.C. Hsia dans [Hs] obtient une estimation exacte de celle du polynôme modulaire classique. Ici, on suit un parcours similaire, et on obtient une majoration du même ordre. On notera pour $z \in \Omega$ tel que $|z|_i > 1$:

$$(30) \quad y = j(z) \quad \text{et} \quad \overline{\Phi}_{a,y}(X) = \overline{\Phi}_a(X, y).$$

On commence par majorer la hauteur des polynômes $\overline{\Phi}_{a,y}(X)$ pour certains y . On aura besoin, pour cela, d'exprimer $\deg \overline{\Delta}(z)$ en fonction de $|z|_i$.

Proposition 9. *Soit $z \in \Omega$ tel que $|z|_i = q^{n-\varepsilon} > 1$, où $n \in \mathbb{N}$ et $0 \leq \varepsilon < 1$, alors on a l'égalité*

$$\deg \overline{\Delta}(z) = -C_\varepsilon |z|_i,$$

où $C_\varepsilon = q^\varepsilon(q(1-\varepsilon) + \varepsilon)$.

Preuve - On rappelle tout d'abord le lemme suivant démontré par M.L. Brown dans [B] (lemme 2.6.1) et qui estime la valeur absolue de $t(z)$ en fonction de celle de z .

Lemme 7 [B]. *Soit $z \in \Omega$ satisfaisant $|z| = |z|_A = q^{m-\varepsilon}$, où $m \in \mathbb{Z}$ et $0 \leq \varepsilon < 1$. Si on pose $n = \max\{0, m\}$, alors*

$$|t(z)| = \left| \frac{\tilde{\pi}z}{T^n} \right|^{-q^n}.$$

En particulier, si $n = m \geq 0$ alors $|t(z)| = q^{q^n(\varepsilon - \frac{q}{q-1})}$.

On rappelle que C est le module de Carlitz (voir (4)), ainsi pour $a \in A$ on a :

$$(31) \quad C_a = \sum_{i=0}^{\deg a} l_i(a) \mathcal{F}^i \quad \text{avec} \quad \deg l_i(a) = (\deg a - i)q^i \leq \frac{|a| - q^i}{q - 1}.$$

On définit par $f_a(t) = t^{|a|}C_a\left(\frac{1}{t}\right)$ le polynôme réciproque de C_a . Ainsi, si a est unitaire, on a

$$f_a(t) = \sum_{i=0}^{\deg a} l_i(a)t^{|a|-q^i} = 1 + \sum_{i=0}^{\deg a-1} l_i(a)t^{|a|-q^i} = 1 + \epsilon_a(t).$$

Soient $\varepsilon < 1$ et $t \in \mathcal{C}$ tel que $|t| \leq q^{\varepsilon - \frac{q}{q-1}}$, alors on a les majorations

$$\begin{aligned} \deg(l_i(a)t^{|a|-q^i}) &\leq (|a| - q^i) \left(\frac{1}{q-1} + \deg(t) \right), \\ &\leq (q-1) \left(\frac{1}{q-1} + \deg(t) \right) \leq -(q-1)(1-\varepsilon). \end{aligned}$$

Ainsi, si $|t| \leq q^{\varepsilon - \frac{q}{q-1}}$ alors

$$(32) \quad f_a(t) = 1 + \epsilon_a(t) \quad \text{avec} \quad |\epsilon_a(t)| \leq q^{-(q-1)(1-\varepsilon)}.$$

On rappelle la formule du produit obtenue par E.U. Gekeler dans [Ge4] :

$$\overline{\Delta}(z) = -t(z)^{q-1} \prod_{a \in A^+} f_a(t(z))^{(q^2-1)(q-1)},$$

où A^+ désigne le sous-ensemble de A formé des éléments unitaires.

Soit $z \in \mathcal{C}$ tel qu'il existe $n \in \mathbb{Z}$ pour lequel on a $|z| = |z|_A = q^{n-\varepsilon} > q^{-1}$. Le lemme 7 donne les majorations

$$|t(z)| \leq q^{q^n(\varepsilon - \frac{q}{q-1})} \leq q^{\varepsilon - \frac{q}{q-1}}$$

et d'après (32), on a la majoration

$$|\epsilon_a(t)| \leq q^{-(q-1)(1-\varepsilon)}.$$

En reportant dans la formule du produit, on obtient l'égalité suivante

$$(33) \quad \overline{\Delta}(z) = -t(z)^{q-1} \prod_{a \in A^+} (1 + \epsilon_a(t(z)))^{(q^2-1)(q-1)} = -t(z)^{q-1} (1 + \zeta(t(z))),$$

avec $|\zeta(t(z))| \leq q^{-(q-1)(1-\varepsilon)}$.

On termine alors la preuve de la proposition 9. Puisque $|z|_i > 1$, on peut trouver $u \in A$, vérifiant les égalités $|z|_i = |z|_A = |z - u|$. On pose $z' = z - u$, ainsi $|z'| = |z'|_A = q^{n-\varepsilon}$ donc on a

$$|\zeta(t(z'))| \leq q^{-(q-1)(1-\varepsilon)}.$$

Or, puisque $\overline{\Delta}$ est une forme modulaire, $\overline{\Delta}(z) = \overline{\Delta}(z')$ et on a les égalités

$$\begin{aligned} \deg \overline{\Delta}(z) &= -(q-1)q^n \left(\frac{q}{q-1} - \varepsilon \right), \\ &= -q^{n-\varepsilon} (q^\varepsilon (q - \varepsilon(q-1))) = -|z|_i C_\varepsilon, \end{aligned}$$

d'où la proposition. □

On peut maintenant donner une majoration de la hauteur des polynômes $\overline{\Phi}_{a,y}$ pour certains y .

Proposition 10. *Soit $z \in \Omega$ tel que $|z| = |z|_i = q^{1-\varepsilon}$ où $0 < \varepsilon < 1$, et $y = j(z)$. Alors on a*

$$m(\overline{\Phi}_{a,y}) \leq (2(q^2 - 1) \deg a + q(q + 1))\psi(a).$$

Preuve - Avec ces notations, on a $\overline{\Phi}_{a,y}(X) = \prod_{\alpha \in \Delta_a^*(\Gamma)} (X - h_\alpha(z))$, et donc on a l'égalité

$$(34) \quad m(\Phi_{a,y}) = \sum_{\alpha \in \Delta_a^*(\Gamma)} \max\{0, \deg(h_\alpha(z))\}.$$

On est ainsi amené à majorer $\deg(h_\alpha(z))$, et donc aussi $\deg(\Delta \circ \alpha(z))$, pour α parcourant $\Delta_a^*(\Gamma)$. On se donne $\alpha = \begin{bmatrix} a_0 & b_0 \\ 0 & d_0 \end{bmatrix} \in \Delta_a^*(\Gamma)$. On a :

$$(35) \quad |\alpha(z)|_i = \left| \frac{a_0 z + b_0}{d_0} \right|_i = \left| \frac{a_0 z}{d_0} \right| = \left| \frac{az}{d_0^2} \right|.$$

On distinguera deux cas.

Premier cas : Si $|\alpha(z)|_i > 1$, c'est-à-dire $|d_0| < \sqrt{|az|}$, alors d'après la proposition 9 on a $\deg \overline{\Delta}(\alpha(z)) = -C_\varepsilon |\alpha(z)|_i < 0$. On obtient les majorations suivantes

$$\begin{aligned} \deg(h_\alpha(z)) &= (q^2 - 1) \deg a_0 + C_\varepsilon |z| (1 - |\alpha(z)|_i), \\ &\leq (q^2 - 1) \deg a + C_\varepsilon |z|, \\ &\leq (q^2 - 1) \deg a + q(q(1 - \varepsilon) + \varepsilon). \end{aligned}$$

Finalement on a montré l'inégalité

$$\deg(h_\alpha(z)) \leq (q^2 - 1) \deg a + q(q + 1).$$

Second cas : Si $|\alpha(z)|_i \leq 1$, c'est-à-dire $|d_0| \geq \sqrt{|az|}$, on reprend la construction par L.C. Hsia [Hs] d'un élément γ de $SL_2(A)$ tel que $|\gamma \alpha(z)|_i > 1$. Cette construction utilise les suites de Farey, que l'on ne détaillera pas ici. On pose $N = [\deg d_0 - 1/2 \deg(az)]$. D'après la proposition 3.4 de [Hs], il existe u et v dans A tels que $(u, v) = 1$ et $\deg u < \deg v \leq N$, avec :

$$\left| \frac{b_0}{d_0} - \frac{u}{v} \right| \leq \frac{1}{|u|q^{N+1}}.$$

Le théorème de Bezout donne l'existence de deux éléments r et s de A , pour lesquels la matrice $\gamma = \begin{bmatrix} s & -r \\ u & -v \end{bmatrix}$ est dans $SL_2(A)$.

On a alors :

$$|\gamma\alpha(z)|_i = \frac{|\alpha(z)|_i}{|u\alpha(z) - v|^2} = \frac{|\alpha(z)|_i}{|u|^2 \max \left\{ |\alpha(z)|_i, \left| \frac{b_0}{d_0} - \frac{u}{v} \right| \right\}^2}.$$

En effet, on a

$$\begin{aligned} |u\alpha(z) - v| &= |u| \left| \frac{a_0 z}{d_0} + \left(\frac{b_0}{d_0} - \frac{u}{v} \right) \right|, \\ &= |u| \max \left\{ |\alpha(z)|_i, \left| \frac{b_0}{d_0} - \frac{u}{v} \right| \right\} \quad \text{car} \quad |z| = |z|_i > 1. \end{aligned}$$

En distinguant deux cas, L.C. Hsia obtient dans [Hs] les relations suivantes.

Lemme 8 [Hs].

Si $|\alpha(z)|_i \leq \left| \frac{b_0}{d_0} - \frac{u}{v} \right|$ alors on a $|\gamma\alpha(z)|_i = \frac{|\alpha(z)|_i}{|u|^2 \left| \frac{b_0}{d_0} - \frac{u}{v} \right|^2} \geq q^{2N+2} |\alpha(z)|_i > 1$.

Si $|\alpha(z)|_i > \left| \frac{b_0}{d_0} - \frac{u}{v} \right|$ alors on a $|\gamma\alpha(z)|_i = \frac{1}{|u|^2 |\alpha(z)|_i} \geq \frac{1}{q^{2N} |\alpha(z)|_i} > 1$.

La fonction $\overline{\Delta}$ est une forme modulaire de poids $q^2 - 1$, ainsi on a l'égalité

$$\overline{\Delta}(\gamma\alpha(z)) = (u\alpha(z) - v)^{q^2-1} \overline{\Delta}(\alpha(z)).$$

a) Si $|\alpha(z)|_i \leq \left| \frac{b_0}{d_0} - \frac{u}{v} \right|$ alors :

$$\begin{aligned} \deg \overline{\Delta}(\alpha(z)) &= \deg \overline{\Delta}(\gamma\alpha(z)) - (q^2 - 1) \deg(u\alpha(z) - v), \\ &= -C_\varepsilon |\gamma\alpha(z)|_i - (q^2 - 1) \left(\deg(u) + \deg \left(\frac{b_0}{d_0} - \frac{u}{v} \right) \right), \\ &\leq (q^2 - 1) \deg(d_0 v), \\ &\leq (q^2 - 1)(\deg a + \deg d_0). \end{aligned}$$

b) Si $|\alpha(z)|_i > \left| \frac{b_0}{d_0} - \frac{u}{v} \right|$ alors :

$$\begin{aligned} \deg \overline{\Delta}(\alpha(z)) &= \deg \overline{\Delta}(\gamma\alpha(z)) - (q^2 - 1) \deg(u\alpha(z) - v), \\ &= -C_{1-\varepsilon} |\gamma\alpha(z)|_i - (q^2 - 1) \left(\deg(u) + \deg \left(\frac{a_0 z}{d_0} \right) \right), \\ &\leq (q^2 - 1) \deg(d) \leq (q^2 - 1) \deg a. \end{aligned}$$

Dans tous les cas, on obtient la majoration

$$\begin{aligned} \deg(h_\alpha(z)) &\leq (q^2 - 1)(\deg a + \deg d_0) + (q^2 - 1) \deg a_0 + C_\varepsilon |z|, \\ (36) \quad &\leq 2(q^2 - 1) \deg a + q(q + 1). \end{aligned}$$

En reportant dans (34), on obtient facilement la proposition. □

On utilise maintenant, comme L.C. Hsia, une méthode d'interpolation pour obtenir la majoration suivante de la hauteur du polynôme $\overline{\Phi}_a$.

Proposition 11. *Il existe une constante $c_0 > 0$ telle que pour tout $a \in A$ on ait*

$$H(\overline{\Phi}_a) \leq c_0(\psi(a) \deg a + 1).$$

On utilisera, pour montrer cette proposition le résultat qui suit (lemme 5.1 de [Hs]).

Lemme 9 [Hs]. *Soient $0 < \lambda_1 \leq \lambda_2$ deux nombres positifs de l'anneau des valuations de $\mathcal{C}$. Soit $P(X) \in \mathcal{C}[X]$ de degré D , il existe une constante $\kappa > 0$ ne dépendant que de λ_1 et de λ_2 telle que l'on a*

$$\left| m(P) - \log_q \sup_{\lambda_1 \leq |y| \leq \lambda_2} |P(y)| \right| \leq \kappa D.$$

On applique ce lemme aux coefficients de Φ_a qui sont des polynômes en j :

$$\Phi_a(X) = \sum_{i=0}^{\psi(a)} U_i(j) X^i.$$

On sait que pour tout z dans Ω tel que $|z| = |z|_i = q^{1-\varepsilon}$ où $0 < \varepsilon < 1$ on a

$$(37) \quad \deg(U_i(j(z))) \leq (2(q^2 - 1) \deg a + q(q + 1))\psi(a).$$

On fixe ε_1 et ε_2 réels vérifiant les inégalités $0 < \varepsilon_1 < \varepsilon_2 < 1$ et on pose $\lambda_1 = q^{q(q-(q-1)\varepsilon_2)}$ et $\lambda_2 = q^{q(q-(q-1)\varepsilon_1)}$. La fonction modulaire j fournit une bijection entre $GL_2(A) \setminus \Omega$ et $\mathcal{C}$, ainsi pour tout y dans $\mathcal{C}$ tel que $\lambda_1 \leq |y| \leq \lambda_2$, il existe $\eta \in \Omega$, vérifiant $y = j(\eta)$ et $|\eta| = |\eta|_i = q^{1-\varepsilon}$ avec $\varepsilon_1 < \varepsilon < \varepsilon_2$. Donc, on a

$$(38) \quad \log_q \sup_{\lambda_1 \leq |y| \leq \lambda_2} |U_i(y)| \leq (2(q^2 - 1) \deg a + q(q + 1))\psi(a).$$

Comme les U_i sont des polynômes de degrés inférieurs à $\psi(a)$, le lemme 9 donne de plus la majoration

$$(39) \quad \left| m(U_i) - \log_q \sup_{\lambda_1 \leq |y| \leq \lambda_2} |U_i(y)| \right| \leq \kappa \psi(a).$$

Les majorations (38) et (39) donnent alors clairement la proposition. $\square$

4 - Démonstration du théorème

4.1. Construction d'une fonction auxiliaire

On construit, pour tout entier naturel N , une fonction $F_N(t) = P_N(\overline{\Delta}(t), j(t))$, vérifiant

$$(40) \quad \begin{aligned} P_N(X_1, X_2) &\in A[X_1, X_2], \\ \deg_{X_i} P_N &\leq L_i - 1, \\ \text{ord}_0 F_N(t) &\geq N(q-1), \end{aligned}$$

où les entiers L_i seront déterminés ultérieurement en fonction de N .

Si on écrit P_N sous la forme $P_N = \sum_{\mathbf{i}} p_{\mathbf{i}} X_1^{i_1} X_2^{i_2}$, alors on a les développements

$$(41) \quad \begin{aligned} F_N(t) &= \sum_{\mathbf{i}} p_{\mathbf{i}} \left(\sum_{n_1 \geq 1} \delta_{n_1} t^{(q-1)n_1} \right)^{i_1} \left(\sum_{n_2 \geq -1} \gamma_{n_2} t^{(q-1)n_2} \right)^{i_2}, \\ &= \sum_{n \geq -L_2} f_n t^{n(q-1)}, \end{aligned}$$

où les coefficients δ_{n_1} et γ_{n_2} sont introduits en (12) et (13). On est donc amené à trouver des solutions dans A du système linéaire suivant.

$$(S) \quad f_n = 0, \quad n = -L_2, \dots, N-1.$$

Pour cela, on utilise le lemme de Siegel suivant (voir par exemple [ADR]).

Lemme 10. *Soient, pour $1 \leq i \leq m$ et $1 \leq j \leq n$, des éléments $a_{i,j}$ de A . On note M_0 un majorant de leurs degrés. Si $m < n$, alors il existe $x_1, \dots, x_n$ dans A non tous nuls tels que l'on ait*

$$\sum_{j=1}^n a_{i,j} x_j = 0 \quad 1 \leq i \leq m,$$

$$\deg x_j \leq \frac{m}{n-m} M_0 + 1 \quad 1 \leq j \leq n.$$

Il existe donc des solutions au système (S) dès que $N + L_2 < L = L_1 L_2$. De plus, les majorations données en (12) et en (13) sur les coefficients des développements des fonctions $\overline{\Delta}$ et j , impliquent que les degrés des coefficients de ce système ne sont pas plus grands que $N + L_2$. Le lemme de Siegel permet donc de choisir P_N dont la hauteur vérifie la majoration

$$(42) \quad H(P_N) \leq \frac{N + L_2}{L - N - L_2} (N + L_2) + 1.$$

4.2. Majoration du degré de $F_N(t)$

Soit $M(q-1)$ l'ordre d'annulation de $F_N(t)$ en zéro. Par construction de F_N , on a clairement $M \geq N$. Soit f_M le premier coefficient non nul dans le développement (41) en série entière de F_N . On pose $G_N(t) = \sum_{n \geq 0} f_{n+M} t^{n(q-1)}$, de sorte que l'on ait

$$(43) \quad F_N(t) = t^{M(q-1)} G_N(t).$$

Soit $\rho \in \mathbb{R}$, on majore le degré de $F_N(t)$ pour t de degré inférieur ou égal à ρ . Les inégalités de Cauchy dans le cadre non-archimédien donnent ici

$$(44) \quad \begin{aligned} \deg G_N(t) &\leq \sup_{n \geq 0} \{ \deg(f_{n+M}) + n(q-1)\rho \}, \\ &\leq \sup_{n \geq 0} \{ n + M + L_2 + n(q-1)\rho + H(P_N) \} \text{ on choisit } \rho = -\frac{1}{q-1}, \\ &\leq M + L_2 + H(P_N). \end{aligned}$$

On a donc montré la proposition suivante

Proposition 12. Pour tout $t \in \mathcal{C}$ vérifiant $\deg(t) \leq -\frac{1}{q-1}$, on a la majoration

$$\deg F_N(t) \leq M(q-1) \deg(t) + M + L_2 + H(P_N).$$

4.3. Construction d'un nombre algébrique non nul

On fixe désormais τ dans $\mathcal{C}$ tel que $\deg(\tau) \leq -\frac{1}{q-1}$, et on suppose que les nombres $\overline{\Delta}(\tau)$ et $j(\tau)$ sont algébriques sur k . Puisque les fonctions Δ et j sont algébriquement indépendantes sur $\mathcal{C}$ (lemme 1), la fonction F_N n'est pas identiquement nulle, et donc on peut trouver a dans A unitaire, de degré minimal tel que $F(\tau_a) \neq 0$, où $\tau_a = \frac{1}{C_a(1/\tau)}$. On pose :

$$(45) \quad W_N(t) = t^{-M(q-1)} F_N(t) \prod_{\substack{b \in A^+ \\ 1 \leq \deg b < \deg a}} \frac{\tau}{t - \tau_b}.$$

Il est montré dans [ADR] (lemme 13) que $|\tau_b| = |\tau|^{b|}$, ainsi on a les égalités suivantes.

$$\begin{aligned} |W_N(0)| &= |f_M| \prod_{\substack{b \in A^+ \\ 1 \leq \deg b < \deg a}} |\tau| |\tau_b|^{-1} = |f_M| |\tau|^{\frac{q \deg a - q}{q-1}} \prod_{\substack{b \in A^+ \\ 1 \leq \deg b < \deg a}} |\tau|^{-q \deg b}, \\ &= |f_M| |\tau|^{\frac{q \deg a - q}{q-1}} \prod_{1 \leq i < \deg a} |\tau|^{-q^{2i}} = |f_M| |\tau|^{\frac{-q^2 \deg a + q \deg a + 1 + q \deg a - q}{q^2 - 1}}. \end{aligned}$$

Or, comme $f_M \in A$, alors $|f_M| \geq 1$, et donc

$$(46) \quad |\tau|^{\frac{-q^{2 \deg a} + q^{\deg a+1} + q^{\deg a} - q}{q^2 - 1}} \leq |W_N(0)|.$$

D'autre part, d'après la majoration de $\deg F_N(t)$, on a

$$(47) \quad \begin{aligned} |W_N(0)| &\leq \sup \{|W_N(z)|, \text{ tel que } z \in \mathcal{C}, |z| = |\tau|\}, \\ &\leq q^{(M+L_2+H(P_N))}. \end{aligned}$$

Les deux inégalités (46) et (47) donnent alors la majoration

$$|\tau|^{\frac{-q^{2 \deg a} + q^{\deg a+1} + q^{\deg a} - q}{q^2 - 1}} \leq q^{(M+L_2+H(P_N))}.$$

Et donc, il existe une constante $c_1 > 0$ ne dépendant que de q et de τ , et vérifiant

$$(48) \quad |a|^2 = q^{2 \deg a} \leq c_1(M + H(P_N) + L_2).$$

4.4. Majoration de la hauteur de $\overline{\Delta}(\tau_a)$

Soit $x \in \overline{k}$, on note $P_{\min}(x)$ son polynôme minimal dans $A[X]$. On appelle mesure de Mahler de x celle de son polynôme minimal, et on a :

$$(49) \quad m(x) = [k(x) : k]h(x).$$

On reprend la démonstration du lemme 5 des Stéphanos [BS et al.], pour obtenir le résultat analogue suivant.

Lemme 11. *Soit $P \in A[X, Y]$ et $x, y \in \overline{k}$ tels que $P(x, y) = 0$. Si le polynôme $P(X, y)$ n'est pas constant alors on a la majoration*

$$m(x) \leq [k(y) : k]H(P) + m(y) \deg_Y P.$$

Preuve - On pose $d_y = [k(y) : k]$, on note a_0 le coefficient dominant du polynôme minimal de y dans $A[X]$, et $y_1 = y, y_2, \dots, y_{d_y}$ ses conjugués répétés avec multiplicité. Le degré en Y du polynôme P sera noté D . On considère le polynôme suivant.

$$Q(X) = a_0^D \prod_{j=1}^{d_y} P(X, y_j)$$

Par construction, ses coefficients sont des entiers algébriques, et sont des fonctions symétriques en les y_j . Par conséquent, ils sont dans A . Alors, puisque $Q(x) = 0$, le polynôme minimal de x divise Q dans $A[X]$. Par hypothèse, $Q(X, y)$ n'est pas constant ainsi Q n'est pas nul.

On a donc les majorations suivantes

$$\begin{aligned}
m(x) = H(P_{\min}(x)) &\leq H(Q) \leq D \deg a_0 + \sum_{j=1}^{d_y} H(P(X, y_j)), \\
&\leq D \deg a_0 + \sum_{j=1}^{d_y} \max_{|z|=1} \deg(P(z, y_j)), \\
&\leq D \deg a_0 + \sum_{j=1}^{d_y} (H(P) + D \max\{0, \deg y_j\}), \\
&\leq d_y H(P) + m(y) D,
\end{aligned}$$

d'où le lemme. $\square$

On utilise ce lemme avec $P = \overline{\Phi}_a$ et $y = j(\tau)$. Si l'on note $\alpha_a = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in \Delta_a^*(\Gamma)$, alors $\tau_a = t(\alpha_a(z))$. On choisit $x = a^{q^2-1} \frac{\Delta(\tau_a)}{\Delta(\tau)}$. On a alors clairement l'égalité $\overline{\Phi}_a(x, y) = 0$. On obtient la majoration

$$(50) \quad m \left(a^{q^2-1} \frac{\Delta(\tau_a)}{\Delta(\tau)} \right) \leq [k(j(\tau)) : k] H(\overline{\Phi}_a) + m(j(\tau)) \deg_Y \overline{\Phi}_a.$$

Or, on a montré précédemment (propositions 8 et 11) les majorations $\deg_Y \overline{\Phi}_a \leq \psi(a)$ et $H(\overline{\Phi}_a) \leq c_0(\psi(a) \deg a + 1)$. Alors, sachant que l'on a

$$\begin{aligned}
h(\overline{\Delta}(\tau_a)) &\leq h \left(a^{q^2-1} \frac{\Delta(\tau_a)}{\Delta(\tau)} \right) + h(\overline{\Delta}(\tau)) - (q^2 - 1) \deg a, \\
&\leq m \left(a^{q^2-1} \frac{\Delta(\tau_a)}{\Delta(\tau)} \right) + h(\overline{\Delta}(\tau)) - (q^2 - 1) \deg a,
\end{aligned}$$

et connaissant la majoration (20) de $\psi(a)$, on obtient facilement la proposition suivante.

Proposition 13. *Il existe une constante $c_2 > 0$ ne dépendant que de q et de τ , telle que pour tout a dans A on ait*

$$h(\overline{\Delta}(\tau_a)) \leq c_2(\psi(a) \deg a + 1).$$

4.5. Inégalité de Liouville

C'est dans cette partie que l'on aboutit à une contradiction, en appliquant le lemme de Liouville suivant, corollaire du lemme 4 de [M].

Lemme 12. *Soit P un polynôme en ν variables à coefficients dans A et $\lambda_1, \dots, \lambda_\nu$ des éléments de $\mathcal{C}$ contenus dans une extension de degré au plus D de k . Alors si $P(\lambda_1, \dots, \lambda_\nu)$ est non nul on a*

$$\deg P(\lambda_1, \dots, \lambda_\nu) \geq -D \left(\sum_{i=1}^{\nu} (\deg_{X_i} P) h(\lambda_i) + H(P) \right).$$

On applique ce lemme aux polynômes P_N , avec $\nu = 2$, $\lambda_1 = \overline{\Delta}(\tau_a)$ et $\lambda_2 = j(\tau_a)$. D'une part, la majoration ci-dessous est vue dans [ADR].

$$(51) \quad h(j(\tau_a)) \leq c_3 h(j(\tau)) + \log_q |a| + 1,$$

où $c_3 > 0$, comme toutes les constantes c_i qui apparaissent dans la suite, ne dépend que de q et de τ . D'autre part, la proposition 13 donne

$$(52) \quad h(\overline{\Delta}(\tau_a)) \leq c_2(\psi(a) \deg a + 1).$$

D'après la proposition 6, on peut trouver une constante $c_4 > 0$ pour laquelle on a la majoration

$$(53) \quad [\mathcal{M}_a : k] \leq c_4(|a| \log \log |a| + 1),$$

où $\mathcal{M}_a$ est l'extension de k engendrée par les nombres $j(\tau_a)$ et $\overline{\Delta}(\tau_a)$. Enfin, d'après la proposition 12, on a

$$\begin{aligned} \deg F_N(\tau_a) &\leq H(P_N) + M((q-1) \deg(\tau_a) + 1) + L_2, \\ &\leq H(P_N) + M((q-1)|a| \deg(\tau) + 1) + L_2. \end{aligned}$$

On choisit maintenant $L_1 = [N^{3/8}]$ et $L_2 = [N^{3/4}]$. On a bien

$$N + L_2 < L_1 L_2 = [N^{3/8}][N^{3/4}],$$

du moins, pour N suffisamment grand.

De plus, il existe une constante $c_5 > 0$ telle que l'on a l'inégalité $H(P_N) \leq c_5(N^{7/8} + 1)$. D'autre part, on a la majoration $|a|^2 \leq c_1(M + H(P_N) + L_2)$ donc on peut trouver $c_6 > 0$ vérifiant

$$|a|^2 \leq c_6 M.$$

Enfin, étant donnés les choix de L_1 et L_2 , et puisque $N \leq M$, il existe $c_7 > 0$ vérifiant la majoration

$$\deg F_N(\tau_a) \leq -c_7 M |a|.$$

En reportant dans l'inégalité de Liouville, on obtient l'existence de $c_8 > 0$ telle que

$$|a| M \leq c_8(|a| \log \log |a| + 1) \left(N^{3/8} \psi(a) \deg a + N^{3/4} \deg a + N^{7/8} + 1 \right).$$

Alors, sachant que $N \leq M$, que $|a|^2 \leq c_6 M$, et connaissant une majoration de $\psi(a)$ (voir (20)), on obtient le résultat suivant

$$(54) \quad \exists c_9 > 0, \quad M \leq c_9(\log \log M + 1) \left(M^{7/8} \log M \log \log M + M^{3/4} \log M + M^{7/8} + 1 \right).$$

On aboutit, pour N assez grand, à une contradiction. □

5 - Conséquence

L'analogue du théorème de Chudnovsky pour les modules de Drinfeld de rang 2, démontré par A. Thiery, donne sous certaines hypothèses la transcendance sur k du nombre $\frac{w_2}{\tilde{\pi}}$. Le théorème B donne aussi ce résultat. On considère un module de Drinfeld Υ de rang 2 défini sur $\bar{k}$ par l'égalité

$$\Upsilon_T(X) = TX + gX^q + \Delta X^{q^2}.$$

Son invariant modulaire $j(\Upsilon) = \frac{g^{q+1}}{\Delta}$ est donc algébrique sur k . On se donne une base (w_1, w_2) du réseau $\Lambda = \Lambda_\Upsilon$ associé à Υ . Le réseau $\Lambda' = A \oplus \frac{w_2}{w_1}A$ définit un module de Drinfeld Υ' vérifiant

$$\Upsilon'_T(X) = TX + w_1^{q-1}gX + w_1^{q^2-1}\Delta X^{q^2}.$$

Les deux modules Υ et Υ' étant isomorphes, ils ont même invariant modulaire, ainsi on a

$$j(\Upsilon) = j(\Upsilon') = \frac{g^{q+1}}{\Delta} \in \bar{k}.$$

Or, si l'on pose $z = \frac{w_2}{w_1} \in \mathcal{H}$, alors on a l'égalité

$$\Delta(z) = w_1^{q^2-1}\Delta = \tilde{\pi}^{q^2-1}\overline{\Delta}(t(z)) \quad \text{avec } \Delta(z) \in \bar{k}.$$

Le théorème démontré ici, dit alors que si $|t(z)| < q^{-\frac{1}{q-1}}$, alors $\overline{\Delta}(t(z)) \notin \bar{k}$. On obtient ainsi le corollaire suivant.

Corollaire. *Soit Υ un module de Drinfeld de rang 2 défini sur $\bar{k}$, et soit $\Lambda = w_1A \oplus w_2A$ son réseau associé. On a l'implication*

$$\deg \left(e_c \left(\tilde{\pi} \frac{w_2}{w_1} \right) \right) > \frac{1}{q-1} \quad \implies \quad \frac{w_1}{\tilde{\pi}} \notin \bar{k}.$$

Partie III : Problème de Lehmer et T -modules de dimension 2

1 - Introduction

1.1. Problème de Lehmer classique

On se donne α un nombre algébrique sur $\mathbb{Q}$, et l'on note $h(\alpha)$ sa hauteur de Weil logarithmique et absolue. On sait que $h(\alpha)$ est nul si et seulement si α est une racine de l'unité. Le problème de Lehmer consiste alors à donner la meilleure minoration possible de $h(\alpha)$ en fonction de $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, quand α n'est pas une racine de l'unité. Le résultat optimal espéré est le suivant.

Conjecture 1. *Il existe un nombre $c > 0$ tel que pour tout α dans $\mathbb{G}_m(\overline{\mathbb{Q}})$, qui n'est pas une racine de l'unité on ait*

$$h(\alpha) \geq \frac{c}{D},$$

où $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Des travaux ont déjà abouti dans ce sens ; la meilleure minoration connue à ce jour reste celle de E. Dobrowolski [Do] qui obtient le théorème suivant.

Théorème 1 [Do]. *Il existe une constante $c > 0$ telle que pour tout α dans $\mathbb{G}_m(\overline{\mathbb{Q}})$, de degré D sur $\mathbb{Q}$ qui n'est pas une racine de l'unité on ait*

$$h(\alpha) \geq \frac{c}{D} \left(\frac{\log \log(3D)}{\log(3D)} \right)^3.$$

Des analogues de ce résultat ont été démontrés, notamment pour les points de $\mathbb{G}_m^N(\overline{\mathbb{Q}})$ par F. Amoroso et S. David [AD] et pour les points algébriques de certaines variétés abéliennes définies sur un corps de nombres et admettant des multiplications complexes, par S. David et M. Hindry [DH]. Ici, on s'intéresse au même problème pour une famille de groupes algébriques appelés T -modules. On associe à ces objets une hauteur canonique (voir [De2]), qui est l'analogue de la hauteur de Néron-Tate pour les variétés abéliennes. On obtiendra une minoration de la hauteur canonique de points algébriques non de torsion, en fonction de leur degré. Mais avant d'énoncer ce résultat, on en définit le contexte.

1.2. T -modules

On rappelle dans ce paragraphe, quelques définitions déjà données dans l'introduction. On désigne par A l'anneau de polynômes $\mathbb{F}_q[T]$. Pour tous entiers $n > 0$ et $d \geq 0$, par T -module de dimension n , de degré d et défini sur une extension finie E de $k = \mathbb{F}_q(T)$, on entend la donnée d'un couple $(\mathbb{G}_a^n, \Phi)$, où Φ est un homomorphisme injectif d'anneaux

$$\Phi : \begin{cases} A & \longrightarrow & \text{End}_E(\mathbb{G}_a^n) \\ T & \longmapsto & \Phi_T = a_0 \mathcal{F}^0 + \cdots + a_d \mathcal{F}^d \end{cases}$$

où les a_i ($i = 0, \dots, d$) sont des matrices $n \times n$ à coefficients dans E avec $a_d \neq 0$, où T est la seule valeur propre de a_0 , et où $\mathcal{F}$ est l'endomorphisme de Frobenius sur $\mathbb{G}_a^n$:

$$\mathcal{F} : (x_1, \dots, x_n) \longmapsto (x_1^q, \dots, x_n^q).$$

Exemples :

- Un module de Drinfeld de rang r est un T -module de degré r et de dimension 1. En particulier, le module de Carlitz donné par

$$(1) \quad C : T \longmapsto T\mathcal{F}^0 + \mathcal{F}^1,$$

est un module de Drinfeld de rang 1 défini sur k .

- Etant donnés $\phi^{(1)}, \dots, \phi^{(n)}$ des modules de Drinfeld, leur T -module produit est défini par

$$(2) \quad \Phi : T \longmapsto \begin{pmatrix} \phi_T^{(1)} & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \phi_T^{(n)} \end{pmatrix}.$$

- Enfin, la puissance tensorielle de Carlitz $C^{\otimes n}$ est le T -module de dimension n suivant

$$(3) \quad C^{\otimes n} : T \longmapsto \begin{pmatrix} T & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & T \end{pmatrix} \mathcal{F}^0 + \begin{pmatrix} 0 & \dots & \dots & 0 \\ \vdots & & & \vdots \\ 0 & & & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix} \mathcal{F}^1.$$

Un morphisme $\Delta : (\mathbb{G}_a^n, \phi) \longrightarrow (\mathbb{G}_a^m, \psi)$ de T -modules est un morphisme algébrique vérifiant

$$\Delta \circ \phi(T) = \psi(T) \circ \Delta.$$

Une isogénie est un morphisme surjectif de T -modules dont le noyau est fini.

On rappelle que $H \subset \mathbb{G}_a^n$ est un sous- T -module de $(\mathbb{G}_a^n, \Phi)$ si c'est un sous-groupe algébrique connexe de $\mathbb{G}_a^n$, et s'il vérifie

$$(4) \quad \Phi_T(H) \subset H.$$

De la même façon, pour $b \in A = \mathbb{F}_q[T]$ non nul, on entendra par sous- b -module un sous-groupe algébrique connexe H vérifiant $\Phi_b(H) \subset H$. Un T -module est dit simple s'il ne possède pas de sous- T -module propre de dimension non nulle.

Si $(\mathbb{G}_a^n, \Phi)$ est un T -module défini sur E , et si b est un élément non nul de A , un point $\mathbf{x}_0 \in \mathbb{G}_a^n$ est dit de b -torsion si $\Phi_b(\mathbf{x}_0) = 0$. On dira de plus, qu'il est de b -torsion primitive, si pour tout v dans A , on a l'équivalence suivante.

$$(5) \quad \Phi_v(\mathbf{x}_0) = 0 \quad \Longleftrightarrow \quad b|v$$

On rappelle que l'on a noté, dans l'introduction, k_∞ le corps complété de k pour la valuation $1/T$ -adique, et $\mathcal{C}$ le complété de sa clôture algébrique $\bar{k}_\infty$. On désigne encore par $\bar{k}$ la clôture algébrique de k dans $\mathcal{C}$.

Soit $(\mathbb{G}_a^n, \Phi)$ un T -module de dimension n , défini sur une extension finie E de k . On sait (voir [An]) qu'il existe une unique fonction (dite exponentielle associée à Φ) $e_\Phi : \mathcal{C}^n \longrightarrow \mathcal{C}^n$ entière, $\mathbb{F}_q$ -linéaire et qui vérifie :

$$(6) \quad \begin{cases} e_\Phi(d\Phi_T(\mathbf{z})) = \Phi_T(e_\Phi(\mathbf{z})), \\ e'_\Phi(0, \dots, 0) = I_n, \end{cases}$$

où pour chaque $\mu \in A$, $d\Phi_\mu$ est la matrice coefficient devant $\mathcal{F}^0$ dans Φ_μ , et où I_n désigne la matrice identité de dimension n . Cette fonction est clairement un isomorphisme local de $\mathcal{C}^n$ dans $\mathcal{C}^n$.

Dans la suite, on considérera seulement les T -modules pour lesquels la fonction e_Φ est surjective sur $\mathcal{C}^n$.

1.3. Minoration de la hauteur canonique

On rappelle la définition de la hauteur de Weil usuelle. Si L est une extension finie de degré D sur k , la hauteur de $\mathbf{x} = (x_0, \dots, x_n) \in \mathbb{P}^n(L)$ est donnée par

$$h(\mathbf{x}) = \frac{1}{D} \sum_{w \in M_L} d_w \max_{i=0, \dots, n} (-w(x_i)),$$

où la somme est prise sur toutes les places w de L , et où d_w désigne le degré résiduel en la place w , normalisée par $w(L) = \mathbb{Z} \cup \{+\infty\}$. Soit $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{G}_a^n(\bar{k})$, alors la hauteur de Weil de $\mathbf{x}$ est définie comme étant la hauteur du point projectif $(1, x_1, \dots, x_n)$. Ici, on s'intéresse à la hauteur canonique $\hat{h}$ associée à un T -module, introduite par L. Denis dans [De2]. Cette hauteur est définie si la matrice dominante a_d de Φ_T est inversible. Elle est l'analogue de la hauteur de Néron-Tate sur une variété abélienne, utilisée par S. David et M. Hindry dans [DH]. On verra ultérieurement qu'elle vérifie de bonnes propriétés, notamment la suivante.

Pour tout $\mathbf{x}$ in $\mathbb{G}_a^n(\bar{k})$, $\hat{h}(\mathbf{x}) = 0$ si et seulement si $\mathbf{x}$ est un point de torsion du T -module, c'est-à-dire si et seulement si il existe $a \in A$ non nul tel que $\Phi_a(\mathbf{x}) = 0$.

Un analogue du théorème de Dobrowolski a déjà été obtenu pour les courbes elliptiques par M. Laurent [La] et par L. Denis [De2] pour le module de Carlitz à savoir le résultat suivant.

Théorème 2 [De2]. *Il existe un réel η effectivement calculable en fonction de q , tel que pour tout α appartenant à la clôture séparable de k , de degré $\leq \delta$ et non de torsion pour le module de Carlitz C on ait*

$$\hat{h}_C(\alpha) \geq \frac{\eta}{\delta} \left(\frac{\log \log(3\delta)}{\log(3\delta)} \right)^3,$$

où $\hat{h}_C$ est la hauteur associée au module de Carlitz.

Dans [De5], L. Denis donne également des énoncés semblables à la conjecture de Lehmer, mais dans des cas assez particuliers.

Théorème 3 [De5]. Soit $x \in \bar{k}_\infty$ possédant au moins un conjugué dans k_∞ . Si x n'est pas de torsion pour le module de Carlitz C et est de degré D sur k , alors on a la minoration

$$\hat{h}_C(x) \geq \frac{1}{qD},$$

où $\hat{h}_C$ est la hauteur associée au module de Carlitz.

Ce résultat est ensuite étendu à des modules de Drinfeld dont les coefficients vérifient certaines conditions, notamment celle d'être entiers. On pourra consulter les théorèmes 2 et 3 de [De5] pour des énoncés complets.

On peut adapter les méthodes de composition utilisées par L. Denis à la dimension supérieure ; cependant la minoration obtenue est plus mauvaise que celle que l'on démontre ici. En effet, les méthodes employées ne permettent pas d'avoir mieux qu'un D au dénominateur. En dimension supérieure, on peut espérer une minoration beaucoup plus fine, à l'image de celle obtenue par F. Amoroso et S. David dans [AD] (théorème 1.5).

Théorème 4 [AD]. Pour tout entier $N \geq 1$, il existe un réel $c(N) > 0$, et un entier $\kappa(N) \geq 1$ tels que pour tout élément $\alpha \in \mathbb{G}_m^N(\bar{\mathbb{Q}})$ de degré D sur $\mathbb{Q}$, dont les coordonnées sont multiplicativement indépendantes, on ait

$$h(\alpha) > \frac{c(N)}{D^{1/N}} \log(3D)^{-\kappa(N)}.$$

Ici, on obtient un résultat du même ordre, mais pour certains T -modules seulement. Par analogie avec le cas des variétés abéliennes, on voit que la conjecture suivante est la meilleure possible.

Conjecture 3. Soit $(\mathbb{G}_a^n, \Phi)$ un T -module, défini sur une extension E finie de k , et $\hat{h}$ sa hauteur canonique associée. Alors, il existe une constante $c = c(\Phi) > 0$ telle que pour tout $\alpha \in \mathbb{G}_a^n(\bar{E})$, de degré inférieur à D sur E , et qui n'est pas de torsion modulo tous les sous- b -modules de Φ ($b \in A$ non nul), on ait la minoration

$$\hat{h}(\alpha) > \frac{c}{D^{1/n}}.$$

En réalité, on peut espérer mieux en remplaçant dans la minoration $D^{1/n}$ par l'indice d'obstruction $\delta_E(\alpha)$ de α sur E défini au paragraphe 2.4.

Lorsque l'on essaie d'adapter les preuves de [AD] et de [DH] aux T -modules, plusieurs obstructions se présentent. La première tient à la structure même du T -module. En effet, dans le cadre des groupes multiplicatifs, ou des variétés abéliennes, les groupes sont par définition stables sous l'action de $\mathbb{Z}$. Ici, l'action de $A = \mathbb{F}_q[T]$ est beaucoup plus forte, et les groupes (en particulier les stabilisateurs de variétés) ne sont pas stables par cette action. On s'est donc limité, pour démontrer les lemmes de géométrie, à des T -modules vérifiant certaines hypothèses galoisiennes, que l'on explicite ci-dessous.

Les points de torsion primitive sont les analogues des racines primitives n -ièmes de l'unité pour $\mathbb{G}_m$. On sait que dans ce cas, elles sont conjuguées sur $\mathbb{Q}$, et que leur polynôme minimal est le n -ième polynôme cyclotomique. La première hypothèse impose simplement aux points de torsion primitive de $(\mathbb{G}_a^n, \Phi)$ d'avoir suffisamment de conjugués sur E .

(Gal 1) *Il existe une constante $C(\Phi) > 0$ telle que pour tout $b \in A$ non nul, tout point de b -torsion primitive possède au moins $|b|^{C(\Phi)}$ conjugués sur E .*

On rappelle encore le fait suivant : soient $n, p \in \mathbb{N}$ des entiers non nuls, si p est premier à n , alors l'application qui à $x \in \mathbb{G}_m$ associe le point x^p , permute les racines primitives n -ièmes de l'unité. La deuxième hypothèse est l'analogue de cette proposition pour les T -modules.

(Gal 2) *Soient b et v des éléments non nuls de A . Si v est premier à b , alors Φ_v permute les conjugués sur E de tout point de b -torsion primitive.*

Lors de la démonstration du lemme-clef de Dobrowolski (paragraphe 4), on a besoin de l'analogue du petit théorème de Fermat. Celui-ci est vérifié pour les variétés abéliennes, à condition qu'elles soient à multiplications complexes. Ici, on imposera de manière tout aussi naturelle, une condition supplémentaire au T -module Φ . Pour $\nu_0 \in A$ irréductible et unitaire, on note $(\mathcal{H}_{\nu_0})$ l'hypothèse suivante.

$$(\mathcal{H}_{\nu_0}) \quad \Phi_{\nu_0}(X_1, \dots, X_n) \equiv (X_1^{q^{d \deg \nu_0}}, \dots, X_n^{q^{d \deg \nu_0}}) \pmod{\nu_0}.$$

On remarquera que cette condition a un sens pour tous les éléments irréductibles et unitaires de A , sauf un nombre fini. En effet, il ne faut ici considérer que des polynômes $\nu_0 \in A$ qui sont premiers à un dénominateur fixé de Φ_T . On demandera à Φ , de vérifier l'hypothèse $(\mathcal{H}_{\nu_0})$ pour « beaucoup » de ν_0 , ce qui signifie encore que l'ensemble

$$(7) \quad H_m(\Phi) = \{\nu_0 \in A, \text{ irréductible, unitaire, } (\mathcal{H}_{\nu_0}) \text{ vérifiée, et } |\nu_0| \leq m\}$$

devra être suffisamment grand.

D'autre part, les sous- T -modules étant des analogues de sous-groupes algébriques, ils sont plus généraux que les variétés abéliennes. On aura donc besoin d'imposer l'hypothèse suivante.

(H) *Soit H un sous-groupe algébrique connexe de $\mathbb{G}_a^n(\bar{k})$ tel qu'il existe un élément $a \in A$ avec $\deg a > 0$, vérifiant $\Phi_a(H) \subset H$. Alors H est un sous- T -module de $(\mathbb{G}_a^n, \Phi)$.*

Enfin, une dernière obstruction est liée à la caractéristique positive et aux phénomènes d'inséparabilité. En effet, une grande différence avec la caractéristique 0, est que les composantes $\bar{k}$ -irréductibles $V_1, \dots, V_l$ d'une variété V définie sur k , peuvent être multiples. En d'autres termes, on n'a pas en général l'égalité

$$\deg_k(V) = \sum_{i=1}^l \deg(V_i).$$

C'est en partie pour cette raison que l'on se restreint à des T -modules de dimension 2 et définis sur le corps k .

Avec ces notations, on prouve le théorème suivant.

Théorème C. *Soit $(\mathbb{G}_a^2, \Phi)$ un T -module de degré d , défini sur k et pour lequel la matrice dominante a_d est inversible. On suppose que pour ce T -module, les hypothèses (H), (Gal 1) et (Gal 2) sont vérifiées et que :*

$$\exists t \geq 1, \quad \exists C > 0, \quad \forall m \in \mathbb{N}, \quad \text{card}(H_m(\Phi)) \geq C \frac{m^{1/t}}{\log m}.$$

Alors il existe une constante $\kappa_0 > 0$, telle que pour tout $\alpha \in \mathbb{G}_a^2(\bar{k})$ séparable de degré D sur k qui n'est pas de torsion modulo les sous- T -modules de Φ , on ait la minoration

$$\hat{h}(\alpha) \geq \kappa_0 \frac{1}{D^{1/2}} \left(\frac{(\log \log(3D))^V}{(\log(3D))^U} \right),$$

où $U = dt^4(42d + 17) + 3$ et $V = dt(21d + 8) + 2$.

Avant de commencer la preuve, on rappelle dans la partie qui suit quelques définitions et propositions concernant la séparabilité des extensions transcendentes, les variétés géométriquement réduites ainsi que l'indice d'obstruction d'un point algébrique. Le lecteur familier avec ces notions pourra débiter sa lecture au paragraphe 3. Dans ce dernier, on montre quelques résultats de géométrie. On remarquera que la non-stabilité des groupes par les morphismes Φ_a (où $a \in A \setminus \{0\}$), a rendu l'adaptation des preuves de [AD] et [DH] plus difficile.

La partie 4 est consacrée à la preuve du lemme-clef de Dobrowolski, et la cinquième à celle du lemme de zéros. Ensuite, à l'aide d'un lemme de Siegel, on construit une fonction auxiliaire dont on extrapole les zéros. La démonstration (paragraphe 7) est alors basée sur le choix de bons paramètres, de sorte que, si la hauteur canonique de α est supposée trop petite, les résultats précédents conduisent à une contradiction. Enfin, dans une dernière partie, on donnera quelques T -modules particuliers, auxquels s'appliquent le théorème C. Dans toute la suite, les constantes C_i pour $i \geq 1$, ne dépendront que du T -module $(\mathbb{G}_a^n, \Phi)$.

2 - Séparabilité

2.1. Généralités

2.1.1. Extensions algébriques séparables

Soit l un corps de caractéristique p non nulle. On se donne $\mathcal{L}$ un domaine universel de l , c'est-à-dire un corps algébriquement clos, contenant l et de degré de transcendance infini sur l . On note $\bar{l}$ la clôture algébrique de l dans $\mathcal{L}$. Un élément $x \in \bar{l}$ est dit *séparable* si son polynôme minimal sur l l'est, c'est-à-dire s'il n'a que des racines simples dans $\bar{l}$. Une extension algébrique L de l est dite séparable si tous ses éléments le sont. Si de plus une telle extension est finie, on sait que son degré est égal au nombre de l -morphisms injectifs du corps L dans $\bar{l}$.

Pour étendre cette notion de séparabilité à des extensions transcendentes, on a recours à quelques définitions.

2.1.2. Disjonction linéaire et indépendance algébrique

Dans la suite, toutes les extensions de l seront telles que le domaine universel $\mathcal{L}$ garde sur elles un degré de transcendance infini. Soient $l \hookrightarrow L$ et $l \hookrightarrow K$ deux extensions de corps. On dira que L et K sont *linéairement disjointes* sur l si toute famille d'éléments de L , libre sur l , le reste sur K . On peut voir qu'en fait cette définition est symétrique en L et en K . On a de plus la proposition suivante ([L2] proposition 1 chapitre III).

Proposition 1 [L2]. *Si $l \hookrightarrow L$ et $l \hookrightarrow F \hookrightarrow K$ sont des extensions, alors L et K sont linéairement disjointes sur l si et seulement si L et F sont linéairement disjointes sur l , et K et FL sont linéairement disjointes sur F .*

Soient $l \hookrightarrow L$ et $l \hookrightarrow K$ deux extensions de corps. On dira que L et K sont *algébriquement indépendantes* sur l si toute famille finie d'éléments de L , algébriquement indépendante sur l , le reste sur K . Comme précédemment, cette définition est symétrique en L et K . Si L et K sont linéairement disjointes sur l alors elles sont algébriquement indépendantes sur l , mais la réciproque est clairement fausse. Avec ces définitions, on a la caractérisation suivante des extensions algébriques séparables : une extension algébrique $l \hookrightarrow L$ est séparable si et seulement si L et $l^{1/p}$ sont linéairement disjointes sur l . C'est à partir de cette équivalence que l'on étend la notion de séparabilité à des extensions transcendentes.

2.1.3. Extensions séparables : cas général

Soit L une extension de type fini de l . On dit que L est *séparablement engendrée* sur l si l'on peut trouver une base de transcendance $(t) = (t_1, \dots, t_r)$ telle que L est séparable sur $l(t)$. Une telle base est appelée base de transcendance séparante de L sur l . On note $l^{1/p^\infty} = \varprojlim_m l^{1/p^m}$ le compositum de tous les l^{1/p^m} . On a alors le résultat suivant (voir [L2] théorème 1 chapitre III).

Proposition 2 [L2]. *Si $l \hookrightarrow L$ est une extension, alors les conditions suivantes sont équivalentes :*

- (1) L et l^{1/p^∞} sont linéairement disjointes sur l ,
- (2) il existe un entier m tel que L et l^{1/p^m} sont linéairement disjointes sur l ,
- (3) tout corps intermédiaire, qui est de type fini sur l , est séparablement engendré sur l .

Une telle extension est dite *séparable*. On donne alors quelques corollaires tirés de [L2], classiquement connus pour les extensions algébriques séparables.

Corollaires.

- (1) Si $l \hookrightarrow L$ est séparable, alors toute extension intermédiaire est séparable sur l .
- (2) Si $l \hookrightarrow L$ et $L \hookrightarrow K$ sont séparables, alors $l \hookrightarrow K$ est séparable.
- (3) Si $l \hookrightarrow L$ est séparable et si L et K sont algébriquement indépendantes sur l , alors LK est séparable sur K .

2.2. Variétés algébriques

2.2.1. Points génériques et spécialisations

Soit $n \in \mathbb{N}$ un entier non nul. Un ensemble algébrique défini sur un corps l est appelé *l -variété* s'il est irréductible sur l . Un ensemble algébrique défini sur l est une l -variété si son idéal associé dans $l[\mathbf{X}] = l[X_1, \dots, X_n]$ est premier. Tout ensemble algébrique Z défini sur l s'écrit comme union finie de l -variétés $Z = V_1 \cup \dots \cup V_r$; cette décomposition est unique, à l'ordre près, si l'on impose $V_i \not\subseteq V_j$ quand $i \neq j$. On appelle $V_1, \dots, V_r$ les l -composantes de Z .

Soit $\mathcal{P}$ un idéal premier de $l[\mathbf{X}]$. L'homomorphisme $l[\mathbf{X}] \longrightarrow l[\mathbf{X}]/\mathcal{P}$ induit un isomorphisme sur l . On identifiera l à son image, ainsi quitte à recomposer par l'isomorphisme inverse, on peut supposer que l'homomorphisme précédent fixe le corps l . Pour $i = 1, \dots, n$ on note ζ_i l'image de X_i par cet homomorphisme.

$$l[\mathbf{X}]/\mathcal{P} \simeq l[\zeta_1, \dots, \zeta_n]$$

On a de plus le lemme suivant (voir par exemple [L2] lemme, paragraphe 3 chapitre II).

Lemme 1 [L2]. *On se donne $l(\zeta_1, \dots, \zeta_n)$ une extension de type fini de l . Alors, il existe un monomorphisme $l(\zeta_1, \dots, \zeta_n) \longrightarrow \mathcal{L}$, qui est l'identité sur l .*

Ainsi, il existe $(\mathbf{x}) = (x_1, \dots, x_n) \in \mathcal{L}^n$ tel que

$$l(\zeta_1, \dots, \zeta_n) \simeq l(\mathbf{x}).$$

Alors, $l[\mathbf{x}]$ est isomorphe à $l[\mathbf{X}]/\mathcal{P}$, et si $f(\mathbf{X}) \in l[\mathbf{X}]$ on a l'équivalence suivante

$$f(\mathbf{X}) \in \mathcal{P} \iff f(\mathbf{x}) = 0.$$

On dira que $(\mathbf{x})$ est un *zéro générique* de $\mathcal{P}$. Les autres zéros génériques de $\mathcal{P}$ sont les $(\mathbf{x}')$ pour lesquels il existe un isomorphisme $l[\mathbf{x}] \longrightarrow l[\mathbf{x}']$ fixant l . Un idéal premier $\mathcal{P} \in l[\mathbf{X}]$ détermine donc une classe d'équivalence (sur l) formée des points $(\mathbf{x})$ de $\mathcal{L}^n$ tels que $\mathcal{P}$ est le noyau de l'application $l[\mathbf{X}] \longrightarrow l[\mathbf{x}]$. Inversement, à chaque $(\mathbf{x})$ de $\mathcal{L}^n$, on associe l'idéal $\mathcal{P} = \{f(\mathbf{X}) \in l[\mathbf{X}], f(\mathbf{x}) = 0\}$. Il est premier, et $(\mathbf{x})$ en est clairement un zéro générique. Soit V une l -variété, et $\mathcal{P}$ son idéal premier associé. On appelle *point générique* de V tout zéro générique de $\mathcal{P}$. Inversement, si $(\mathbf{x})$ est un point de $\mathcal{L}^n$, et si $\mathcal{P}$ est son idéal associé, la l -variété associée à $\mathcal{P}$ est appelée *lieu de $(\mathbf{x})$* .

On a donc une correspondance naturelle entre :

- (1) les idéaux premiers,
- (2) les variétés,
- (3) les classes d'équivalence de points génériques.

Soit maintenant $(\mathbf{x}') \in \mathcal{L}^n$ un autre point, et $\mathcal{P}'$ son idéal associé dans $l[\mathbf{X}]$. Si $\mathcal{P}'$ contient l'idéal $\mathcal{P}$, c'est-à-dire si tout polynôme à coefficients dans l qui s'annule en $(\mathbf{x})$ s'annule aussi en $(\mathbf{x}')$, on dit que $(\mathbf{x}')$ est une *spécialisation de $(\mathbf{x})$ sur l* . Dans ce cas, on peut définir un homomorphisme $l[\mathbf{x}] \longrightarrow l[\mathbf{x}']$. Inversement, un tel homomorphisme fournit clairement une spécialisation de $(\mathbf{x})$. Enfin, si V est le lieu de $(\mathbf{x})$, alors $(\mathbf{x}')$ est une spécialisation de $(\mathbf{x})$ sur l si et seulement si $\mathbf{x}' \in V$.

2.2.2. Corps de définition

Soit L un corps, et $\mathcal{I} \in L[\mathbf{X}]$ un idéal. On dira que $\mathcal{I}$ est défini sur un corps l , si $\mathcal{I}$ a une base dont les polynômes sont à coefficients dans l . Soit $f(\mathbf{X}) \in \mathcal{I}$, on l'écrit comme combinaison linéaire de monômes en $\mathbf{X}$:

$$f(\mathbf{X}) = \sum_{\lambda} a_{\lambda} M_{\lambda}(\mathbf{X}).$$

Si $\sigma : L \longrightarrow L$ est un automorphisme, on définit

$$f^{\sigma}(\mathbf{X}) = \sum_{\lambda} \sigma(a_{\lambda}) M_{\lambda}(\mathbf{X}),$$

et $\mathcal{I}^{\sigma}$ l'idéal formé des f^{σ} quand f parcourt $\mathcal{I}$. On a alors le résultat suivant.

Proposition 3 [L2]. *Soit $l \hookrightarrow L$ une extension et $\mathcal{I}$ un idéal de $L[\mathbf{X}]$. Alors, il existe un corps de définition minimal de $\mathcal{I}$ contenant l , i.e. un corps $l_0 \subset L$ contenant l et tel que*

- (1) $\mathcal{I}$ est défini sur l_0 ,
- (2) si $\mathcal{I}$ est défini sur l_1 , et si $l \subset l_1$ alors $l_0 \subset l_1$.

De plus, si $\sigma : L \longrightarrow L$ est un automorphisme :

$$\mathcal{I}^{\sigma} = \mathcal{I} \iff l_0 \text{ est fixé par } \sigma.$$

La preuve sans l'hypothèse « contenant l » (théorème 7 chapitre III [L2]) est due à A. Weil. Elle s'adapte très bien ici. On donne simplement la construction du corps l_0 , qui sera utile par la suite.

On considère le L -espace vectoriel $L[\mathbf{X}]/\mathcal{I}$, dont l'ensemble des monômes $\{M(\mathbf{X})\}$ forme une famille génératrice. On en extrait une base $B = \{M_{\beta}(\mathbf{X})\}$. Alors, pour tout monôme $M(\mathbf{X})$ il existe une écriture unique

$$M(\mathbf{X}) \equiv \sum_{\beta} b_{M,\beta} M_{\beta}(\mathbf{X}) \pmod{\mathcal{I}},$$

où les $b_{M,\beta}$ sont dans L . On pose alors, $l_0 = l(b_{M,\beta})_{M,\beta}$. D'autre part, comme $L[\mathbf{X}]$ est noethérien, l_0 est inclus dans une extension de type fini de l , donc est aussi de type fini sur l .

On relèvera cependant quelque subtilité à cette notion de corps de définition : ce n'est pas parce qu'une $\bar{l}$ -variété est l'ensemble des zéros d'un idéal défini sur L , que cette variété est elle-même définie sur L , même si l'idéal restreint à $L[\mathbf{X}]$ est premier (c'est vrai si cet idéal est premier dans $\bar{l}[\mathbf{X}]$). En effet, par exemple si $l = k = \mathbb{F}_q(T)$, et $V = \{T^{1/p}\}$, alors V est l'ensemble des zéros du polynôme irréductible $X^p - T \in k[X]$ mais n'est pas définie sur k .

On donne maintenant une caractérisation du corps de définition. Ici, $\mathcal{P} \subset L[\mathbf{X}]$ est un idéal premier, dont on choisit un zéro générique $(\mathbf{x})$. Alors, la famille $\{M_{\beta}(\mathbf{x})\}$ forme une base de $L[\mathbf{x}]$ sur L , mais n'engendre pas nécessairement $l[\mathbf{x}]$ sur l . On a cependant le résultat suivant ([L2] théorème 8 chapitre III).

Proposition 4 [L2]. *Soit $K \hookrightarrow L$ une extension et $(\mathbf{x})$ un point de $\mathcal{L}^n$. Soit $\mathcal{P}$ l'idéal déterminé par $(\mathbf{x})$ dans $L[\mathbf{X}]$. Alors, $\mathcal{P}$ est défini sur K si et seulement si $K(\mathbf{x})$ et L sont linéairement disjoints sur K .*

On s'intéresse maintenant à ce qu'il advient d'un idéal après extension séparable. On cite pour cela un extrait de la proposition 8 du chapitre III de [L2].

Proposition 5 [L2]. *Soit $\mathcal{P} \subset l[\mathbf{X}]$ un idéal et $(\mathbf{x})$ un zéro générique. Soit L une extension de l . Si $l \hookrightarrow l(\mathbf{x})$ ou si $l \hookrightarrow L$ est séparable, alors l'idéal $\mathcal{P}.L[\mathbf{X}]$ est l'intersection des idéaux premiers de $L[\mathbf{X}]$ s'annulant sur l'ensemble algébrique déterminé par $\mathcal{P}.L[\mathbf{X}]$.*

Ceci implique en particulier, que dans ce cas, l'idéal $\mathcal{P}.L[\mathbf{X}]$ est égal à son radical.

2.3. Variétés géométriquement réduites (G.R.)

2.3.1. Variétés conjuguées

Soit $l \hookrightarrow L$ une extension et $\sigma : L \longrightarrow L^\sigma$ un isomorphisme. Si $f(\mathbf{X}) \in L[\mathbf{X}]$, on peut définir $f^\sigma(\mathbf{X}) \in L^\sigma[\mathbf{X}]$, ainsi que $\mathcal{I}^\sigma \subset L^\sigma[\mathbf{X}]$ si $\mathcal{I}$ est un idéal de $L[\mathbf{X}]$. Soit $\mathcal{I}$ l'idéal d'un ensemble algébrique Z , alors $\mathcal{I}^\sigma$ est l'idéal d'un autre ensemble algébrique que l'on note Z^σ . De plus, si $\mathcal{P} \subset L[\mathbf{X}]$ est premier, il en est de même pour $\mathcal{P}^\sigma \subset L^\sigma[\mathbf{X}]$. Ainsi, si V est une L -variété, alors V^σ est une L^σ -variété. Soit $(\mathbf{x})$ un point générique de V . Si on peut étendre σ à $L(\mathbf{x})$, (ce qui est le cas lorsque L est de type fini sur un corps l fixé par σ) on note $(\mathbf{x}^\sigma) = (x_1^\sigma, \dots, x_n^\sigma)$. C'est un point générique de V^σ sur L^σ . A chaque automorphisme σ de $\text{Aut}(\mathcal{L})$, on associe ainsi des variétés conjuguées à V . On a de plus ([L2] théorème 9 chapitre III) la proposition suivante.

Proposition 6 [L2]. *Soit V une $\bar{l}$ -variété, et l_0 son plus petit corps de définition contenant l . Pour tout $\sigma \in \text{Aut}(\mathcal{L})$ fixant l on a*

$$V = V^\sigma \iff l_0 \text{ est fixé à gauche par } \sigma.$$

Ainsi, V^σ est entièrement déterminée par l'action de σ sur l_0 qui est une extension finie de l .

Soit V une l -variété, alors elle se décompose en un nombre fini de $\bar{l}$ -variétés qui sont conjuguées entre elles. Par exemple, si $(\mathbf{x})$ est un point algébrique sur l , ses conjugués sont les $(\mathbf{x}^\sigma)$ où σ est un l -isomorphisme de $l(\mathbf{x})$. Soit N le degré de $l(\mathbf{x})$ sur l . Alors, $(\mathbf{x})$ a au plus N conjugués distincts, et il en a exactement N si et seulement si $l \hookrightarrow l(\mathbf{x})$ est séparable. On veut étendre ce résultat pour des variétés de dimensions supérieures. Pour cela on énonce le résultat suivant ([L2] théorème 10 chapitre III).

Proposition 7. *Soit V une $\bar{l}$ -variété, et l_0 son plus petit corps de définition contenant l . Alors le nombre de $\bar{l}$ -variétés conjuguées sur l de V et distinctes, est égal au degré de séparabilité $[l_0 : l]_s$.*

Preuve - Soit L une extension normale de l contenant l_0 . D'après la proposition précédente, un élément σ de $\text{Aut}(L/l)$ fixe V si et seulement si le corps l_0 est fixé par σ . Soit $\text{Aut}(L/l_0)$ le groupe des automorphismes de L fixant le corps l_0 . Son indice dans $\text{Aut}(L/l)$ est le nombre de variétés l -conjuguées, mais c'est aussi $[l_0 : l]_s$. $\square$

2.3.2. Extensions régulières

Soit $(\mathbf{x})$ un point de $\mathcal{L}^n$, et V_0 la variété qu'il définit sur $\bar{l}$. Le but de ce paragraphe est de comparer son corps de définition minimal F contenant l , et le corps $G = l(\mathbf{x}) \cap \bar{l}$. On aura besoin pour cela de la définition suivante ([L2] théorème 2 chapitre III).

Soit $l \hookrightarrow L$ une extension. On dira que L est une *extension régulière* de l , si l'une des conditions équivalentes suivantes est réalisée :

- $l \hookrightarrow L$ est séparable et l est algébriquement fermé dans L (i.e. $L \cap \bar{l} = l$),
- L et $\bar{l}$ sont linéairement disjoints sur l .

Par exemple, si V_0 est une $\bar{l}$ -variété définie sur $L \supset l$, et si l'on choisit un point générique $(\mathbf{x})$, alors $L(\mathbf{x})$ est régulière sur L . D'autre part, en utilisant cette équivalence, on peut montrer la proposition suivante.

Proposition 8. *Soit $(\mathbf{x})$ un point de $\mathcal{L}^n$, et V_0 la variété qu'il détermine sur $\bar{l}$. On note F son corps de définition minimal contenant l , et G le corps $l(\mathbf{x}) \cap \bar{l}$. Alors on a toujours*

$$G \subset F.$$

Si de plus $l(\mathbf{x})$ est séparable sur l , alors $G = F$.

Preuve - Comme F est un corps de définition de V_0 , les extensions $F(\mathbf{x})$ et $\bar{l} = \bar{F}$ sont linéairement disjoints sur F . Ainsi, F est algébriquement fermé dans $F(\mathbf{x})$, par conséquent on a l'inclusion

$$G = l(\mathbf{x}) \cap \bar{l} \subset F(\mathbf{x}) \cap \bar{l} = F.$$

On suppose maintenant que $l(\mathbf{x})$ est séparable sur l . Comme $G \subset \bar{l}$, d'après le point (3) du corollaire de la proposition 2, l'extension $G \hookrightarrow G(\mathbf{x})$ est aussi séparable. Or, par construction, G est algébriquement fermé dans $G(\mathbf{x})$, d'après l'équivalence précédente $\bar{G} = \bar{l}$ et $G(\mathbf{x})$ sont linéairement disjoints sur G . Par conséquent, G est un corps de définition de V_0 . La proposition 3 affirme alors qu'il contient le corps F . $\square$

2.3.3. Variétés géométriquement réduites (G.R.)

On se donne un corps l , une l -variété V et $(\mathbf{x}) \in \mathcal{L}^n$ un point générique. Soit V_1 la $\bar{l}$ -variété déterminée par ce point, et F son corps minimal de définition contenant l . Alors, avec ces notations, on a le résultat suivant ([W] chapitre I proposition 23).

Proposition 9. *L'extension $l \hookrightarrow l(\mathbf{x})$ est séparable si et seulement si $l \hookrightarrow F$ l'est aussi.*

Preuve - On suppose tout d'abord que l'extension $l \hookrightarrow F$ est séparable. D'après la proposition 4, $\bar{l}$ et $F(\mathbf{x})$ sont linéairement disjoints sur F , donc $F \hookrightarrow F(\mathbf{x})$ est séparable. Alors, il en est de même pour $l \hookrightarrow F(\mathbf{x})$; a fortiori, l'extension $l \hookrightarrow l(\mathbf{x})$ est séparable. Réciproquement, on suppose maintenant que l'extension $l \hookrightarrow l(\mathbf{x})$ est séparable. Soit $l_s \supset l$ la sous-extension maximale de F qui est séparable sur l . Comme l_s est une extension algébrique de l , les extensions l_s et $l(\mathbf{x})$ sont algébriquement indépendantes sur l . Ainsi,

$l_s \hookrightarrow l_s(\mathbf{x})$ est aussi séparable.

Soit $M_0(\mathbf{x})$ un monôme, que l'on décompose dans la base $\{M_\beta(\mathbf{x})\}$:

$$(8) \quad M_0(\mathbf{x}) = b_1 M_1(\mathbf{x}) + \cdots + b_r M_r(\mathbf{x}).$$

Si F n'est pas séparable sur l , alors on peut trouver une telle relation, où les b_i ne sont pas tous dans l_s . Par unicité de l'écriture de $M_0(\mathbf{x})$ dans la base $\{M_\beta(\mathbf{x})\}$, les monômes $M_0(\mathbf{x}), \dots, M_r(\mathbf{x})$ sont linéairement indépendants sur l_s . Puisque $l_s \hookrightarrow l_s(\mathbf{x})$ est séparable, les extensions $l_s(\mathbf{x})$ et l_s^{1/p^∞} sont linéairement disjointes sur l_s , et donc les monômes $M_0(\mathbf{x}), \dots, M_r(\mathbf{x})$ sont linéairement indépendants sur l_s^{1/p^∞} . Or les b_i sont dans l_s^{1/p^∞} . La relation (8) donne donc une contradiction, et $l \hookrightarrow F$ est séparable.

On donne une deuxième preuve de cette implication. On suppose que $l \hookrightarrow l(\mathbf{x})$ est séparable. Comme précédemment, on note $G = l(\mathbf{x}) \cap \bar{l}$. La proposition 8 donne l'égalité $G = F \subset l(\mathbf{x})$. Ainsi, F est bien séparable sur l . $\square$

On dira dans ce cas que V_1 est une variété géométriquement réduite (G.R.) sur l .

Corollaire. Soit $V_1, \dots, V_r$ les $\bar{l}$ -composantes d'une l -variété V . Si V_1 est G.R. sur l , alors pour tout i , V_i l'est aussi.

Exemples :

- Si Z est un ensemble algébrique défini sur l et de dimension 0, alors les $\bar{l}$ -composantes de Z sont G.R. sur l si et seulement si les coordonnées de ces points sont séparables sur l .
- Soit $P \in \bar{l}[\mathbf{X}]$ irréductible, dont l'un des coefficients vaut 1. Alors la $\bar{l}$ -variété déterminée par P est G.R. si et seulement si ses coefficients sont séparables sur l .
- Pour qu'une $\bar{l}$ -variété soit G.R. sur l , il suffit qu'elle ait au moins un corps de définition séparable sur l .

Applications :

- Soit V une l -variété dont toutes les $\bar{l}$ -composantes $V_1, \dots, V_r$ sont G.R. sur l . On note $\mathcal{P}$ son idéal de définition dans $l[\mathbf{X}]$. On note $\mathcal{P}_1, \dots, \mathcal{P}_r$ les idéaux de définition des composantes irréductibles de V dans $\bar{l}[\mathbf{X}]$. Alors, d'après la proposition 5, on a l'égalité

$$(9) \quad \mathcal{P}.\bar{l}[\mathbf{X}] = \bigcap_{i=1}^r \mathcal{P}_i.$$

- Soit V_1 une $\bar{l}$ -variété et F son corps de définition minimal contenant l . Alors V_1 possède au plus $[F : l]$ $\bar{l}$ -variétés conjuguées, et elle en a exactement $[F : l]$ si et seulement si elle est G.R. sur l .

2.4. Indice d'obstruction

Soit V_0 une l -variété, et V_1 une de ses $\bar{l}$ -composantes. On note l_1 le plus petit corps de définition de V_1 contenant l . La notion de degré sur l de V_0 est bien définie par la fonction de Hilbert. Ici V_1 peut posséder moins de conjuguées que le degré $[l_1 : l]$, on est donc amené à tenir compte des multiplicités éventuelles. Soit $[l_1 : l] = [l_1 : l]_s [l_1 : l]_i = r.[l_1 : l]_i$. Alors, V_0 a exactement r variétés l -conjuguées que l'on note $V_1, \dots, V_r$. Soient $\mathcal{P}_1, \dots, \mathcal{P}_r$

les idéaux de $\bar{l}[\mathbf{X}]$ définis par $V_1, \dots, V_r$ respectivement, et $\mathcal{P}_0$ l'idéal de V_0 dans $l[\mathbf{X}]$. On a alors l'égalité

$$\mathcal{P}_0 \bar{l}[\mathbf{X}] = \bigcap_{i=1, \dots, r} \mathcal{Q}_i,$$

où chaque $\mathcal{Q}_i$ est $\mathcal{P}_i$ -primaire. Comme les $\mathcal{Q}_i$ sont permutés transitivement par les isomorphismes de $\bar{l}$ fixant l , ils sont tous de même longueur notée $L(V_0)$. Le lemme 3.2 de [P1] donne ici l'égalité

$$(10) \quad \begin{aligned} \deg_l(V_0) &= L(V_0)(\deg V_1 + \dots + \deg V_r), \\ &= rL(V_0) \deg V_1. \end{aligned}$$

En particulier, si V_1 est G.R. alors $L(V_0) = 1$ et $r = [l_1 : l]$, on a donc

$$(11) \quad \deg_l(V_0) = [l_1 : l] \deg(V_1) = \deg \left(\bigcup_{\sigma \in \text{Aut}(\bar{l}/l)} \sigma(V_1) \right).$$

On peut maintenant définir la notion d'indice d'obstruction $\delta_E(\alpha)$ d'un élément α de $\mathbb{G}_a^n(\bar{E})$, où E est une extension finie de $k = \mathbb{F}_q(T)$.

$$(12) \quad \delta_E(\alpha) = \min \{ \deg_E(V)^{1/\text{codim} V}, V \text{ est une } E\text{-variété passant par } \alpha \}$$

Dans le cas où la dimension n est égale à 1, cette définition coïncide avec celle de degré de α sur E . On dispose également de l'encadrement suivant.

$$1 \leq \delta_E(\alpha) \leq [E(\alpha) : E]^{1/n}.$$

Il suffit, pour le voir, de considérer la E -variété de dimension 0, formée des conjugués de α . Il semble alors naturel de se poser la question suivante.

Question. *Soit α un point de $\mathbb{G}_a^n(\bar{E})$, séparable sur E . Existe-t-il une E -variété V_0 dont les $\bar{E}$ -composantes sont G.R. sur E , et telle que*

$$\deg_E(V_0) = \delta_E(\alpha)^{\text{codim} V_0} ?$$

On sait néanmoins y répondre partiellement via la proposition suivante.

Proposition 10. *Soit E une extension finie de k et α un point de $\mathbb{G}_a^n(\bar{E})$, séparable sur E . Alors les $\bar{E}$ -composantes de toute hypersurface E -irréductible passant par α et de degré minimal, sont géométriquement réduites sur E .*

Preuve - Soit V une hypersurface E -irréductible passant par α et de degré minimal. On note $P(X_1, \dots, X_n) \in E[\mathbf{X}]$ un polynôme la définissant. On suppose que les composantes de V ne sont pas G.R. sur E . Soit $(\mathbf{x})$ un point générique de V , l'extension $E \hookrightarrow E(\mathbf{x})$ n'est alors pas séparable. D'après le théorème 2 (chapitre I) de [W], on a

$$\forall j \in \{1, \dots, n\}, \quad \frac{\partial P}{\partial X_j}(\mathbf{x}) = 0.$$

Par conséquent, le polynôme $\frac{\partial P}{\partial X_j}$ est un élément de l'idéal de V , qui n'est autre que l'idéal engendré par P . Comme il est de degré strictement plus petit que celui de P , nécessairement, le polynôme $\frac{\partial P}{\partial X_j}$ est identiquement nul, et ceci quelque soit l'indice $j \in \{1, \dots, n\}$. Ainsi, il existe un polynôme $Q(\mathbf{X}) \in E[\mathbf{X}]$ tel que

$$P(X_1, \dots, X_n) = Q(X_1^p, \dots, X_n^p).$$

Soit $(\theta_1, \dots, \theta_l)$ une base minimale de E sur E^p . En développant les coefficients de P dans cette base et en regroupant les puissance p -ièmes, on peut écrire

$$P(\mathbf{X}) = \sum_{\substack{j=1, \dots, l \\ \mathbf{i}=(i_1, \dots, i_l) \\ 0 \leq i_j \leq p-1}} Q_{\mathbf{i}}(\mathbf{X})^p \theta_1^{i_1} \dots \theta_l^{i_l},$$

où les $Q_{\mathbf{i}}(\mathbf{X})$ sont des éléments de $E[\mathbf{X}]$. On spécialise cette égalité en $\mathbf{X} = \alpha$, et on en prend la puissance $1/p$. On obtient la relation suivante.

$$0 = \sum_{\substack{j=1, \dots, l \\ \mathbf{i}=(i_1, \dots, i_l) \\ 0 \leq i_j \leq p-1}} Q_{\mathbf{i}}(\alpha) \left(\theta_1^{1/p}\right)^{i_1} \dots \left(\theta_l^{1/p}\right)^{i_l}.$$

Comme P est de degré minimal et comme les $Q_{\mathbf{i}}(\mathbf{X})$ sont de degrés strictement plus petits que celui de P , cette relation est non triviale. Ainsi, la famille

$$\left\{ \left(\theta_1^{1/p}\right)^{i_1} \dots \left(\theta_l^{1/p}\right)^{i_l}, 0 \leq i_j \leq p-1 \text{ pour } j = 1, \dots, l \right\}$$

est liée sur $E(\alpha)$. Puisque α est séparable sur E , les extensions $E(\alpha)$ et $E^{1/p}$ sont linéairement disjointes sur E . Par conséquent, cette famille est aussi liée sur E . Il existe donc un polynôme non nul $H(X_1, \dots, X_l) \in E[X_1, \dots, X_l]$ de degré en chaque variable inférieur à $p-1$ vérifiant $H(\theta_1^{1/p}, \dots, \theta_l^{1/p}) = 0$. Quitte à échanger les indices, cela implique que $\theta_l^{1/p}$ est séparable sur $E(\theta_1^{1/p}, \dots, \theta_{l-1}^{1/p})$. Comme $E^{1/p} = E(\theta_1^{1/p}, \dots, \theta_l^{1/p})$ est purement inséparable sur E , alors le degré de séparabilité $[E^{1/p} : E]_s$ est nul. Par suite, nécessairement $\theta_l^{1/p}$ est un élément de $E(\theta_1^{1/p}, \dots, \theta_{l-1}^{1/p})$, ce qui contredit la minimalité de la base $(\theta_1, \dots, \theta_l)$.

Les composantes de V sont donc bien géométriquement réduites. $\square$

On obtient en particulier la réponse à la question précédente en dimension 2.

Corollaire. *Soit α un point de $\mathbb{G}_a^2(\overline{E})$, séparable sur E . Alors, il existe une E -variété V_0 dont les $\overline{E}$ -composantes sont G.R. sur E , et telle que*

$$\deg_E(V_0) = \delta_E(\alpha)^{\text{codim } V_0}.$$

3 - Géométrie

Dans un premier temps, on se donne un T -module $(\mathbb{G}_a^n, \Phi)$ de degré d , défini sur une extension finie E de k . Le groupe $\mathbb{G}_a^n$ se plonge dans $\mathbb{P}^n$ via le morphisme suivant.

$$\eta : \begin{array}{ccc} \mathbb{G}_a^n & \longrightarrow & \mathbb{P}^n, \\ (x_1, \dots, x_n) & \longmapsto & (1 : \dots : x_n). \end{array}$$

Soit V une $\bar{k}$ -variété de $\mathbb{G}_a^n$. Comme précédemment, par degré de V , noté $\deg V$, on entend le degré de l'adhérence de Zariski de $\eta(V)$ dans $\mathbb{P}^n$. Le stabilisateur de V est noté G_V .

$$(13) \quad G_V = \{\mathbf{x} \in \mathbb{G}_a^n, V + \mathbf{x} = V\} = \bigcap_{\mathbf{y} \in V} (V - \mathbf{y})$$

On désigne encore par G_V^0 la composante neutre de G_V , c'est-à-dire sa composante connexe passant par 0. On sait, d'après la proposition du paragraphe 7.3 de [Hu] (page 53), que cette composante connexe est aussi une composante irréductible de G_V . On a, par définition du stabilisateur, l'inégalité $\dim G_V \leq \dim V$. D'autre part, comme dans le paragraphe 2 de [AD], on peut montrer la majoration

$$\deg G_V \leq (\deg V)^{\dim V + 1 - \dim G_V}.$$

Dans ce qui suit, on adapte les preuves de [AD] à notre cadre.

Lemme 2. *Soit V une $\bar{k}$ -variété propre de $\mathbb{G}_a^n$, et $a \in A$ non nul. On a alors les égalités suivantes.*

$$(i) \quad \deg(\Phi_a^{-1}(V)) = q^{d \deg a \cdot \text{codim} V} \deg V$$

$$(ii) \quad \deg(\Phi_a(V)) = \frac{q^{d \deg a \dim V}}{|\ker \Phi_a \cap G_V|} \deg V$$

Preuve - On suit la démonstration du lemme 6 de [Hi] pour démontrer (i). On définit le morphisme algébrique Φ_a^h de la façon suivante.

$$\Phi_a^h(x_0, \dots, x_n) = \left(x_0^{q^{d \deg a}}, x_0^{q^{d \deg a}} \Phi_a(x_1/x_0, \dots, x_n/x_0) \right) \quad (x_0 \neq 0).$$

D'après le lemme 1 de [De2], le morphisme Φ_a^h est un prolongement de Φ_a à $\mathbb{P}^n$, c'est-à-dire que le diagramme ci-dessous est commutatif.

$$\begin{array}{ccc} \mathbb{G}_a^n & \xrightarrow{\eta} & \mathbb{P}^n \\ \Phi_a \downarrow & \circlearrowleft & \downarrow \Phi_a^h \\ \mathbb{G}_a^n & \longrightarrow & \mathbb{P}^n \end{array}$$

Soit D la classe d'équivalence rationnelle d'un hyperplan de $\mathbb{P}^n$. Si V est une sous variété de $\mathbb{G}_a^n$, on note $\bar{V}$ l'adhérence de Zariski de $\eta(V)$ dans $\mathbb{P}^n$. Pour un cycle $Z = \sum n_i P_i$ de dimension 0, on notera encore $\deg_0(Z) = \sum n_i$. Alors, on a la relation

$$\deg V = \deg_0(\bar{V} \cdot D^{\dim V}).$$

On a de plus le résultat d'équivalence linéaire

$$\Phi_a^*(\mathcal{O}_{\mathbb{P}^n}(1)) \simeq q^{d \deg a} \mathcal{O}_{\mathbb{P}^n}(1),$$

où Φ_a^* désigne $(\Phi_a^h)^{-1}$. D'autre part, la démonstration de la proposition II.2.11 de [B2] est aussi valable ici, ainsi $\Phi_a^*(V)$ est linéairement équivalent au fermé $\overline{\Phi_a^{-1}(V)}$. Pour conclure, on effectue le calcul suivant.

$$\begin{aligned} q^{dn \deg a} \deg V &= q^{dn \deg a} \deg_0 (\overline{V} \cdot D^{\dim V}), \\ &= \deg_0 (\Phi_a^*(\overline{V} \cdot D^{\dim V})), \\ &= \deg_0 (\Phi_a^*(\overline{V}) \cdot \Phi_a^*(D)^{\dim V}), \\ &= \deg_0 (\overline{\Phi_a^{-1}(V)} \cdot (q^{d \deg a} D)^{\dim V}), \\ &= q^{d \deg a \cdot \dim V} \deg_0 (\overline{\Phi_a^{-1}(V)} \cdot D^{\dim V}), \\ &= q^{d \deg a \cdot \dim V} \deg (\Phi_a^{-1}(V)). \end{aligned}$$

Ainsi, l'assertion (i) est bien démontrée.

On remarque ensuite que $\Phi_a^{-1}(\Phi_a(V)) = V + \ker \Phi_a$. On applique alors ce qui précède à la variété $\Phi_a(V)$.

$$\begin{aligned} \deg (\Phi_a^{-1}(\Phi_a(V))) &= q^{d \deg a \cdot \text{codim } V} \deg (\Phi_a(V)), \\ &= \deg(V + \ker \Phi_a), \\ &= |\ker \Phi_a / (\ker \Phi_a \cap G_V)| \deg V, \\ &= \frac{q^{dn \deg a}}{|\ker \Phi_a \cap G_V|} \deg V. \end{aligned}$$

□

Les lemmes 2 et 3 de [Do] affirment que les conjugués des multiples d'un point sont essentiellement distincts. On étend ce résultat à des variétés de dimension 0 ou 1.

Proposition 11. *Soit $(\mathbb{G}_a^2, \Phi)$ un T -module défini sur E , vérifiant les hypothèses (Gal 1) et (Gal 2). Soit V une E -variété propre de $\mathbb{G}_a^2$, et $V_1, \dots, V_l$ ses $\overline{E}$ -composantes. Si V n'est pas réunion de translatés d'un sous- B -module de $(\mathbb{G}_a^2, \Phi)$ (pour $B \in A$ non nul) par des points de torsion, alors pour tous $a, b \in A \setminus \{1\}$ unitaires et premiers entre eux, et pour tous i, j dans $\{1, \dots, l\}$, on a*

$$\Phi_a(V_i) \neq \Phi_b(V_j),$$

ce qui implique en particulier $\Phi_a(V) \neq \Phi_b(V)$.

Preuve - Si V est de dimension 0, la proposition est assez claire. En effet, dans ce cas V est de la forme $\{\sigma(\mathbf{x}), \sigma \in \text{Aut}(\overline{E}/E)\}$, où $\mathbf{x}$ est un élément de $\mathbb{G}_a^2(\overline{E})$. Si l'on avait l'égalité $\Phi_a(\sigma_1(\mathbf{x})) = \Phi_b(\sigma_2(\mathbf{x}))$, comme σ_1 commute avec Φ_a et Φ_b , en posant $\sigma = \sigma_1^{-1} \circ \sigma_2$, on aurait aussi $\Phi_a(\mathbf{x}) = \Phi_b(\sigma(\mathbf{x}))$. Soit $n \in \mathbb{N}$ pour lequel on a $\sigma^n(\mathbf{x}) = \mathbf{x}$. Alors, on montrerait facilement la relation

$$\Phi_{a^n}(\mathbf{x}) = \Phi_{b^n}(\mathbf{x}).$$

Comme $a^n - b^n \neq 0$, le point $\mathbf{x}$ serait de torsion, et il en serait de même pour tous ses conjugués.

On suppose désormais que la dimension de V vaut 1. On se propose tout d'abord de prouver le résultat intermédiaire suivant.

Soit V_0 une $\overline{E}$ -variété, et $a, b \in A$ unitaires et premiers entre eux. Si $\Phi_a(V_0) = \Phi_b(V_0)$, alors V_0 est le translaté d'un sous- T -module de $(\mathbb{G}_a^2, \Phi)$ par un point de torsion.

Dans un premier temps, on ne suppose pas a et b unitaires, et on montre ce point lorsque $|a| \neq |b|$. L'égalité des variétés $\Phi_{a^n}(V_0)$ et $\Phi_{b^n}(V_0)$ pour $n \in \mathbb{N}$, entraîne celle de leurs degrés. Le point (i) du lemme 2 assure alors de la relation suivante.

$$\frac{|a|^{dn \dim V_0}}{|\ker \Phi_{a^n} \cap G_{V_0}|} = \frac{|b|^{dn \dim V_0}}{|\ker \Phi_{b^n} \cap G_{V_0}|}.$$

On suppose, par exemple $|a| < |b|$. Puisque V_0 est de dimension 1, on obtient

$$\left(\frac{|b|}{|a|}\right)^{dn \dim V_0} = \left(\frac{|b|}{|a|}\right)^{dn} \leq |\ker \Phi_{b^n} \cap G_{V_0}|.$$

On construit grâce à cette minoration, une suite infinie de points de torsion primitive dans G_{V_0} . Soit $n_0 \in \mathbb{N}$ tel que $\left(\frac{|b|}{|a|}\right)^{dn_0} \geq 2$. Alors, il existe un diviseur b_0 de b^{n_0} , et un point $\mathbf{x}_0$ de b_0 -torsion primitive, qui est dans G_{V_0} . On suppose avoir construit une suite $n_0, \dots, n_j$ d'entiers, pour lesquels il existe $b_0, \dots, b_j \in A$ distincts vérifiant

$$\forall i = 0, \dots, j \quad b_i | b^{n_i},$$

et tels qu'il existe dans G_{V_0} au moins un point $\mathbf{x}_i$ de b_i -torsion primitive. Soit n_{j+1} un entier tel que $\left(\frac{|b|}{|a|}\right)^{dn_{j+1}} \geq |b_0 \cdots b_j|^{2d} + 1$. Alors, il existe un diviseur b_{j+1} de $b^{n_{j+1}}$, distinct des $b_0, \dots, b_j$, pour lequel au moins un point $\mathbf{x}_{j+1}$ de G_{V_0} est de b_{j+1} -torsion primitive. On construit de cette manière une suite $(b_i)_{i \in \mathbb{N}}$ d'éléments de A , qui en particulier, sont tous premiers à a .

On note W l'union de G_{V_0} et de ses composantes conjuguées sur E . Alors W contient chacun des $\mathbf{x}_i$ et ses conjugués. Comme ils sont au moins $|b_i|^{C(\Phi)}$ d'après (Gal 1), et comme d'après (Gal 2), l'application Φ_a les permute, on a alors

$$|W \cap \Phi_a(W)| \geq |b_i|^{C(\Phi)}.$$

Puisque les b_i sont en nombre infini, l'ensemble algébrique $W \cap \Phi_a(W)$ est nécessairement de dimension 1. Ainsi, W et $\Phi_a(W)$ ont au moins une composante commune. Or, tout isomorphisme fixant E commute avec Φ_a , on a donc l'existence d'une composante $\sigma(G_{V_0})$ conjuguée sur E à G_{V_0} , telle que $G_{V_0} = \Phi_a(\sigma(G_{V_0}))$. Soit m un entier pour lequel on a $\sigma^m(G_{V_0}) = G_{V_0}$. Alors, $G_{V_0} = \Phi_{a^m}(G_{V_0})$ est un sous- a^m -module H de $(\mathbb{G}_a^2, \Phi)$.

On montre de plus l'égalité $\Phi_a(H) = \Phi_b(H)$. Soit $\mathbf{z} \in H$, on peut trouver $\mathbf{y} \in \mathbb{G}_a^2$ pour lequel on a $\Phi_a(\mathbf{z}) = \Phi_b(\mathbf{y})$. Par définition de H , on a $V_0 + \mathbf{z} = V_0$. Ainsi, on a les égalités suivantes.

$$\Phi_a(V_0) + \Phi_a(\mathbf{z}) = \Phi_a(V_0),$$

$$\Phi_b(V_0) + \Phi_b(\mathbf{y}) = \Phi_b(V_0).$$

Il existe donc $\mathbf{z}' \in H$ et $\mathbf{z}_b \in \ker \Phi_b$ pour lesquels on a $\mathbf{y} = \mathbf{z}' + \mathbf{z}_b$. Par conséquent, $\Phi_a(\mathbf{z}) = \Phi_b(\mathbf{y}) = \Phi_b(\mathbf{z}') \in \Phi_b(H)$. Par symétrie du problème, on a l'inclusion inverse et donc l'égalité.

De plus H est un groupe, donc on a $\Phi_{b-a}(H) \subset \Phi_a(H) = \Phi_b(H)$. Comme H est irréductible, l'inclusion est en fait une égalité.

Or, $H = G_{V_0}$ est de dimension 1, ainsi il existe $\mathbf{x} \in \mathbb{G}_a^2$ vérifiant $V_0 = H + \mathbf{x}$. Alors, de la relation $\Phi_a(V_0) = \Phi_b(V_0)$ on tire

$$\Phi_a(H) + \Phi_a(\mathbf{x}) = \Phi_b(H) + \Phi_b(\mathbf{x}).$$

Par conséquent, $\Phi_{b-a}(\mathbf{x})$ appartient à $\Phi_a(H) = \Phi_{b-a}(H)$. Il existe donc $h \in H$ tel que $\Phi_{b-a}(\mathbf{x}) = \Phi_{b-a}(h)$. Alors $\mathbf{x} - h$ est un point de torsion et on a encore $V_0 = H + (\mathbf{x} - h)$.

On traite maintenant le cas où a et b sont unitaires, et où $|a| = |b|$. Si G_{V_0} est de dimension 1, alors V_0 est un translaté de G_{V_0} , ce dernier est donc irréductible. Il existe de plus $\mathbf{x} \in \mathbb{G}_a^2$ pour lequel on a $V_0 = G_{V_0} + \mathbf{x}$. Comme précédemment, on a l'égalité $\Phi_{b-a}(G_{V_0}) = \Phi_b(G_{V_0})$. Or a et b sont unitaires et de même degré, par conséquent, $|b - a| < |b|$. On est donc ramené au cas précédent.

On montre ensuite que, supposer G_{V_0} de dimension 0, conduit à une absurdité. On prouve tout d'abord que dans ce cas, $G_{V_0} \cap \ker \Phi_a$ et $G_{V_0} \cap \ker \Phi_b$ sont réduits à $\{0\}$. D'une part, comme on a $|a| = |b|$ et $\Phi_a(V_0) = \Phi_b(V_0)$, le point (ii) du lemme 2 donne

$$|G_{V_0} \cap \ker \Phi_a| = |G_{V_0} \cap \ker \Phi_b| = p^n,$$

où n désigne la dimension sur $\mathbb{F}_p$, de chacun des groupes $G_{V_0} \cap \ker \Phi_a$ et $G_{V_0} \cap \ker \Phi_b$. On a de même

$$\Phi_{a^2}(V_0) = \Phi_{ab}(V_0) = \Phi_{b^2}(V_0) \quad \text{et} \quad |a^2| = |ab| = |b^2|.$$

D'autre part, a et b sont premiers entre eux, par conséquent on a la somme directe de $\mathbb{F}_p$ -espaces vectoriels $\ker \Phi_{ab} = \ker \Phi_a \oplus \ker \Phi_b$. Il en découle la minoration suivante.

$$\begin{aligned} |G_{V_0} \cap \ker \Phi_{a^2}| &= |G_{V_0} \cap \ker \Phi_{b^2}| = |G_{V_0} \cap \ker \Phi_{ab}|, \\ &\geq |(G_{V_0} \cap \ker \Phi_a) \oplus (G_{V_0} \cap \ker \Phi_b)| = p^{2n}. \end{aligned}$$

En réitérant, on obtient une minoration du type $|G_{V_0}| \geq p^{2^i n}$, ceci pour tout entier i . Comme G_{V_0} est fini, cela entraîne $n = 0$, c'est-à-dire

$$G_{V_0} \cap \ker \Phi_a = G_{V_0} \cap \ker \Phi_b = \{0\}.$$

On s'intéresse maintenant aux ensembles algébriques $\Phi_a^{-1}(V_0)$ et $\Phi_b^{-1}(V_0)$. En prenant l'image réciproque de l'égalité $\Phi_a(V_0) = \Phi_b(V_0)$, par Φ_a puis par Φ_b , on obtient

$$\Phi_a^{-1}(V_0) + \ker \Phi_{ab} = \Phi_b^{-1}(V_0) + \ker \Phi_{ab}.$$

Soit V'_0 une composante de $\Phi_b^{-1}(V_0)$, alors il existe $\mathbf{z} \in \ker \Phi_{ab}$ tel que $V'_0 + \mathbf{z}$ est une composante de $\Phi_a^{-1}(V_0)$. Or, il existe $\mathbf{z}_a \in \ker \Phi_a$ et $\mathbf{z}_b \in \ker \Phi_b$ tels que l'on a $\mathbf{z} = \mathbf{z}_a + \mathbf{z}_b$.

On note alors $V'_1 = V'_0 + \mathbf{z}_b$. On voit clairement que V'_1 est à la fois une composante de $\Phi_a^{-1}(V_0)$ et de $\Phi_b^{-1}(V_0)$. Ainsi, on a les égalités

$$\begin{aligned}\Phi_a^{-1}(V_0) &= V'_1 + \ker\Phi_a, \\ \Phi_b^{-1}(V_0) &= V'_1 + \ker\Phi_b.\end{aligned}$$

En utilisant les égalités $G_{V_0} \cap \ker\Phi_a = \{0\}$ et $\ker\Phi_a \cap \ker\Phi_b = \{0\}$, on montre facilement que $G_{V'_1} \cap \ker\Phi_b$ est trivial, ainsi $\deg(V'_1 + \ker\Phi_b) = |\ker\Phi_b| \deg(V'_1)$. Le point (i) du lemme 2 donne donc

$$\begin{aligned}\deg(\Phi_b^{-1}(V_0)) &= |b|^d \deg(V_0), \\ &= \deg(V'_1 + \ker\Phi_b), \\ &= |b|^{2d} \deg(V'_1).\end{aligned}$$

Par conséquent, V'_1 est une $\overline{E}$ -variété qui vérifie

$$\Phi_a(V'_1) = \Phi_b(V'_1) = V_0, \quad \deg(V'_1) = \frac{\deg(V_0)}{|b|^d} \quad \text{et} \quad \dim(G_{V'_1}) = 0.$$

En répétant ce travail j fois, on montre que $|b|^{dj}$ divise $\deg(V_0)$, et ceci quelque soit l'entier j , ce qui donne la contradiction annoncée.

On a donc démontré, que si V_0 est une $\overline{E}$ -variété vérifiant $\Phi_a(V_0) = \Phi_b(V_0)$, avec $a, b \in A$ unitaires et premiers entre eux, alors V_0 est un translaté de sous- T -module par un point de torsion.

On revient maintenant à l'énoncé général de la proposition. Si $V = V_1 \cup \dots \cup V_l$ est une E -variété vérifiant $\Phi_a(V) = \Phi_b(V)$, alors

$$\forall i \in \{1, \dots, l\}, \exists \sigma_i \in \text{Aut}(\overline{E}/E), \quad \Phi_a(V_i) = \Phi_b(\sigma_i(V_i)).$$

Puisque Φ est défini sur E , alors Φ_b et σ_i commutent. Aussi, pour tout entier $m \geq 0$ on a

$$\Phi_{a^m}(V_i) = \Phi_{b^m}(\sigma_i^m(V_i)).$$

Soit $m_i \in \mathbb{N} \setminus \{0\}$ pour lequel on a $\sigma_i^{m_i}(V_i) = V_i$, alors $\Phi_{a^{m_i}}(V_i) = \Phi_{b^{m_i}}(V_i)$ et a^{m_i} et b^{m_i} sont unitaires et premiers entre eux. D'après ce qui précède, V_i est le translaté d'un sous- T -module H_i par un point de torsion. Ainsi, V est bien réunion de translatés de sous- T -modules par des points de torsion. $\square$

Soit V une E -variété, et $V_1, \dots, V_l$ ses $\overline{E}$ -composantes. On note

$$(14) \quad \begin{aligned}E_1(V) &= \{a \in A, \exists i, j \in \mathbb{N}, 1 \leq i < j \leq l, \Phi_a(V_i) = \Phi_a(V_j)\}, \\ E_2(V) &= \{a \in A, \exists i \in \mathbb{N}, 1 \leq i \leq l, \deg(\Phi_a(V_i)) < \deg(V_i)\}, \\ E(V) &= E_1(V) \cup E_2(V).\end{aligned}$$

On désigne par A_{irr}^+ l'ensemble des éléments de A irréductibles et unitaires. On notera encore $E^+(V) = E(V) \cap A_{\text{irr}}^+$ et pour $i = 1$ ou 2 , $E_i^+(V) = E_i(V) \cap A_{\text{irr}}^+$. L'objectif de la proposition suivante est de majorer le cardinal de $E^+(V)$ en fonction du degré de V .

Proposition 12. Soit $(\mathbb{G}_a^2, \Phi)$ un T -module défini sur E , et satisfaisant les hypothèses (H), (Gal 1) et (Gal 2). Il existe une constante $C_1(\Phi) > 0$ telle que pour toute E -variété propre V de $\mathbb{G}_a^2$, on ait la majoration

$$|E^+(V)| \leq C_1(\Phi) \log \deg_E(V).$$

Preuve - On commence par majorer $|E_1^+(V)|$. Soit $r \in \mathbb{N}$ maximal (on verra qu'il existe) tel qu'on peut trouver $b_1, \dots, b_r \in A_{\text{irr}}^+$ distincts, $\beta_1, \dots, \beta_r \in A$ vérifiant

$$(15) \quad \begin{aligned} \forall i, j \in \{1, \dots, r\} \quad (b_i, \beta_j) &= 1, \\ \forall i, j \in \{1, \dots, r\}, i \neq j, \quad (\beta_i, \beta_j) &= 1, \\ \forall i \in \{1, \dots, r\}, \quad (b_i, T) &= 1 \text{ et } (\beta_i, T) = 1, \end{aligned}$$

et pour lesquels on a $\forall i \in \{1, \dots, r\}, \exists x_i \in \ker \Phi_{\beta_i}, \exists y_i \in \ker \Phi_{b_i}, \exists s_i \in \{2, \dots, l\}$ tels que

$$V_{s_i} = V_1 + x_i = V_1 + y_i.$$

Comme $V_{s_i} \neq V_1$, cela implique en particulier que les y_i ne sont pas nuls, et que pour tout indice i , y_i et x_i sont distincts. On remarque de plus que, quitte à prendre au lieu de β_i un de ses diviseurs, on peut supposer que chaque x_i est de β_i -torsion primitive. On note

$$(16) \quad N(V) = \{b_1, \dots, b_r, T\} \cup \{b \in A_{\text{irr}}^+, \exists i \in \{1, \dots, r\}, b | \beta_i\}.$$

Alors, pour majorer le cardinal de $E_1^+(V)$, il suffit de majorer le cardinal de $N(V)$ ainsi que celui de $F(V) = E_1^+(V) \setminus N(V)$.

Majoration de $|F(V)|$:

La démonstration suit en partie celle de F. Amoroso et S. David (lemme 2.3 [AD]), qui ont eux-même adapté celle de Dobrowolski (lemme 3 [Do]) aux dimensions supérieures. Pour tout élément a de A , et tout indice $i \in \{1, \dots, l\}$, on note

$$(17) \quad \mathcal{J}(a, i) = \{j \in \{1, \dots, l\}, \Phi_a(V_i) = \Phi_a(V_j)\}.$$

Il est clair que pour $a \in A$ fixé, les ensembles $\mathcal{J}(a, i)$ ($1 \leq i \leq l$) ont même cardinal et sont soit égaux, soit disjoints. Soit $b \in F(V)$, et $a = a_1 \cdots a_\nu$ où les $a_i \in F(V)$ sont distincts.

On montre dans un premier temps l'inclusion

$$\bigcup_{j \in \mathcal{J}(a, i)} \mathcal{J}(b, j) \subset \mathcal{J}(ab, i).$$

En effet, soit $j \in \mathcal{J}(a, i)$ et $m \in \mathcal{J}(b, j)$. Alors, on a $\Phi_a(V_i) = \Phi_a(V_j)$ et $\Phi_b(V_j) = \Phi_b(V_m)$. Par conséquent, $\Phi_{ba}(V_i) = \Phi_{ab}(V_m)$, et donc m est un élément de $\mathcal{J}(ab, i)$.

Soient alors $j_1, j_2 \in \mathcal{J}(a, i)$ pour lesquels l'intersection $\mathcal{J}(b, j_1) \cap \mathcal{J}(b, j_2)$ n'est pas vide. On a donc d'une part l'égalité $\Phi_a(V_i) = \Phi_a(V_{j_1}) = \Phi_a(V_{j_2})$, et d'autre part

$\Phi_b(V_{j_1}) = \Phi_b(V_{j_2})$. En appliquant respectivement Φ_a^{-1} et Φ_b^{-1} à ces deux relations, on obtient l'existence de $\mathbf{x} \in \ker \Phi_a$ et de $\mathbf{y} \in \ker \Phi_b$ pour lesquels on a :

$$V_{j_2} = V_{j_1} + \mathbf{x} = V_{j_1} + \mathbf{y}.$$

Mais, en appliquant à cette relation un E -isomorphisme bien choisi, on peut se ramener à $j_1 = 1$. Le couple (a, b) satisfait donc aux conditions (15), ce qui contredit la maximalité de r (vue dans la majoration de $|N(V)|$) si j_2 est distinct de j_1 . Ainsi, nécessairement on a l'égalité $j_2 = j_1$.

L'inclusion précédente est par conséquent disjointe, et puisque pour tout $j \in \mathcal{J}(a, i)$, les ensembles $\mathcal{J}(b, j)$ ont même cardinal, on obtient la minoration suivante.

$$|\mathcal{J}(ab, i)| \geq |\mathcal{J}(a, i)| \cdot |\mathcal{J}(b, i)|$$

Par récurrence, on montre facilement que si $b_1, \dots, b_\nu \in F(V)$ sont distincts, alors on a

$$\prod_{j=1}^{\nu} |\mathcal{J}(b_j, i)| \leq \left| \mathcal{J} \left(\prod_{j=1}^{\nu} b_j, i \right) \right| \leq l.$$

Enfin, si $b \in F(V)$, par définition $|\mathcal{J}(b, i)| \geq 2$ pour au moins un des indices i , et donc pour tous les éléments de $\{1, \dots, l\}$, ainsi on a

$$2^{|F(V)|} \leq \prod_{b \in F(V)} |\mathcal{J}(b, 1)| \leq \left| \mathcal{J} \left(\prod_{b \in F(V)} b, 1 \right) \right| \leq l.$$

Par suite, on obtient la majoration cherchée

$$(18) \quad |F(V)| \leq \frac{\log l}{\log 2}.$$

Majoration de $|N(V)|$:

On commence par donner le lemme suivant, dont le cadre n'est plus restrictif sur Φ .

Lemme 3. Soient $(\mathbb{G}_a^n, \Phi)$ un T -module défini sur E , $\mathbf{z}_1, \dots, \mathbf{z}_J \in \mathbb{G}_a^n$ et $b_1, \dots, b_J$ des éléments de A premiers entre eux deux à deux. Si pour tout $i \in \{1, \dots, J\}$ le point $\mathbf{z}_i$ est de b_i -torsion primitive, alors pour tous $\lambda_1, \dots, \lambda_J \in \mathbb{F}_q$ tous non nuls, le point $\lambda_1 \mathbf{z}_1 + \dots + \lambda_J \mathbf{z}_J$ est de $(b_1 \cdots b_J)$ -torsion primitive.

Preuve - On note $\mathbf{y} = \lambda_1 \mathbf{z}_1 + \dots + \lambda_J \mathbf{z}_J$. Soit $b' \in A \setminus \mathbb{F}_q$ un diviseur de $b_1 \cdots b_J$ tel que $\Phi_{b'}(\mathbf{y}) = 0$. On note $d_1 = (b', b_1)$. Comme $\Phi_{b_1 \cdots b_J}(\mathbf{y}) = 0$, on a aussi $\Phi_{d_1 b_2 \cdots b_J}(\mathbf{y}) = 0$, et donc comme $\lambda_1 \neq 0$,

$$\Phi_{d_1 b_2 \cdots b_J}(\mathbf{z}_1) = 0.$$

Or $\Phi_{b_1}(\mathbf{z}_1) = 0$, et $(d_1 b_2 \cdots b_J, b_1) = d_1$ donc $\Phi_{d_1}(\mathbf{z}_1) = 0$. Mais $\mathbf{z}_1$ est de b_1 -torsion primitive, donc nécessairement, il existe $\mu_1 \in \mathbb{F}_q^*$ tel que $b_1 = \mu_1 d_1$. On procède de même pour tous les indices $i \in \{1, \dots, J\}$. Comme les b_i sont premiers entre eux, on ne peut qu'avoir $b' = \mu b_1 \cdots b_J$, où $\mu \in \mathbb{F}_q^*$, ce qui achève la preuve du lemme. $\square$

On poursuit la preuve de la proposition 12. On considère pour cela l'ensemble algébrique $W = \bigcup_{i=1}^l G_{V_i}$, et on distingue deux cas.

Premier cas : $\dim(W) = 0$.

Par construction, le point $x_1 - y_1 + \cdots + x_r - y_r$ est dans G_{V_1} , et d'après le lemme précédent, il est de $(b_1\beta_1 \cdots b_r\beta_r)$ -torsion primitive. Selon l'hypothèse (Gal 1), il possède au moins $|b_1\beta_1 \cdots b_r\beta_r|^{C(\Phi)}$ conjugués, qui d'ailleurs sont dans W . Par conséquent, on a

$$|b_1\beta_1 \cdots b_r\beta_r|^{C(\Phi)} \leq |W| \leq l \deg G_{V_1} \leq l(\deg V_1)^2 \leq (\deg_E V)^2.$$

En particulier, le nombre r existe bien, et par définition de $N(V)$ il s'en suit que

$$(19) \quad |N(V)| \leq \frac{\log |b_1\beta_1 \cdots b_r\beta_r|}{\log q} + 1 \leq \frac{2}{C(\Phi) \log q} \log \deg_E(V) + 1.$$

Second cas : $\dim(W) = 1$.

On a ici $V_i = G_{V_i} + t_i$ ($1 \leq i \leq l$), et donc les G_{V_i} sont irréductibles sur $\bar{E}$. On considère encore deux sous-cas.

$$- \quad \dim(W \cap \Phi_T(W)) = 1.$$

On va montrer que nécessairement, $N(V)$ est réduit à $\{T\}$, c'est-à-dire que l'entier r qui intervient dans la définition de $N(V)$ est égal à 0. En effet, dans ce cas, il existe un E -isomorphisme σ tel que

$$G_{V_1} = \Phi_T(\sigma(G_{V_1})).$$

Et donc, on peut trouver un entier m tel que $G_{V_1} = \Phi_{T^m}(G_{V_1})$. Ainsi, selon l'hypothèse (H), $G_{V_1} = H$ est un sous- T -module de $(\mathbb{G}_a^2, \Phi)$. S'il existe des nombres $\beta_1, b_1 \in A$, $x_1 \in \ker \Phi_{\beta_1}$, $y_1 \in \ker \Phi_{b_1}$ et un indice $s_1 \neq 1$ tels que l'on ait les égalités $V_{s_1} = V_1 + x_1 = V_1 + y_1$. Cela implique en particulier que $G_{V_{s_1}} = G_{V_1} = H$, et donc

$$H = V_1 - t_1 = V_{s_1} - t_2.$$

D'après l'égalité $\Phi_{b_1}(V_1) = \Phi_{b_1}(V_{s_1})$, on a $\Phi_{b_1}(t_2 - t_1) \in \Phi_{b_1}(H) = H$. De même, on montre $\Phi_{\beta_1}(t_2 - t_1) \in H$. Comme b_1 et β_1 sont premiers entre eux, on a donc $t_2 - t_1 \in H$, et par là même $V_{s_1} = V_1$, ce qui est exclu. Ainsi, si $\dim(W \cap \Phi_T(W)) = 1$ alors $r = 0$ et

$$|N(V)| = 1.$$

$$- \quad \dim(W \cap \Phi_T(W)) = 0.$$

Comme précédemment, il existe au moins un point de $(b_1\beta_1 \cdots b_r\beta_r)$ -torsion primitive dans W , et ses conjugués y sont également. Comme T est premier à $b_1\beta_1 \cdots b_r\beta_r$, d'après l'hypothèse (Gal 2), Φ_T permute ces conjugués, ainsi on a encore

$$|b_1\beta_1 \cdots b_r\beta_r|^{C(\Phi)} \leq |W \cap \Phi_T(W)| \leq q^d(\deg W)^2 \leq q^d(\deg_E V)^2.$$

Par suite, on obtient encore l'existence de r , ainsi que la majoration

$$(20) \quad |N(V)| \leq \frac{4}{C(\Phi) \log q} \log \deg_E(V) + d + 1.$$

On peut donc conclure quant à la majoration du cardinal de $E_1^+(V)$.

$$(21) \quad \begin{aligned} |E_1^+(V)| &\leq \frac{6}{C(\Phi) \log q} \log \deg_E(V) + d + 2 + \frac{\log l}{\log 2}, \\ &\leq C_1 \log \deg_E(V). \end{aligned}$$

On passe maintenant à la majoration de $|E_2^+(V)|$. Soit $b \in E_2^+(V)$, alors pour tout indice $i \in \{1, \dots, l\}$, on a aussi $\deg(\Phi_b(V_i)) < \deg(V_i)$. Ainsi, $E_2^+(V)$ s'écrit encore

$$E_2^+(V) = \{b \in A_{\text{irr}}^+, \deg(\Phi_b(V_1)) < \deg(V_1)\}.$$

D'après le point (i) du lemme 2, on a l'égalité

$$\deg(\Phi_b(V_1)) = \frac{q^{d \deg(b) \dim(V_1)}}{|G_{V_1} \cap \ker \Phi_b|} \deg(V_1).$$

Si V_1 est de dimension 0, elle est réduite à un point et on a l'égalité

$$\deg(\Phi_b(V_1)) = \deg(V_1) = 1.$$

A fortiori l'ensemble $E_2^+(V)$ est vide.

On suppose maintenant que la dimension de V_1 vaut 1. Alors $E_2^+(V)$ s'écrit

$$E_2^+(V) = \{b \in A_{\text{irr}}^+, |G_{V_1} \cap \ker \Phi_b| > q^{d \deg(b)}\}.$$

Soient $b_1, \dots, b_m$ des éléments distincts de $E_2^+(V)$. Alors, on a la somme directe suivante d'espaces vectoriels sur $\mathbb{F}_p$

$$\bigoplus_{i=1}^m (G_{V_1} \cap \ker \Phi_{b_i}) \subset G_{V_1}.$$

Pour $i = 1, \dots, m$, on désigne par n_i la dimension sur $\mathbb{F}_p$ de $G_{V_1} \cap \ker \Phi_{b_i}$. Alors, d'une part, d'après l'inclusion précédente on a $|G_{V_1}| \geq p^{n_1 + \dots + n_m}$ et d'autre part, par définition de $E_2^+(V)$, on a

$$\forall i = 1, \dots, m \quad n_i \geq d \deg(b_i) \frac{\log q}{\log p}.$$

Ainsi on obtient la minoration $|G_{V_1}| \geq |b_1 \cdots b_m|^d$.

Si G_{V_1} est de dimension 0, alors on a clairement

$$|E_2^+(V)| \leq \frac{\log |G_{V_1}|}{d \log q} \leq \frac{2}{d \log q} \log \deg(V).$$

Sinon, G_{V_1} est de dimension 1, et à nouveau, on considère l'ensemble $W = \bigcup_{i=1}^l G_{V_i}$.

Premier cas : $\dim(W \cap \Phi_T(W)) = 1$.

D'après l'hypothèse (H), le groupe G_{V_1} est un sous- T -module de $(\mathbb{G}_a^2, \Phi)$, alors comme il est irréductible, pour tout $a \in A \setminus \{0\}$, on a $\Phi_a(G_{V_1}) = G_{V_1}$. Le point (ii) du lemme 2 donne alors l'égalité $|G_{V_1} \cap \ker \Phi_a| = q^{d \deg(a)}$, ainsi $E_2^+(V)$ est vide.

Second cas : $\dim(W \cap \Phi_T(W)) = 0$.

Comme précédemment, au moins un point de $(b_1 \dots b_m)$ -torsion primitive et ses conjugués sont dans l'intersection $W \cap \Phi_T(W)$, on a donc la majoration

$$|b_1 \dots b_m|^{C(\Phi)} \leq q^d (\deg W)^2 \leq q^d (\deg_E V)^2$$

Dans ce cas, on a alors $|E_2^+(V)| \leq \frac{4}{C(\Phi) \log q} \log \deg_E(V) + d$.

Ainsi, on a bien prouvé l'existence d'une constante C_2 pour laquelle on a la majoration

$$|E_2^+(V)| \leq C_2 \log \deg(V). \quad \square$$

On montre enfin la proposition suivante.

Proposition 13. *Soient $(\mathbb{G}_a^2, \Phi)$ un T -module défini sur E , satisfaisant aux hypothèses (H), (Gal 1) et (Gal 2). Soit V une E -variété dont les $\overline{E}$ -composantes $V_1, \dots, V_l$ sont G.R. sur E . Alors, on a les propositions suivantes.*

(i) *Si $a, b \in A$ sont tels que $a \notin E(V)$ et $b \notin E(\Phi_a(V))$, alors $ab \notin E(V)$.*

(ii) *Soit Λ un sous-ensemble fini de A_{irr}^+ ne rencontrant pas $E^+(V)$. Si V n'est pas réunion de translatés de sous- T -modules par des points de torsion, alors on a*

$$\deg_E \left(\bigcup_{\lambda \in \Lambda} \Phi_\lambda(V) \right) \geq |\Lambda| \deg_E(V).$$

(iii) *Soit $a \in A \setminus E(V)$ et V' une E -variété de même dimension que V vérifiant l'inclusion $V \subset \Phi_a^{-1}(V')$. On a l'inégalité*

$$\deg_E(V) \leq \deg_E(V').$$

Preuve - Le point (i) est évident. On montre l'assertion (ii). D'après la proposition 11, pour tous a, b dans A_{irr}^+ distincts et tous $i, j \in \{1, \dots, l\}$, on a $\Phi_a(V_i) \neq \Phi_b(V_j)$. D'autre part, Λ ne rencontre pas $E^+(V)$, donc on a aussi

$$\forall \lambda \in \Lambda, \quad \deg(V_i) \leq \deg(\Phi_\lambda(V_i)).$$

Enfin, comme les $\overline{E}$ -composantes de V sont G.R. sur E , on a

$$\deg_E \left(\bigcup_{\lambda \in \Lambda} \Phi_\lambda(V) \right) = \sum_{\lambda \in \Lambda} \sum_{i=1}^l \deg(\Phi_\lambda(V_i)) \geq |\Lambda| \deg_E(V).$$

On prouve maintenant (iii). Par définition de $E(V)$, si $i, j \in \{1, \dots, l\}$ sont distincts et si $a \in A \setminus E(V)$, alors $\Phi_a(V_i) \neq \Phi_a(V_j)$. Comme dans le point précédent, on montre la majoration $\deg(\Phi_a(V_i)) \geq \deg(V_i)$. Par suite, comme les V_i sont G.R. sur E , on a $\deg_E(\Phi_a(V)) \geq \deg_E(V)$. D'autre part, $\Phi_a(V) \subset V'$ et ces variétés ont même dimension, donc on a

$$\deg_E(V) \leq \deg_E(\Phi_a(V)) = \sum \deg(\Phi_a(V_i)) \leq \sum \deg(V'_j) \leq \deg_E(V'),$$

ce qui achève la preuve du point (iii). $\square$

4 - Lemme-clef de Dobrowolski

Dans ce paragraphe, on se donne un T -module $(\mathbb{G}_a^n, \Phi)$ de degré d , défini sur une extension finie E de k . On suppose de plus que la matrice dominante a_d de Φ_T est inversible, ainsi pour tout $a \in A$, la matrice dominante de $\Phi_a(\mathbf{X})$ (i.e. la matrice coefficient devant $\mathcal{F}^{d \deg a}$) l'est aussi. On choisit aussi un dénominateur $\gamma \in A$ des coefficients matriciels de Φ_T . Ainsi, pour tout $a \in A$, les coefficients de $\gamma^{q^{d \deg a}} \Phi_a(X_1, \dots, X_n)$ sont des matrices à coefficients entiers. On supposera de plus, que l'application exponentielle e_Φ associée à Φ est surjective sur $\mathcal{C}^n$.

On se donne $\nu_0 \in A$ irréductible et unitaire. On note $\mathcal{O}_{\nu_0}(E)$ l'anneau des ν_0 -entiers de E , c'est-à-dire l'ensemble des éléments de E qui sont entiers sur le localisé A_{ν_0} de A en la place ν_0 . On fixe encore $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{G}_a^n(\overline{E})$, séparable sur E . On note $\mathfrak{K} = E(\alpha)$ et $\mathcal{O}_{\nu_0}(\mathfrak{K})$ l'anneau des ν_0 -entiers de $\mathfrak{K}$. Pour $\nu_0 \in A$ irréductible et unitaire, on note $(\mathcal{H}_{\nu_0})$ l'hypothèse suivante :

$$(\mathcal{H}_{\nu_0}) \quad \Phi_{\nu_0}(X_1, \dots, X_n) \equiv (X_1^{q^{d \deg \nu_0}}, \dots, X_n^{q^{d \deg \nu_0}}) \pmod{\nu_0}.$$

Cette condition a un sens pour tous les éléments irréductibles et unitaires de A qui sont premiers au dénominateur fixé γ de Φ_T . On suppose de plus, que $\mathcal{O}_{\nu_0}(E) / (\nu_0 \mathcal{O}_{\nu_0}(E))$ est contenu dans $\mathbb{F}_{q^{d \deg \nu_0}}$. Ceci est vrai en particulier, quand $E = k$.

Puisque la fonction e_Φ est surjective sur $\mathcal{C}^n$, il existe $\mathbf{u} = (u_1, \dots, u_n) \in \mathcal{C}^n$ tel que

$$(22) \quad (\alpha_1, \dots, \alpha_n) = e_\Phi(u_1, \dots, u_n).$$

Soit $\mu \in A$ irréductible et unitaire, et $F \in A[X_1, \dots, X_n, Y_1, \dots, Y_n] = A[\mathbf{X}, \mathbf{Y}]$ tel que

$$(23) \quad \deg_{\mathbf{X}} F \leq L \quad \text{et} \quad \deg_{\mathbf{Y}} F \leq L.$$

On suppose de plus que la fonction

$$(24) \quad G(z_1, \dots, z_n) = F\left(e_\Phi(z_1, \dots, z_n), \Phi_\mu(e_\Phi(z_1, \dots, z_n))\right)$$

s'annule à l'ordre au moins T_0 en $(u_1, \dots, u_n)$, ce qui signifie encore, puisque la fonction e_Φ est un isomorphisme local, que le polynôme

$$(25) \quad F_0(\mathbf{X}) = F(\mathbf{X}, \Phi_\mu(\mathbf{X}))$$

s'annule à l'ordre $\geq T_0$ en α .

On remarque que $\deg_{\mathbf{X}} F_0 \leq L_0 := (1 + |\mu|^d)L$, et que si ν_0 ne divise pas γ alors F_0 est un élément de $\mathcal{O}_{\nu_0}(E)[\mathbf{X}]$.

Pour $\tau \in \mathbb{N}^n$, on note $G^{(\tau)}(z_1, \dots, z_n)$ le coefficient de Taylor d'ordre τ dans son développement autour de $\mathbf{z} = (z_1, \dots, z_n)$. Soit w_0 une place de $\mathfrak{K}$ au dessus de ν_0 . Pour tout $x \in \mathfrak{K}$, on note $|x|_{w_0} = q^{-w_0(x) \deg \nu_0}$, et pour tout $\mathbf{x} = (x_1, \dots, x_n) \in \mathfrak{K}^n$:

$$(26) \quad \|\mathbf{x}\|_{w_0} = \max\{1, |x_1|_{w_0}, \dots, |x_n|_{w_0}\}.$$

Ainsi, si $\log_q$ désigne le logarithme en base q , on a l'égalité

$$\log_q \|\mathbf{x}\|_{w_0} = (\deg \nu_0) \max\{0, -w_0(x_1), \dots, -w_0(x_n)\}.$$

Avec ces notations, on a le résultat suivant.

Proposition 14. *Soit $\nu_0 \in A$ irréductible, unitaire, premier avec γ , tel que le déterminant de la matrice dominante de Φ_T soit inversible dans $\mathcal{O}_{\nu_0}(E)$, et tel que*

$$\mathcal{O}_{\nu_0}(E) \setminus (\nu_0 \mathcal{O}_{\nu_0}(E)) \subset \mathbb{F}_{q^{d \deg \nu_0}}.$$

Soient encore w_0 une place de $\mathfrak{K}$ au dessus de ν_0 , et $\tau = (\tau_1, \dots, \tau_n)$ un n -uplet d'entiers. Alors, sous l'hypothèse $(\mathcal{H}_{\nu_0})$, on a la majoration

$$\left| G^{(\tau)}(d\Phi_{\nu_0}(u)) \right|_{w_0} \leq q^{-(T_0 - |\tau|) \deg \nu_0} \|\Phi_{\nu_0}(\alpha)\|_{w_0}^L \|\Phi_{\nu_0 \mu}(\alpha)\|_{w_0}^L.$$

Preuve - On traite tout d'abord le cas où $\alpha_1, \dots, \alpha_n$ sont ν_0 -entiers. L'anneau $\mathcal{O}_{\nu_0}(E)$ étant principal, il est factoriel, et donc intégralement clos, de corps des fractions E . L'extension $E \hookrightarrow \mathfrak{K}$ est séparable, et $\mathcal{O}_{\nu_0}(\mathfrak{K})$ est la clôture intégrale de $\mathcal{O}_{\nu_0}(E)$ dans $\mathfrak{K}$. Comme $\mathcal{O}_{\nu_0}(E)$ est principal, l'anneau $\mathcal{O}_{\nu_0}(\mathfrak{K})$ est un $\mathcal{O}_{\nu_0}(E)$ -module libre de rang égal à $[\mathfrak{K} : E]$. Ainsi, on peut trouver $\alpha_{n+1}, \dots, \alpha_s$ dans $\mathcal{O}_{\nu_0}(\mathfrak{K})$ tels que, si l'on note encore $\alpha = (\alpha_1, \dots, \alpha_s)$, on ait l'égalité

$$(27) \quad \mathcal{O}_{\nu_0}(\mathfrak{K}) = \mathcal{O}_{\nu_0}(E)[\alpha_1, \dots, \alpha_s] = \mathcal{O}_{\nu_0}(E)[\alpha].$$

On note $\mathfrak{P}$ l'idéal de définition du point $\alpha = (\alpha_1, \dots, \alpha_s)$ dans l'anneau de polynômes $R = \mathcal{O}_{\nu_0}(E)[X_1, \dots, X_s] = \mathcal{O}_{\nu_0}(E)[\mathbf{X}]$.

$$(28) \quad \mathfrak{P} = \{P \in \mathcal{O}_{\nu_0}(E)[\mathbf{X}], P(\alpha) = 0\}.$$

On reprend la démonstration de [AD] pour prouver que l'idéal $\mathfrak{P}^{T_0}$ est primaire. Soit $\mathfrak{m}$ un idéal maximal de R contenant $\mathfrak{P}$. On montre tout d'abord que l'idéal

$$(\mathfrak{P}.R_{\mathfrak{m}})^{T_0} = \mathfrak{P}^{T_0}.R_{\mathfrak{m}}$$

est primaire dans $R_{\mathfrak{m}}$. L'anneau $R_{\mathfrak{m}}$ est local. Il est de plus régulier : en effet, on pose $\mathfrak{m}_0 = \mathfrak{m} \cap \mathcal{O}_{\nu_0}(E)$. Comme $\mathfrak{m}$ est maximal, $\mathfrak{m}_0$ l'est aussi ; c'est donc l'unique idéal maximal de $\mathcal{O}_{\nu_0}(E)$. Ainsi, on a l'égalité $(\mathcal{O}_{\nu_0}(E))_{\mathfrak{m}_0} = \mathcal{O}_{\nu_0}(E)$ et cet anneau est régulier (car de valuation discrète). D'après le corollaire (14.8) de [Na], on a bien la propriété suivante.

$$R_{\mathfrak{m}} = (\mathcal{O}_{\nu_0}(E)[\mathbf{X}])_{\mathfrak{m}} \text{ est régulier.}$$

On montre maintenant que l'anneau $R_{\mathfrak{m}}/\mathfrak{P}R_{\mathfrak{m}}$ est principal. Ceci vient essentiellement de l'égalité $\mathcal{O}_{\nu_0}(\mathfrak{K}) = \mathcal{O}_{\nu_0}(E)[\alpha_1, \dots, \alpha_s]$. Soit $\mathcal{I}$ un idéal de R contenant strictement $\mathfrak{P}$. On note

$$N = \{w_0(P(\alpha)), P \in \mathcal{I} \setminus \mathfrak{P}\}.$$

Cet ensemble possède un élément minimal non nul : soit $P_0 \in \mathcal{I} \setminus \mathfrak{P}$ tel que $w_0(P_0(\alpha))$ soit minimal. Soit $P \in \mathcal{I}$, alors $w_0(P(\alpha).(P_0(\alpha))^{-1}) \geq 0$, et donc $P(\alpha).(P_0(\alpha))^{-1} \in \mathcal{O}_{\nu_0}(\mathfrak{K})$.

Il existe donc $H \in R$ tel que

$$P(\alpha).(P_0(\alpha))^{-1} = H(\alpha).$$

Ainsi, $P - P_0H$ appartient à l'idéal $\mathfrak{P}$, et donc on a $P \equiv P_0H \pmod{\mathfrak{P}}$. L'idéal $\mathcal{I} \bmod \mathfrak{P}$ est principal, par suite

$$R/\mathfrak{P} \text{ est principal.}$$

D'autre part, les idéaux de $R_{\mathfrak{m}}/\mathfrak{P}R_{\mathfrak{m}}$ sont les idéaux contenant $\mathfrak{P}$ et inclus dans $\mathfrak{m}$, donc sont principaux. Ainsi, $R_{\mathfrak{m}}/\mathfrak{P}R_{\mathfrak{m}}$ est principal. Il est de plus clairement local et donc

$$R_{\mathfrak{m}}/\mathfrak{P}R_{\mathfrak{m}} \text{ est un anneau de valuation discrète.}$$

Il est donc a fortiori régulier. D'après un théorème de Chevalley ([ZS] chapitre 8, théorème 26, page 303), il existe un système de paramètres $(z_1, \dots, z_r)$ engendrant $\mathfrak{m}R_{\mathfrak{m}}$, et un entier $l \leq r$ tels que $\mathfrak{P}R_{\mathfrak{m}}$ est l'idéal engendré par $z_1, \dots, z_l$ dans $R_{\mathfrak{m}}$. Ce système est une suite régulière, on en déduit que l'idéal $\mathfrak{P}^{T_0}$ est primaire dans $R_{\mathfrak{m}}$ (voir [ZS] corollaire 2, page 399, lemme 5, page 401). Ceci étant vrai pour tout idéal maximal $\mathfrak{m}$ contenant $\mathfrak{P}$, on en déduit que $\mathfrak{P}^{T_0}$ est primaire dans $\mathcal{O}_{\nu_0}(E)[\mathbf{X}]$.

En effet, soient $c, x \in R$ tels que $cx \in \mathfrak{P}^{T_0}$, et $c \notin \mathfrak{P}$. Alors, pour tout idéal maximal $\mathfrak{m}$ contenant $\mathcal{P}$, $cx \in (\mathfrak{P}R_{\mathfrak{m}})^{T_0} = \mathfrak{P}^{T_0}R_{\mathfrak{m}}$, et $c \notin \mathfrak{P}R_{\mathfrak{m}}$ (sinon, il existerait $m \notin \mathfrak{m}$ tel que $mc \in \mathfrak{P}$ ce qui est impossible). Comme $\mathfrak{P}^{T_0}R_{\mathfrak{m}}$ est primaire, $x \in \mathfrak{P}^{T_0}R_{\mathfrak{m}}$. D'autre part, si $\mathfrak{m}$ est un idéal maximal ne contenant pas $\mathfrak{P}$, alors il ne contient pas $\mathfrak{P}^{T_0}$, et donc $\mathfrak{P}^{T_0}R_{\mathfrak{m}} = R_{\mathfrak{m}}$. Ainsi, on vient de montrer

$$x \in \bigcap_{\mathfrak{m} \text{ max.}} \mathfrak{P}^{T_0}R_{\mathfrak{m}}.$$

On prouve pour terminer, que cette intersection est égale à $\mathfrak{P}^{T_0}$. En effet, soit x un élément de $\bigcap_{\mathfrak{m} \text{ max.}} \mathfrak{P}^{T_0}R_{\mathfrak{m}}$. On pose $D_x = \{a \in R, ax \in \mathfrak{P}^{T_0}\}$. Pour tout idéal maximal $\mathfrak{m}$, il existe $m \in R \setminus \mathfrak{m}$, tel que $mx \in \mathfrak{P}^{T_0}$, c'est-à-dire que pour tout idéal maximal $\mathfrak{m}$, $D_x \not\subseteq \mathfrak{m}$. Ainsi, $D_x = R$ et $x \in \mathfrak{P}^{T_0}$. L'inclusion inverse, bien qu'inutile ici, est évidente. Finalement, on est arrivé au résultat suivant

$$\mathfrak{P}^{T_0} \text{ est } \mathfrak{P}\text{-primaire.}$$

Soit maintenant pour $j = 1, \dots, \delta = [\mathfrak{K} : E]$ l'idéal

$$(29) \quad \mathfrak{M}_j = (X_1 - s_j(\alpha_1), \dots, X_s - s_j(\alpha_s)),$$

où l'on a noté $s_1, \dots, s_\delta$ les E -isomorphismes du corps $\mathfrak{K} = E(\alpha)$ (ils sont distincts car $\mathfrak{K}$ est séparable sur E). C'est l'idéal (maximal) de définition de $s_j(\alpha)$ dans $\overline{E}[\mathbf{X}] = \overline{k}[\mathbf{X}]$.

Alors, puisque α est séparable sur E , on a (voir paragraphe 2) les égalités

$$\mathfrak{P}.\bar{k}[\mathbf{X}] = \bigcap_{j=1}^{\delta} \mathfrak{M}_j = \prod_{j=1}^{\delta} \mathfrak{M}_j.$$

Comme l'application e_{Φ} est un isomorphisme local, le polynôme F_0 s'annule à l'ordre au moins T_0 en α , et est à coefficients dans E , donc

$$F_0 \in (\mathfrak{P}.\bar{E}[\mathbf{X}])^{T_0} \bigcap E[\mathbf{X}].$$

D'après les relations entre extension et contraction des idéaux dans les anneaux de polynômes sur un corps (voir [ZS], chapitre 7, paragraphe 11, page 221), on a l'égalité suivante

$$(\mathfrak{P}.\bar{E}[\mathbf{X}])^{T_0} \bigcap E[\mathbf{X}] = (\mathfrak{P}^{T_0}.\bar{E}[\mathbf{X}]) \bigcap E[\mathbf{X}] = \mathfrak{P}^{T_0}.E[\mathbf{X}].$$

Il existe donc un élément $a \neq 0$ de $\mathcal{O}_{\nu_0}(E)$ tel que $aF_0 \in \mathfrak{P}^{T_0}$. Comme l'idéal $\mathfrak{P}^{T_0}$ est primaire, et puisque a n'est pas dans $\mathfrak{P}$, on obtient que $F_0 \in \mathfrak{P}^{T_0}$. On peut donc écrire

$$(30) \quad F_0 = \sum_{i \in \mathbb{N}^{T_0}} f_{i_1} \cdots f_{i_{T_0}},$$

où les f_{i_j} sont des éléments de $\mathfrak{P}$.

De plus, on a les congruences suivantes

$$\begin{aligned} f_{i_j}(e_{\Phi}(d\Phi_{\nu_0}(\mathbf{u}))) &= f_{i_j}(\Phi_{\nu_0}(e_{\Phi}(\mathbf{u}))), \\ &\equiv f_{i_j}\left((e_{\Phi}(\mathbf{u}))^{q^{d \deg \nu_0}}\right) \pmod{\nu_0} \quad \text{d'après } (\mathcal{H}_{\nu_0}). \end{aligned}$$

D'autre part, on sait que les polynômes f_{i_j} sont à coefficients ν_0 -entiers. Or, on a l'inclusion $\mathcal{O}_{\nu_0}(E) / (\nu_0 \mathcal{O}_{\nu_0}(E)) \subset \mathbb{F}_{q^{d \deg \nu_0}}$, ainsi

$$\begin{aligned} f_{i_j}\left((e_{\Phi}(\mathbf{u}))^{q^{d \deg \nu_0}}\right) &\equiv \left(f_{i_j}(e_{\Phi}(\mathbf{u}))\right)^{q^{d \deg \nu_0}} \pmod{\nu_0}, \\ &\equiv 0 \pmod{\nu_0}. \end{aligned}$$

Alors, puisque l'on a la relation

$$G(d\Phi_{\nu_0}(\mathbf{u}) + \mathbf{z}) = \sum_{i \in \mathbb{N}^{T_0}} f_{i_1}\left(e_{\Phi}(\mathbf{z}) + e_{\Phi}(d\Phi_{\nu_0}(\mathbf{u}))\right) \cdots f_{i_{T_0}}\left(e_{\Phi}(\mathbf{z}) + e_{\Phi}(d\Phi_{\nu_0}(\mathbf{u}))\right),$$

on obtient la minoration

$$w_0\left(G^{(\tau)}(d\Phi_{\nu_0}(\mathbf{u}))\right) \geq T_0 - |\tau|.$$

On suppose maintenant que $\alpha_1, \dots, \alpha_n$ ne sont plus tous ν_0 -entiers, alors les nombres

$$\alpha_1 \nu_0^{\max\{0, -w_0(\alpha_1)\}}, \dots, \alpha_n \nu_0^{\max\{0, -w_0(\alpha_n)\}}$$

le sont. Aussi, on peut reprendre la démonstration précédente avec ces nouveaux nombres entiers, et en remplaçant $G(z)$ par $\nu_0^\rho G(z)$, où :

$$(31) \quad \rho = (1 + |\mu|^d) L |\nu_0|^d \max\{0, -w_0(\alpha_1), \dots, -w_0(\alpha_n)\}.$$

Soit M une matrice $n \times n$ de déterminant inversible dans $\mathcal{O}_{\nu_0}(E)$. Alors, pour tout $\mathbf{x} \in E^n$, on a la majoration

$$\|M \cdot \mathbf{x}\|_{w_0} \leq \|\mathbf{x}\|_{w_0}.$$

Comme M^{-1} est aussi à coefficients dans $\mathcal{O}_{\nu_0}(E)$, on a l'inégalité inverse et donc l'égalité. On applique ce résultat à la matrice coefficient devant $\mathcal{F}^{d \deg \nu_0}$ de Φ_{ν_0} .

$$\Phi_{\nu_0}(\mathbf{X}) = \begin{pmatrix} P_1(\mathbf{X}) \\ \vdots \\ P_n(\mathbf{X}) \end{pmatrix} + M \cdot \begin{pmatrix} X_1^{|\nu_0|^d} \\ \vdots \\ X_n^{|\nu_0|^d} \end{pmatrix},$$

où les P_i sont des polynômes à coefficients dans $\mathcal{O}_{\nu_0}(E)$ de degré $\leq q^{d \deg \nu_0 - 1}$. Comme les α_i ne sont pas tous ν_0 -entiers on a

$$\forall i = 1, \dots, n, \quad |P_i(\alpha)|_{w_0} < \|\alpha\|_{w_0}^{|\nu_0|^d}.$$

Et donc, finalement on a l'égalité

$$\|\Phi_{\nu_0}(\alpha)\|_{w_0} = \|\alpha\|_{w_0}^{|\nu_0|^d}.$$

On montre de la même façon $\|\Phi_{\nu_0 \mu}(\alpha)\|_{w_0} = \|\alpha\|_{w_0}^{|\nu_0|^d |\mu|^d}$. De ces relations, on tire

$$\rho = \frac{L}{\deg \nu_0} \left(\log_q \|\Phi_{\nu_0}(\alpha)\|_{w_0} + \log_q \|\Phi_{\nu_0 \mu}(\alpha)\|_{w_0} \right).$$

Ainsi, on obtient les majorations suivantes.

$$w_0 \left(\nu_0^\rho G^{(\tau)}(d\Phi_{\nu_0}(\mathbf{u})) \right) \geq T_0 - |\tau|,$$

$$w_0 \left(G^{(\tau)}(d\Phi_{\nu_0}(\mathbf{u})) \right) \geq T_0 - |\tau| - \rho,$$

$$\geq T_0 - |\tau| - \frac{1}{\deg \nu_0} \left(L \log_q \|\Phi_{\nu_0}(\alpha)\|_{w_0} + L \log_q \|\Phi_{\nu_0 \mu}(\alpha)\|_{w_0} \right).$$

Et finalement, on a démontré l'inégalité

$$\left| G^{(\tau)}(d\Phi_{\nu_0}(\mathbf{u})) \right|_{w_0} \leq q^{-(T_0 - |\tau|) \deg \nu_0} \|\Phi_{\nu_0}(\alpha)\|_{w_0}^L \|\Phi_{\nu_0 \mu}(\alpha)\|_{w_0}^L,$$

d'où le résultat annoncé. □

5 - Lemme de zéros

On considère un T -module Φ de dimension n défini sur E . Soient $\alpha = (\alpha_1, \dots, \alpha_n)$ un point de $\mathbb{G}_a^n(\overline{E})$, et $N_1, \dots, N_n$ des entiers non nuls. Pour $j = 1, \dots, n$ on fixe aussi des ensembles $\mathcal{P}_j$ vérifiant

$$1 \in \mathcal{P}_j \subset \{a \in A, \deg a \leq N_j\}.$$

On définit encore :

$$\Sigma_j = \{\Phi_{a_j \dots a_n}(\sigma(\alpha)), (a_j, \dots, a_n) \in \mathcal{P}_j \times \dots \times \mathcal{P}_n, \sigma \in \text{Aut}(\overline{E}/E)\}, \text{ si } j = 1, \dots, n,$$

$$\Sigma_{n+1} = \{\sigma(\alpha), \sigma \in \text{Aut}(\overline{E}/E)\}.$$

Ainsi, pour $j = 1, \dots, n$ et $a \in \mathcal{P}_j$, on a

$$\Phi_a(\Sigma_{j+1}) \subset \Sigma_j.$$

Pour $j = 2, \dots, n$, on notera $\mathcal{Q}_j = \{a_1 \dots a_{j-1}, a_i \in \mathcal{P}_i\}$.

Soient enfin $T_1, \dots, T_n$ des entiers strictement positifs. On se propose de montrer le lemme de zéros suivant.

Proposition 15. *Soit $F_0 \in E[X_1, \dots, X_n]$ un polynôme non nul de degré $\leq L_0$, s'annulant à l'ordre au moins $T_1 + \dots + T_n + 1$ sur Σ_1 . Il existe un entier $r \in \{1, \dots, n\}$ et une $\overline{E}$ -variété V rencontrant Σ_{r+1} et de codimension $\leq r$, telle que*

$$T_r^{\text{codim} V} \deg \left(\bigcup_{\substack{\sigma \in \text{Aut}(\overline{E}/E), \\ a \in \mathcal{P}_r}} \Phi_a(\sigma(V)) \right) \leq (L_0 N_1 \dots N_{r-1})^{\text{codim} V}.$$

Il est nécessaire de tenir compte de la multiplicité T_r dans la démonstration du théorème C. Cependant, il est démontré en annexe un résultat similaire ne faisant pas intervenir cette multiplicité, mais dans lequel la majoration obtenue est plus fine.

Preuve - On suit la preuve du théorème 1.4 de [DH]. Cependant, ici à cause de phénomènes d'inséparabilité, on n'obtient pas de supplément galoisien : en effet, la variété V construite n'est pas nécessairement géométriquement réduite.

Pour alléger les notations, on écrira encore F_0 son polynôme homogénéisé

$$X_0^{\deg F_0} F_0 \left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0} \right),$$

et α le point projectif $(1, \alpha_1, \dots, \alpha_n)$. On construit une suite d'idéaux homogènes emboîtés $(\mathcal{I}_r)_{r=1, \dots, n+1}$ de $\overline{\mathcal{A}} = \overline{E}[\mathbf{X}] = \overline{E}[X_0, \dots, X_n]$. Soit $\tau \in \mathbb{N}^n$, l'opérateur $\Delta^{(\tau)}$ est défini par le développement

$$(32) \quad F(\mathbf{X} + e_\Phi(\mathbf{z})) = \sum_{\tau \in \mathbb{N}^n} \Delta^{(\tau)} F(\mathbf{X}) \mathbf{z}^\tau.$$

Pour $a \in A$ et $\tau \in \mathbb{N}^n$, on définit encore l'opérateur $\mathcal{D}_a^{(\tau)}$ par

$$(33) \quad \mathcal{D}_a^{(\tau)} F = \Delta^{(\tau)} (F \circ \Phi_a).$$

Si $\mathcal{I} \subset \overline{E}[\mathbf{X}]$ est un idéal, et si N est un entier, on notera aussi

$$(34) \quad \mathcal{D}_a^N(\mathcal{I}) = (\mathcal{D}_a^{(\tau)}P, \tau \in \mathbb{N}^n, |\tau| < N, P \in \mathcal{I}).$$

On pose alors

$$(35) \quad \begin{aligned} \mathcal{I}_1 &= (F_0), \\ \mathcal{I}_{j+1} &= (\mathcal{D}_a^{T_j}(\mathcal{I}_j), a \in \mathcal{P}_j) \text{ si } j = 1, \dots, n. \end{aligned}$$

On note $\mathcal{X}_j$ l'ensemble algébrique défini par $\mathcal{I}_j$, et $\mathcal{Y}_j$ le sous ensemble algébrique de $\mathcal{X}_j$ formé des $\overline{E}$ -composantes isolées de $\mathcal{X}_j$ rencontrant Σ_j .

Dans un premier temps, on montre par récurrence, que tout polynôme de $\mathcal{I}_j$ s'annule à l'ordre au moins $T_j + \dots + T_n + 1$ en les points de Σ_j . Par hypothèse sur F_0 , c'est vrai au rang 1; on suppose l'avoir démontré pour $\mathcal{I}_j$. Soit $\alpha' \in \Sigma_{j+1}$, alors pour tout $a \in \mathcal{P}_j$, $\Phi_a(\alpha')$ appartient à Σ_j . Soit $P \in \mathcal{I}_j$, $a \in \mathcal{P}_j$ et $\tau \in \mathbb{N}^n$ tel que $|\tau| \leq T_j + \dots + T_n$, alors on a

$$(\Delta^{(\tau)}P)(\Phi_a(\alpha')) = 0.$$

D'autre part, on a les développements suivants.

$$\begin{aligned} (P \circ \Phi_a)(\mathbf{X} + e_\Phi(\mathbf{y}) + e_\Phi(\mathbf{z})) &= \sum_{\tau_1 \in \mathbb{N}^n} \Delta^{(\tau_1)}(P \circ \Phi_a)(\mathbf{X} + e_\Phi(\mathbf{y}))\mathbf{z}^{\tau_1} \\ &= \sum_{\tau_1, \tau_2 \in \mathbb{N}^n} \Delta^{(\tau_2)}(\Delta^{(\tau_1)}(P \circ \Phi_a))(\mathbf{X})\mathbf{y}^{\tau_2}\mathbf{z}^{\tau_1} \\ P(\Phi_a(\mathbf{X}) + e_\Phi(d\Phi_a(\mathbf{y} + \mathbf{z}))) &= \sum_{\tau \in \mathbb{N}^n} (\Delta^{(\tau)}P)(\Phi_a(\mathbf{X}))(d\Phi_a(\mathbf{y} + \mathbf{z}))^\tau \end{aligned}$$

Ces deux développements sont égaux; en les spécialisant en $\mathbf{X} = \alpha'$, on obtient pour tout $\tau_1, \tau_2 \in \mathbb{N}^n$, l'implication

$$|\tau_1| + |\tau_2| \leq T_j + \dots + T_n \implies \Delta^{(\tau_2)}(\Delta^{(\tau_1)}(P \circ \Phi_a))(\alpha') = 0.$$

Les générateurs de $\mathcal{I}_{j+1}$ sont de la forme $\mathcal{D}_a^{(\tau_1)}P$ où $P \in \mathcal{I}_j$, $a \in \mathcal{P}_j$, $\tau_1 \in \mathbb{N}^n$ tel que $|\tau_1| < T_j$. Ainsi, pour tout $\tau_2 \in \mathbb{N}^n$ tel que $|\tau_2| \leq T_{j+1} + \dots + T_n$, on a l'égalité

$$\Delta^{(\tau_2)}(\mathcal{D}_a^{(\tau_1)}P)(\alpha') = 0.$$

Donc $\mathcal{I}_{j+1}$ s'annule à l'ordre au moins $T_{j+1} + \dots + T_n + 1$ sur Σ_{j+1} .

En conséquence, on obtient l'inclusion $\Sigma_j \subset \mathcal{X}_j$, et donc les ensembles algébriques $\mathcal{Y}_j$ ne sont pas trivialement vides. Soit V une composante de $\mathcal{Y}_{j+1}$, alors $\mathcal{X}_j$ contient V , et puisque Σ_{j+1} est un sous-ensemble de Σ_j , la variété V rencontre Σ_j . Ainsi V est contenue dans une composante isolée de $\mathcal{X}_j$ rencontrant Σ_j et est donc incluse dans $\mathcal{Y}_j$. On en déduit les inclusions suivantes.

$$\mathcal{Y}_{n+1} \subset \mathcal{Y}_n \subset \dots \subset \mathcal{Y}_1$$

Par le principe des tiroirs, il existe donc un indice r , que l'on choisit maximal, pour lequel $\dim \mathcal{Y}_r = \dim \mathcal{Y}_{r+1} = d_r$. On a ainsi $n - d_r \leq r$. Soit V une composante irréductible de dimension d_r de $\mathcal{Y}_{r+1}$. Comme V est une composante de $\mathcal{X}_r$ elle est définie par des formes de degré $\leq L_0 N_1 \cdots N_{r-1}$. Soit x un élément de $\Sigma_{r+1} \cap V$. Alors $\Phi_a(x)$ appartient à $\Sigma_r \cap \Phi_a(V)$, et donc $\Phi_a(V)$ est contenue dans $\mathcal{Y}_r$. Comme de plus, les ensembles algébriques V , $\Phi_a(V)$ et $\mathcal{Y}_r$ sont de même dimension d_r , alors $\Phi_a(V)$ est une composante isolée de $\mathcal{Y}_r$. On note $\mathcal{R}_a$ l'idéal de définition de $\Phi_a(V)$. On va montrer l'inclusion

$$\mathcal{D}_1^{T_r}(\mathcal{I}_r) \subset \mathcal{R}_a.$$

Il revient au même de montrer $\mathcal{D}_a^0 \circ \mathcal{D}_1^{T_r}(\mathcal{I}_r) \subset \mathcal{R}$, où $\mathcal{R}$ est l'idéal de V . Soit $P \in \mathcal{I}_r$. Comme précédemment, on a

$$\begin{aligned} (P \circ \Phi_a)(\mathbf{X} + e_\Phi(\mathbf{z})) &= \sum_{\tau \in \mathbb{N}^n} \Delta^{(\tau)}(P \circ \Phi_a)(\mathbf{X}) \mathbf{z}^\tau, \\ &= \sum_{\tau \in \mathbb{N}^n} \mathcal{D}_a^{(\tau)}(P)(\mathbf{X}) \mathbf{z}^\tau, \\ P(\Phi_a(\mathbf{X}) + e_\Phi(d\Phi_a(\mathbf{z}))) &= \sum_{\tau \in \mathbb{N}^n} \Delta^{(\tau)} P(\Phi_a(\mathbf{X})) (d\Phi_a(\mathbf{z}))^\tau. \end{aligned}$$

Comme précédemment, ces développements sont égaux, et donc $\mathcal{D}_a^{(\tau)}(P)(\mathbf{X})$ est combinaison linéaire à coefficients dans E de $\Delta^{(\tau')} P(\Phi_a(\mathbf{X}))$, et donc

$$\mathcal{D}_a^{T_r}(\mathcal{I}_r) \subset \mathcal{D}_a^0 \circ \mathcal{D}_1^{T_r}(\mathcal{I}_r).$$

Comme la matrice $d\Phi_a$ est inversible, on a aussi l'inclusion inverse

$$\mathcal{D}_a^0 \circ \mathcal{D}_1^{T_r}(\mathcal{I}_r) \subset \mathcal{D}_a^{T_r}(\mathcal{I}_r) \subset \mathcal{I}_{r+1}.$$

Enfin, on tire de $V \subset \mathcal{Y}_{r+1} \subset \mathcal{X}_{r+1}$, l'inclusion $\mathcal{I}_{r+1} \subset \mathcal{R}$, d'où le résultat annoncé.

Ici, puisque l'on travaille avec un corps de base algébriquement clos, les résultats de P. Philippon sont utilisables. Les lemmes 4 et 7 de [P2] montrent la minoration suivante

$$e_{\mathcal{I}_r \overline{\mathcal{A}}_{\mathcal{R}_a}}(\overline{\mathcal{A}}_{\mathcal{R}_a}) \geq T_r^{\text{codim} V},$$

où $e_{\mathcal{I}_r \overline{\mathcal{A}}_{\mathcal{R}_a}}(\overline{\mathcal{A}}_{\mathcal{R}_a})$ est la multiplicité de $\overline{\mathcal{A}}_{\mathcal{R}_a}$ relativement à l'idéal $\mathcal{I}_r \overline{\mathcal{A}}_{\mathcal{R}_a}$. On conclut, en appliquant le lemme 5 de [P2], que l'on a la majoration

$$T_r^{\text{codim} V} \deg \left(\bigcup_{\substack{a \in \mathcal{P}_r, \\ \sigma \in \text{Aut}(\overline{E}/E)}} \Phi_a(\sigma(V)) \right) \leq (L_0 N_1 \cdots N_{r-1})^{\text{codim} V}. \quad \square$$

6 - Fonction auxiliaire

6.1. Majoration du rang

Soit $\alpha \in \mathbb{G}_a^n(\bar{k})$, on se donne $\mathbf{u} = (u_1, \dots, u_n) \in \mathcal{C}^n$ tel que $\alpha = e_\Phi(\mathbf{u})$ (ce qui est possible car e_Φ est supposée surjective). Soit $\mu \in A$ irréductible et unitaire. On veut construire un polynôme $F(X_1, \dots, X_n, Y_1, \dots, Y_n) = F(\mathbf{X}, \mathbf{Y})$ à coefficients dans A , vérifiant

$$\deg_{\mathbf{X}} F \leq L \quad \text{et} \quad \deg_{\mathbf{Y}} F \leq L,$$

et tel que la fonction

$$G(\mathbf{z}) = G(z_1, \dots, z_n) = F(e_\Phi(\mathbf{z}), \Phi_\mu(e_\Phi(\mathbf{z})))$$

s'annule à l'ordre au moins T_0 en $\mathbf{u}$.

On a donc à résoudre un système linéaire $(\mathcal{S})$ à coefficients dans $\mathfrak{K} = E(\alpha)$, de dimension $M \times N$, où $M = \binom{L+n}{n}^2$ est le nombre d'inconnues, et $N = \binom{T_0+n}{n}$ est le nombre d'équations. On commence tout d'abord par majorer le rang de ce système linéaire (sur E). Pour cela, on s'inspire de la preuve de [DH], à laquelle on apporte quelques modifications. En effet, pour éviter de « composer » les opérateurs de dérivation, on a recours aux puissances symboliques d'idéaux, qui traduisent, lorsque le corps est algébriquement clos, l'ordre d'annulation sur la variété définissant l'idéal en question.

On note $\mathcal{A} = E[\mathbf{X}] = E[X_1, \dots, X_n]$, et $\mathcal{A}' = E[\mathbf{X}, \mathbf{Y}] = E[X_1, \dots, X_n, Y_1, \dots, Y_n]$. Soit $F(\mathbf{X}, \mathbf{Y}) \in \mathcal{C}[\mathbf{X}, \mathbf{Y}]$, on élargit la définition des opérateurs $\Delta^{(\tau)}$ par l'égalité

$$(36) \quad \forall \mathbf{z} \in \mathcal{C}^n, \quad F(\mathbf{X} + e_\Phi(\mathbf{z}), \mathbf{Y} + \Phi_\mu(e_\Phi(\mathbf{z}))) = \sum_{\tau \in \mathbb{N}^n} \Delta^{(\tau)} F(\mathbf{X}, \mathbf{Y}) z_1^{\tau_1} \cdots z_n^{\tau_n}.$$

On veut construire $F \in k[\mathbf{X}, \mathbf{Y}]$ telle que l'on ait

$$(\mathcal{S}_0) \quad \Delta^{(\tau)} F(\alpha, \Phi_\mu(\alpha)) = 0, \quad \forall \tau \in \mathbb{N}^n, \quad |\tau| \leq T_0 - 1.$$

On considère l'application suivante.

$$(37) \quad i : \begin{cases} \mathbb{G}_a^n & \longrightarrow \mathbb{G}_a^n \times \mathbb{G}_a^n \\ x & \longmapsto (x, \Phi_\mu(x)) \end{cases}$$

Pour $u = (\mathbf{v}, \Phi_\mu(\mathbf{v})) = i(\mathbf{v})$, on note $\mathbf{t}_u$ la translation

$$(38) \quad \mathbf{t}_u : \begin{cases} \mathcal{A}' & \longrightarrow \mathcal{A}', \\ P(\mathbf{X}, \mathbf{Y}) & \longmapsto P(\mathbf{X} + \mathbf{v}, \mathbf{Y} + \Phi_\mu(\mathbf{v})). \end{cases}$$

Soit V une $\bar{E}$ -variété de $\mathbb{G}_a^n$ - c'est-à-dire un ensemble algébrique irréductible défini sur $\bar{E}$ - passant par α . On note ν sa dimension. Alors, $i(V)$ est aussi de dimension ν . Soit $\bar{\mathcal{P}}$ l'idéal de définition de $i(V)$ dans $\bar{E}[\mathbf{X}, \mathbf{Y}]$. On considère le système suivant.

$$(\mathcal{S}_1) \quad \Delta_u^{(\tau)} F \in \mathbf{t}_{-u}(\bar{\mathcal{P}}), \quad \forall u \in i(V), \quad \forall \tau \in \mathbb{N}^n, \quad |\tau| \leq T_0 - 1,$$

où si $u = (\mathbf{v}, \Phi_\mu(\mathbf{v}))$, les $\Delta_u^{(\tau)} F$ sont déterminés par le développement

$$\forall \mathbf{z} \in \mathcal{C}^n, \quad F(\mathbf{X} - \mathbf{v} + e_\Phi(\mathbf{z}), \mathbf{Y} - \Phi_\mu(\mathbf{v}) + \Phi_\mu(e_\Phi(\mathbf{z}))) = \sum_{\tau \in \mathbb{N}^n} \Delta_u^{(\tau)} F(\mathbf{X}, \mathbf{Y}) z_1^{\tau_1} \cdots z_n^{\tau_n}.$$

Il est clair que toute solution de $(\mathcal{S}_1)$ est aussi solution de $(\mathcal{S}_0)$. En effet, si l'on choisit $u = i(\alpha)$, alors les éléments de $\mathfrak{t}_{-i(\alpha)}(\overline{\mathcal{P}})$ sont annulés par $i(0)$ et donc

$$\Delta_{i(\alpha)}^{(\tau)} F(i(0)) = \Delta^{(\tau)} F(i(\alpha)) = 0.$$

On construit maintenant les opérateurs de dérivation dans la direction d'un plan tangent à V . On notera $(e_1, \dots, e_n)$ la base canonique de $\mathbb{G}_a^n$. Soit $i(x) \in i(V)$. Le « plan » tangent à $i(V)$ en $i(x)$ est déterminé par les équations suivantes.

$$(39) \quad \mathbb{T}_x : \sum_{|\tau|=1} \Delta^{(\tau)} P(i(x)) (\mathbf{z} - i(x))^\tau = 0, \quad \forall P \in \overline{\mathcal{P}}.$$

De plus, pour $i(x)$ dans un certain ouvert de Zariski Ω_0 de $i(V)$, on peut supposer que $\mathbb{T}_x$ est un espace de dimension ν . Quitte à renuméroter les indices, on peut supposer qu'il existe un ouvert $\Omega_1 \subset \Omega_0$, tel que pour tout $i(x) \in \Omega_1$, la famille $e_{\nu+1}, \dots, e_n$ se complète en une base de $\mathbb{G}_a^n$, à l'aide d'une base $e_1(x), \dots, e_\nu(x)$ de l'espace vectoriel associé à $\mathbb{T}_x$. Les changements de coordonnées s'écrivent alors ainsi :

$$\begin{bmatrix} z_1(x) \\ \vdots \\ z_\nu(x) \\ z_{\nu+1}(x) \\ \vdots \\ z_n(x) \end{bmatrix} = \begin{bmatrix} a_{1,1} & \dots & a_{1,\nu} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & 0 & \dots & 0 \\ \vdots & & \vdots & 1 & & \\ \vdots & & \vdots & & \ddots & \\ a_{n,1} & \dots & a_{n,\nu} & & & 1 \end{bmatrix} \begin{bmatrix} z_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ z_n \end{bmatrix},$$

$$\begin{bmatrix} z_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} b_{1,1} & \dots & b_{1,\nu} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & 0 & \dots & 0 \\ \vdots & & \vdots & 1 & & \\ \vdots & & \vdots & & \ddots & \\ b_{n,1} & \dots & b_{n,\nu} & & & 1 \end{bmatrix} \begin{bmatrix} z_1(x) \\ \vdots \\ z_\nu(x) \\ z_{\nu+1}(x) \\ \vdots \\ z_n(x) \end{bmatrix},$$

ou encore $\mathbf{z}(x) = A(x)\mathbf{z}$ et $\mathbf{z} = B(x)\mathbf{z}(x) = A(x)^{-1}\mathbf{z}(x)$, les matrices $A(x)$ et $B(x)$ étant à coefficients dans E . Soit $i(x) \in \Omega_1$.

$$\begin{aligned} F(\mathbf{X} + e_\Phi(\mathbf{z}) - \mathbf{v}, \mathbf{Y} + \Phi_\mu(e_\Phi(\mathbf{z}) - \mathbf{v})) &= \sum_{\tau \in \mathbb{N}^n} \Delta_u^{(\tau)} F(\mathbf{X}, \mathbf{Y}) z_1^{\tau_1} \cdots z_n^{\tau_n}, \\ &= \sum_{\tau' \in \mathbb{N}^n} \Delta_u^{x,(\tau')} F(\mathbf{X}, \mathbf{Y}) z_1^{\tau'_1}(x) \cdots z_n^{\tau'_n}(x). \end{aligned}$$

Or, si τ est un élément de $\mathbb{N}^n$, alors on a une égalité de la forme suivante.

$$\begin{aligned} z_1^{\tau_1} \cdots z_n^{\tau_n} &= \prod_{j=1}^{\nu} \left(\sum_{i=1}^{\nu} b_{j,i} z_i(x) \right)^{\tau_j} \prod_{j=\nu+1}^n \left(z_j(x) + \sum_{i=1}^{\nu} b_{j,i} z_i(x) \right)^{\tau_j}, \\ &= \sum_{\substack{|\tau|=|\tau'|, \\ \tau_i \geq \tau'_i, \quad i=\nu+1, \dots, n}} B_{\tau}^x z_1^{\tau'_1}(x) \cdots z_n(x)^{\tau'_n}. \end{aligned}$$

On obtient donc la relation

$$\Delta_u^{x,(\tau')} F = \sum_{\substack{|\tau|=|\tau'|, \\ \tau_i \geq \tau'_i, \quad i=\nu+1, \dots, n}} \beta_{\tau}^x \cdot \Delta_u^{(\tau)} F,$$

où les β_{τ}^x sont dans E . On a une formule analogue exprimant les $\Delta_u^{(\tau)} F$ en fonction des $\Delta_u^{x,(\tau')} F$. On note $\mathbf{t}_i$ le n -uplet $(t_{i,1}, \dots, t_{i,n})$ défini par $t_{i,j} = 0$ si $i \neq j$, et par $t_{i,i} = 1$. Soit r un entier, on écrira

$$\Delta_u^{(r, \mathbf{t}_i)} = \partial_{u,i}^r, \quad \Delta_u^{x,(r, \mathbf{t}_i)} = \partial_{u,i}^{x,r}.$$

Soit maintenant $\mathbf{m}_x$ l'idéal de définition de $i(x)$ dans $\overline{E}[\mathbf{X}, \mathbf{Y}]$, alors par construction de $\mathbb{T}_x$, si $F \in \overline{\mathcal{P}}$, on a

$$\text{pour } i = 1, \dots, \nu, \quad \partial_{u,i}^{x,1} F \in \mathbf{t}_{-u}(\mathbf{m}_x).$$

C'est essentiellement cette propriété que l'on va utiliser, pour montrer que le système $(\mathcal{S}_1)$ est équivalent au système suivant.

$$(\mathcal{S}_2) \quad \Delta_u^{(\tau)} F \in \mathbf{t}_{-u}(\overline{\mathcal{P}}), \quad \forall \tau = (0, \dots, 0, \tau_{\nu+1}, \dots, \tau_n) \in \mathbb{N}^n, \quad |\tau| \leq T_0 - 1,$$

où l'on a au préalable fixé $u = i(\mathbf{v})$ dans Ω_1 .

Il est clair que toute solution de $(\mathcal{S}_1)$ est aussi solution de $(\mathcal{S}_2)$. De plus, si pour tout $\tau \in \mathbb{N}^n$ tel que $|\tau| \leq T - 1$, on a $\Delta_u^{(\tau)} F \in \mathbf{t}_{-u}(\overline{\mathcal{P}})$ pour notre u fixé, alors par translation, on obtient la même chose pour tous les autres u de $i(V)$. Soit F une solution de $(\mathcal{S}_2)$. D'après la remarque précédente, pour que F soit solution de $(\mathcal{S}_1)$, il suffit qu'elle vérifie

$$\Delta_u^{(\tau)} F \in \mathbf{t}_{-u}(\overline{\mathcal{P}}), \quad \forall \tau \in \mathbb{N}^n, \quad |\tau| \leq T_0 - 1.$$

Pour $N \in \mathbb{N}$ non nul, et pour $\overline{\mathcal{J}}$ idéal de $\overline{E}[\mathbf{X}, \mathbf{Y}]$, on note

$$(40) \quad \overline{\mathcal{J}}^{<N>} = \{F \in \overline{E}[\mathbf{X}, \mathbf{Y}], \Delta^{(\tau)} F \in \overline{\mathcal{J}}, \forall \tau \in \mathbb{N}^n, |\tau| \leq N - 1\}.$$

Soit N le plus grand entier pour lequel $\mathbf{t}_{-u}(F) \in (\mathbf{t}_{-u}(\overline{\mathcal{P}}))^{<N>}$, on suppose que $N < T_0$. On choisit $\mathbf{N} = (N_1, \dots, N_n) \in \mathbb{N}^n$ tel que $|\mathbf{N}| = N$, et $\Delta_u^{\mathbf{N}} F \notin \mathbf{t}_{-u}(\overline{\mathcal{P}})$, et pour lequel la somme $N_1 + \dots + N_{\nu}$ est minimale. Puisque l'on a $N < T_0$ et que F est solution de $(\mathcal{S}_2)$, alors $N_1 + \dots + N_{\nu}$ n'est pas nul. On convient par exemple que l'on a $N_1 \geq 1$. On pose $G = \Delta_u^{(0, N_2, \dots, N_n)} F$, alors pour tout $r \in \{0, \dots, N_1 - 1\}$ et tout $i(x) \in \Omega_1$, on a

$$\partial_{u,1}^r G \in (\mathbf{t}_{-u}(\overline{\mathcal{P}}))^{<N_1-r>} \subset (\mathbf{t}_{-u}(\mathbf{m}_x))^{<N_1-r>}.$$

Or la fonction e_Φ est un isomorphisme local, et l'idéal $\mathfrak{t}_{-u}(\mathfrak{m}_x)$ est maximal (donc ses puissances symboliques sont aussi ses puissances), ainsi on a les égalités

$$(\mathfrak{t}_{-u}(\mathfrak{m}_x))^{<N_1-r>} = (\mathfrak{t}_{-u}(\mathfrak{m}_x))^{(N_1-r)} = (\mathfrak{t}_{-u}(\mathfrak{m}_x))^{N_1-r},$$

où $(\mathfrak{t}_{-u}(\mathfrak{m}_x))^{(N_1-r)}$ désigne la puissance symbolique $(N_1 - r)$ -ième de $\mathfrak{t}_{-u}(\mathfrak{m}_x)$. D'autre part, l'ouvert Ω_1 étant dense dans $i(V)$, on a :

$$\overline{\mathcal{P}} = \bigcap_{i(x) \in \Omega_1} \mathfrak{m}_x,$$

ainsi, d'après le corollaire 1 de [EH], on a :

$$\partial_{u,1}^r G \in \bigcap_{i(x) \in \Omega_1} (\mathfrak{t}_{-u}(\mathfrak{m}_x))^{N_1-r} \subset (\mathfrak{t}_{-u}(\overline{\mathcal{P}}))^{(N_1-r)},$$

où $(\mathfrak{t}_{-u}(\overline{\mathcal{P}}))^{(N_1-r)}$ est la puissance symbolique $(N_1 - r)$ -ième de $\mathfrak{t}_{-u}(\overline{\mathcal{P}})$. Alors, il existe H n'appartenant pas à $\overline{\mathcal{P}}$, tel que $\mathfrak{t}_{-u}(H) \cdot \partial_{u,1}^0 G \in (\mathfrak{t}_{-u}(\overline{\mathcal{P}}))^{N_1}$. On va voir que cela entraîne que $\partial_{u,1}^{N_1} G \in \mathfrak{t}_{-u}(\overline{\mathcal{P}})$. Pour cela, on utilisera le lemme suivant.

Lemme 4. *Soit g un entier non nul et $J \in \overline{\mathcal{P}}^g$, et soient $r_1, \dots, r_\nu \in \mathbb{N}$ tels que $r_1 + \dots + r_\nu \leq g$. Alors, on a*

$$\partial_{u,1}^{x,r_1} \circ \dots \circ \partial_{u,\nu}^{x,r_\nu} (J) \in \mathfrak{t}_{-u}(\mathfrak{m}_x).$$

Preuve - Il suffit de le montrer pour $J = J_1 \times \dots \times J_g$, où les J_l sont dans $\overline{\mathcal{P}}$. En utilisant la formule de Leibnitz, on montre facilement que l'on a :

$$(2) \quad (\partial_{u,1}^{x,r_1} \circ \dots \circ \partial_{u,\nu}^{x,r_\nu}) (J) \in \mathfrak{t}_{-u}(\overline{\mathcal{P}})^{g-r},$$

où $r = r_1 + \dots + r_\nu$. Ainsi, si $r < g$ le lemme est démontré.

On suppose maintenant que $r = g \geq 1$. A l'aide de (2), on se ramène au cas où seul un des r_s n'est pas nul ; par exemple $r_1 = r \neq 0$, et $r_2 = \dots = r_\nu = 0$.

$$\partial_{u,1}^{x,r} (J_1 \times \dots \times J_r) = \sum_{\substack{|\mathbf{l}|=r \\ \mathbf{l}=(l_1, \dots, l_r)}} C(\mathbf{l}) \left(\partial_{u,1}^{x,l_1} J_1 \right) \dots \left(\partial_{u,1}^{x,l_r} J_r \right).$$

Si l'un des l_s est nul, alors $\partial_{u,1}^{x,l_s} J_s = \mathfrak{t}_{-u}(J_s) \in \mathfrak{t}_{-u}(\overline{\mathcal{P}})$. Si tous les l_s sont non nuls, alors ils sont tous égaux à 1. Comme les J_s sont dans $\overline{\mathcal{P}}$, $\partial_{u,1}^{x,l_s} J_s = \partial_{u,1}^{x,1} J_s$ appartient à $\mathfrak{t}_{-u}(\mathfrak{m}_x)$. Ainsi, tous les termes de la somme sont dans $\mathfrak{t}_{-u}(\mathfrak{m}_x)$, et donc on a

$$\partial_{u,1}^{x,r} (J_1 \times \dots \times J_r) \in \mathfrak{t}_{-u}(\mathfrak{m}_x). \quad \square$$

Par définition de G , on a $\partial_{u,1}^{N_1} G \notin \mathfrak{t}_{-u}(\overline{\mathcal{P}})$. Or, on a l'égalité

$$(3) \quad \partial_{u,1}^{N_1} G = \sum_{|\tau|=N_1} \gamma_\tau \cdot \Delta_u^{x,(\tau)}(G).$$

Soit $\tau \in \mathbb{N}^n$ tel que $|\tau| = N_1$ et $i(x) \in \Omega_1$. On distingue deux cas.

Premier cas : $\tau_{\nu+1} = \dots = \tau_n = 0$.

D'après le lemme précédent, comme $HG \in \overline{\mathcal{P}}^{N_1}$, on a $\Delta_u^{x,(\tau)}(HG) \in \mathfrak{t}_{-u}(\mathfrak{m}_x)$. De plus, la formule de Leibnitz donne

$$\Delta_u^{x,(\tau)}(HG) = \sum_{\rho_1 + \rho_2 = \tau} C_{\tau}^{\rho_1} \cdot \Delta_u^{x,(\rho_1)}(H) \cdot \Delta_u^{x,(\rho_2)}(G).$$

Si $|\rho_2| < N_1$, soit $\rho \in \mathbb{N}^n$ tel que $|\rho| = |\rho_2|$, alors

$$\Delta_u^{(\rho)}G = \Delta_u^{(\rho)} \circ \Delta_u^{(0, N_2, \dots, N_n)}F = c(\rho, \mathbf{N})\Delta_u^{(\rho')}F,$$

où $c(\rho, \mathbf{N})$ est un produit de coefficients binomiaux et $\rho' = \rho + (0, N_2, \dots, N_n)$. Comme $|\rho| < N_1$, alors $|\rho'| < N$ et donc $\Delta_u^{(\rho')}F \in \mathfrak{t}_{-u}(\overline{\mathcal{P}})$. Ainsi $\Delta_u^{(\rho)}G \in \mathfrak{t}_{-u}(\overline{\mathcal{P}})$. Or $\Delta_u^{x,(\rho_2)}G$ est combinaison linéaire des $\Delta_u^{(\rho)}G$ tels que $|\rho| = |\rho_2|$, donc $\Delta_u^{x,(\rho_2)}G \in \mathfrak{t}_{-u}(\overline{\mathcal{P}}) \subset \mathfrak{t}_{-u}(\mathfrak{m}_x)$. Il reste donc

$$\mathfrak{t}_{-u}(H) \cdot \Delta_u^{x,(\tau)}G \in \mathfrak{t}_{-u}(\mathfrak{m}_x).$$

Second cas : il existe $i \in \{\nu + 1, \dots, n\}$ tel que $\tau_i \neq 0$.

Soit $\rho \in \mathbb{N}^n$ tel que $|\rho| = |\tau|$, et tel que pour $i = \nu + 1, \dots, n$ on ait $\rho_i \geq \tau_i$. Alors, nécessairement $\rho_1 + \dots + \rho_{\nu} < N_1 + \dots + N_{\nu}$. Comme précédemment, on a l'égalité $\Delta_u^{(\rho)}G = c(\rho, \mathbf{N})\Delta_u^{(\rho')}F$, où $\rho' = \rho + (0, N_2, \dots, N_n) = (\rho'_1, \dots, \rho'_n)$. On obtient $|\rho'| = N$ et $\rho'_1 + \dots + \rho'_{\nu} < N_1 + \dots + N_{\nu}$. Par choix de $\mathbf{N}$, nécessairement $\Delta_u^{(\rho')}F \in \mathfrak{t}_{-u}(\overline{\mathcal{P}})$ et par suite, $\Delta_u^{(\rho)}G \in \mathfrak{t}_{-u}(\overline{\mathcal{P}})$. Comme dans le premier cas, on a

$$\Delta_u^{x,(\tau)}(G) \in \mathfrak{t}_{-u}(\overline{\mathcal{P}}) \subset \mathfrak{t}_{-u}(\mathfrak{m}_x).$$

En reportant dans l'égalité (3), on obtient :

$$\forall i(x) \in \Omega_1, \quad \mathfrak{t}_{-u}(H) \cdot \partial_{u,1}^{N_1}G \in \mathfrak{t}_{-u}(\mathfrak{m}_x).$$

Comme Ω_1 est dense dans $i(V)$, on obtient que $\mathfrak{t}_{-u}(H) \cdot \partial_{u,1}^{N_1}G \in \mathfrak{t}_{-u}(\overline{\mathcal{P}})$. Mais H n'appartient pas à $\overline{\mathcal{P}}$, et $\mathfrak{t}_{-u}(\overline{\mathcal{P}})$ est un idéal premier on a donc l'appartenance

$$\partial_{u,1}^{N_1}G \in \mathfrak{t}_{-u}(\overline{\mathcal{P}}).$$

On aboutit alors une contradiction, ce qui donne $N \geq T_0$, et donc on a

$$\Delta_u^{(\tau)}F \in \mathfrak{t}_{-u}(\overline{\mathcal{P}}), \quad \forall \tau \in \mathbb{N}^n, \quad |\tau| \leq T_0 - 1.$$

On peut utiliser les résultats de M. Chardin, car on travaille dans $\overline{\mathcal{A}}' = \overline{E}[\mathbf{X}, \mathbf{Y}]$. Pour majorer le rang du système $(\mathcal{S}_0)$ où l'on impose de plus les majorations

$$\deg_{\mathbf{X}} F \leq L \quad \text{et} \quad \deg_{\mathbf{Y}} F \leq L,$$

il suffit de majorer le rang du système $(\mathcal{S}_2)$ auquel on ajoute les mêmes contraintes. On considère la projection :

$$\Pi : \quad \overline{\mathcal{A}}' \longrightarrow \overline{\mathcal{A}}' / \mathfrak{t}_{-u}(\overline{\mathcal{P}}).$$

Alors, $\Delta_u^{(\tau)} F$ appartient à $\mathfrak{t}_{-u}(\overline{\mathcal{P}})$ si et seulement si son image $\Pi(\Delta_u^{(\tau)} F)$ par Π est nulle. Le nombre de conditions à écrire est donc plus petit que $\dim_{\mathcal{C}} \left(\overline{\mathcal{A}}' / \mathfrak{t}_{-u}(\overline{\mathcal{P}}) \right)_L$. La majoration de la fonction de Hilbert obtenue par M. Chardin [C] permet de conclure ici, que le rang du système $(\mathcal{S}_2)$ sur $\overline{E}$ est inférieur à

$$\begin{aligned} C_3 T_0^{n-\nu} \dim_{\mathcal{C}} \left(\overline{\mathcal{A}}' / \mathfrak{t}_{-u}(\overline{\mathcal{P}}) \right)_L &\leq C_4 T_0^{n-\nu} \deg(i(V)) L^\nu, \\ &\leq C_5 T_0^{n-\nu} \deg(V) (|\mu|^d L)^\nu. \end{aligned}$$

La projection Π étant définie sur E_V (le plus petit corps de définition de V contenant E), le système $(\mathcal{S}_2)$ est à coefficients dans E_V . Ainsi, le rang sur E de $(\mathcal{S}_2)$ est majoré par

$$(41) \quad C_6 [E_V : E] T_0^{n-\nu} \deg(V) (|\mu|^d L)^\nu.$$

6.2. Extrapolation

Dans la preuve du théorème principal, on se placera dans des conditions particulières et à l'aide du paragraphe précédent, on construira une fonction auxiliaire s'annulant à un certain ordre en un point donné. On trouvera ensuite des zéros supplémentaires à cette fonction, ceci via le lemme suivant.

Lemme 5. *Soit $\nu_0 \in A$ irréductible et soit $c > 0$ vérifiant*

$$\max(h(\Phi_{\nu_0}(\alpha)), h(\Phi_{\nu_0\mu}(\alpha))) \leq c.$$

Soit un polynôme non nul $F \in A[\mathbf{X}, \mathbf{Y}]$ tel que $F_0(\mathbf{X}) = F(\mathbf{X}, \Phi_\mu(\mathbf{X}))$ s'annule en α à l'ordre au moins T_0 , et vérifiant

$$\deg_{\mathbf{X}} F \leq L \quad \text{et} \quad \deg_{\mathbf{Y}} F \leq L.$$

Alors F_0 est nul en $\Phi_{\nu_0}(\alpha)$ à un ordre supérieur à

$$\frac{T_0 \deg \nu_0 - (h(F) + 2cL)}{\deg \nu_0 + c_\Phi \log T_0},$$

où c_Φ est une constante effectivement calculable, ne dépendant que de Φ .

Avant de commencer la preuve de ce lemme, on donne une estimation des coefficients matriciels de la fonction exponentielle e_Φ . On adopte pour cela quelques notations. Si M est une matrice, $M^{(q^i)} = \mathcal{F}^i(M)$ désignera ce même objet dont on a élevé à la puissance q^i tous les coefficients. On a l'écriture

$$(42) \quad e_\Phi(\mathbf{z}) = \sum_{m \geq 0} c_m \mathbf{z}^{q^m},$$

où les matrices c_m sont à coefficients dans le corps de définition E de Φ , et où l'on impose $c_0 = I_n$. On définit encore la suite $(D_m)_{m \geq 0}$ d'éléments de A par

$$(43) \quad \begin{cases} D_0 &= 1, \\ D_m &= [m] D_{m-1}^q, \quad \text{où } [m] = T^{q^m} - T. \end{cases}$$

Si v est une place du corps E , et si $M = [M_{i,j}]$ est une matrice à coefficients dans E , on note $v(M) = \inf_{i,j} \{v(M_{i,j})\}$. On montre alors facilement que si M et M' sont deux matrices à coefficients dans E ,

$$(44) \quad \begin{aligned} -v(M.M') &\leq -v(M) - v(M'), \\ -v(M + M') &\leq \max\{-v(M), -v(M')\}, \\ v(M^{(q^i)}) &= q^i v(M). \end{aligned}$$

On décompose enfin $a_0 = d\Phi_T = TI_n + N$ où N est une matrice nilpotente dont on note $\text{ord}(N)$ l'ordre. Avec ces notations, on peut montrer le lemme suivant.

Lemme 6.

- (i) pour tout $m \geq 0$, $\deg D_m = mq^m$,
- (ii) pour tous $r, m_1, \dots, m_l \in \mathbb{N}$ tels que $q^{m_1} + \dots + q^{m_l} \leq q^r$, $D_{m_1} \cdots D_{m_l}$ divise D_r ,
- (iii) Pour tout $m \geq 0$ et toute place finie v de E , on a

$$-v(D_m c_m) \leq q^m \max\{0, -v(a_i), i = 1, \dots, d\} + 2\text{ord}(N)mq^m \max\{0, -v(N)\},$$

(iv) Pour tout $m \geq 0$ et toute place infinie v de E , en notant e_v l'indice de ramification de E_v par rapport à k_∞ , on a

$$-v(D_m c_m) \leq q^m \max\{0, -v(a_i), i = 1, \dots, d\} + 2\text{ord}(N)mq^m \max\{0, -v(N)\} + e_v(d-1)mq^m.$$

Preuve - Les assertions (i) et (ii) découlent facilement de la définition de la suite (D_m) . Pour montrer les assertions suivantes, on reprend la preuve du lemme 8.2 de [B1], en ajoutant quelques modifications dûes à la non-commutativité des matrices. L'équation fonctionnelle

$$e_\Phi(a_0 \mathbf{z}) = \Phi_T(e_\Phi(\mathbf{z})),$$

où $a_0 = d\Phi_T = TI_n + N$, donne

$$\begin{aligned} \sum_{m \geq 0} c_m (a_0 \mathbf{z})^{q^m} &= \sum_{i=0}^d a_i \left(\sum_{m \geq 0} c_m \mathbf{z}^{q^m} \right)^{q^i}, \\ \sum_{m \geq 0} c_m a_0^{(q^m)} \mathbf{z}^{q^m} &= \sum_{i=0}^d \sum_{m \geq 0} a_i c_m^{(q^i)} \mathbf{z}^{q^{m+i}}. \end{aligned}$$

On obtient $a_0 c_0 = c_0 a_0$ (vérifié par choix de $c_0 = I_n$) et pour tout $m \geq 1$, l'égalité

$$c_m a_0^{(q^m)} = \sum_{i=0}^d a_i c_{m-i}^{(q^i)}.$$

Pour toutes matrices carrées M_1 et M_2 de même dimension, et tout entier $m \geq 0$, on note $[M_1, M_2]_m = M_1 M_2^{(q^m)} - M_2 M_1$. On a ainsi

$$c_m (T^{q^m} I_n + N^{(q^m)}) - (T I_n + N) c_m = [m] c_m + [c_m, N]_m = \sum_{i=1}^d a_i c_{m-i}^{(q^i)}.$$

On va montrer que cette égalité détermine entièrement les matrices c_m par récurrence. Pour alléger les notations, on désigne par B la matrice du membre de gauche.

$$c_m = \frac{1}{[m]} (B - [c_m, N]_m) = \frac{1}{[m]} (B - c_m N^{(q^m)} + N c_m).$$

Ainsi

$$[c_m, N]_m = \frac{1}{[m]} \left([B, N]_m - c_m (N^{(q^m)})^2 + 2Nc_m N^{(q^m)} - N^2 c_m \right).$$

On reporte dans l'égalité précédente, et on recommence l'opération plusieurs fois. Les matrices N et $N^{(q^m)}$ qui encadrent les c_m , apparaissent avec des puissances toujours plus élevées. Ainsi, au bout d'un nombre fini de telles opérations (par exemple 2 fois l'ordre de nilpotence de N), les c_m disparaissent du membre de droite et on obtient une égalité de la forme

$$c_m = \frac{1}{[m]} \left(\sum_{l_1+l_2 \leq 2\text{ord}(N)-1} r_{(l_1, l_2)} N^{l_1} B (N^{(q^m)})^{l_2} \right),$$

où les $r_{(l_1, l_2)}$ sont dans $\mathbb{F}_q$.

$$D_m c_m = \sum_{l_1+l_2 \leq 2\text{ord}(N)-1} \sum_{i=1}^d r_{(l_1, l_2)} N^{l_1} a_i c_{m-i}^{(q^i)} D_{m-i}^{q^i} \left(\frac{D_{m-1}^q}{D_{m-i}^{q^i}} \right) (N^{(q^m)})^{l_2}.$$

Or, $\frac{D_{m-1}^q}{D_{m-i}^{q^i}}$ est un élément de A , donc pour une place v de E on a

$$-v \left(\frac{D_{m-1}^q}{D_{m-i}^{q^i}} \right) \leq 0 \quad \text{si } v \text{ est finie,}$$

$$-v \left(\frac{D_{m-1}^q}{D_{m-i}^{q^i}} \right) \leq e_v \deg \left(\frac{D_{m-1}^q}{D_{m-i}^{q^i}} \right) \leq e_v (d-1) q^m \quad \text{si } v \text{ est infinie.}$$

On en déduit par récurrence sur m que si $v \nmid \infty$:

$$\begin{aligned} -v(D_m c_m) &\leq \max_{i, l_1, l_2} \left\{ -v \left(N^{l_1} a_i c_{m-i}^{(q^i)} D_{m-i}^{q^i} \left(\frac{D_{m-1}^q}{D_{m-i}^{q^i}} \right) (N^{(q^m)})^{l_2} \right) \right\}, \\ &\leq 2\text{ord}(N) q^m \max\{0, -v(N)\} + (1 + q^{m-1}) \max\{0, -v(a_i), i = 1, \dots, d\} \\ &\quad + 2\text{ord}(N)(m-1) q^{m-1} \max\{0, -v(N)\}, \\ &\leq q^m \max\{0, -v(a_i), i = 1, \dots, d\} + 2\text{ord}(N) m q^m \max\{0, -v(N)\}. \end{aligned}$$

On montre de même que si $v \mid \infty$ alors :

$$-v(D_m c_m) \leq q^m \max\{0, -v(a_i), i = 1, \dots, d\} + 2\text{ord}(N) m q^m \max\{0, -v(N)\} + e_v (d-1) m q^m,$$

d'où le lemme. $\square$

Preuve du lemme 5 - Soit $w \in M_{\mathfrak{K}}$. Le lemme-clef de Dobrowolski (proposition 14) dit que si w est une place au dessus de ν_0 , alors on a la majoration

$$|G^{(\tau)}(d\Phi_{\nu_0}(u))|_w \leq q^{-(T_0 - |\tau|) \deg \nu_0} \|\Phi_{\nu_0}(\alpha)\|_w^L \|\Phi_{\nu_0 \mu}(\alpha)\|_w^L.$$

On note $|F|_w$ le maximum des $|f_j|_w$ où les f_j sont les coefficients de F (si w est finie alors $|F|_w = 1$). Si $M = [M_{i,j}]$ est une matrice à coefficients dans $\mathfrak{K}$, on désigne par $|M|_w$ le maximum de 1 et des $|M_{i,j}|_w$. On note encore $\|\Phi\|_w = \max_{i=0, \dots, d} \{1, |a_i|_w\}$.

Si w n'est pas au dessus de ν_0 , en utilisant le lemme 6, on montre la majoration :

$$\left| G^{(\tau)}(d\Phi_{\nu_0}(u)) \right|_w \leq |F|_w \|\Phi_{\nu_0}(\alpha)\|_w^L \|\Phi_{\nu_0\mu}(\alpha)\|_w^L |N|_w^{4\text{ord}(N)|\tau| \log_q |\tau|} \|\Phi\|_w^{|\tau|} q^{e_w(d-1)|\tau| \log_q |\tau|},$$

où l'on convient que $e_w = 0$ si w est une place finie.

Si $G^{(\tau)}(d\Phi_{\nu_0}(u)) \neq 0$, la formule du produit donne $\prod_{w \in M_{\mathbb{R}}} \left| G^{(\tau)}(d\Phi_{\nu_0}(u)) \right|_w^{[\mathbb{R}_w:k_w]/[\mathbb{R}:k]} = 1$.

Donc

$$0 \leq -(T_0 - |\tau|) \deg \nu_0 + h(F) + Lh(\Phi_{\nu_0}(\alpha)) + Lh(\Phi_{\nu_0\mu}(\alpha)) + c_{\Phi} |\tau| \log |\tau|.$$

Vu le résultat à démontrer, on peut se restreindre à $|\tau| \leq T_0$. Ainsi

$$\begin{aligned} |\tau|(\deg \nu_0 + c_{\Phi} \log T_0) &\geq T_0 \deg \nu_0 - (h(F) + Lh(\Phi_{\nu_0}(\alpha)) + Lh(\Phi_{\nu_0\mu}(\alpha))), \\ &\geq T_0 \deg \nu_0 - (h(F) + 2cL), \end{aligned}$$

ce qui achève la preuve. $\square$

7 - Conclusion

7.1. Choix des paramètres

Avant de débiter la preuve, on rappelle quelques propriétés de la hauteur canonique associée à un T -module Φ , de dimension n , de degré d , défini sur k et dont on suppose que la matrice a_d est inversible (théorème 1 [De2]).

Lemme 7 [De2]. *Il existe une fonction $\hat{h}$ de $\mathbb{G}_a^n(\bar{k})$ dans $\mathbb{R}$, vérifiant les propriétés suivantes :*

1) *pour tout polynôme $P \in A$ de degré $r > 0$ et tout $\mathbf{x} \in \mathbb{G}_a^n(\bar{k})$, on a*

$$\hat{h}(\mathbf{x}) = \lim_{m \rightarrow \infty} q^{-mdr} h\left(\Phi_{P^m}(\mathbf{x})\right),$$

2) *pour tout polynôme $P \in A$ de degré $r > 0$ et tout $\mathbf{x} \in \mathbb{G}_a^n(\bar{k})$, on a*

$$\hat{h}\left(\Phi_P(\mathbf{x})\right) = q^{dr} \hat{h}(\mathbf{x}),$$

3) *la fonction $\hat{h} - h$ est bornée sur $\mathbb{G}_a^n(\bar{k})$, ainsi il existe $\Gamma(\Phi) > 0$ tel que $|\hat{h} - h| \leq \Gamma(\Phi)$.*

4) *$\hat{h}$ est l'unique fonction sur $\mathbb{G}_a^n(\bar{k})$ vérifiant à la fois la propriété 2) pour un polynôme donné de degré > 0 , et la propriété 3),*

5) *Pour tout couple de réels $C', C'' > 0$, il n'existe qu'un nombre fini d'éléments $\mathbf{x} \in \mathbb{G}_a^n(\bar{k})$ définis sur une extension algébrique de k de degré $\leq C'$, et tels que $\hat{h}(\mathbf{x}) \leq C''$,*

6) *$\hat{h}(\mathbf{x}) = 0$ si et seulement si $\mathbf{x}$ est un point de torsion du T -module (c'est-à-dire si et seulement si il existe $a \in A$ non nul tel que $\Phi_a(\mathbf{x}) = 0$),*

7) *Si γ est un point de torsion, alors pour tout $\mathbf{x} \in \mathbb{G}_a^n(\bar{k})$ on a $\hat{h}(\mathbf{x} + \gamma) = \hat{h}(\mathbf{x})$,*

8) *Pour tous $\mathbf{x}$ et $\mathbf{y}$ dans $\mathbb{G}_a^n(\bar{k})$ on a $\hat{h}(\mathbf{x} + \mathbf{y}) \leq \hat{h}(\mathbf{x}) + \hat{h}(\mathbf{y})$.*

On se place désormais dans le cadre du théorème C. Ainsi, on se donne Φ un T -module de dimension 2, de degré d et défini sur k . On suppose de plus que la matrice dominante

a_d de $\Phi_T(\mathbf{X})$ est inversible. On supposera encore que pour ce T -module, on a

$$\exists t \geq 1, \quad \exists C > 0, \quad \forall m \in \mathbb{N} \setminus \{0, 1\}, \quad \text{card}(H_m(\Phi)) \geq C \frac{m^{1/t}}{\log m},$$

où l'on a noté $H_m(\Phi) = \{\nu_0 \in A, \text{ irréductible, unitaire, } (\mathcal{H}_{\nu_0}) \text{ vérifiée et } |\nu_0| \leq m\}$.

Soit $\alpha \in \mathbb{G}_a^2(\bar{k})$ séparable sur k . On note $\mathfrak{K} = k(\alpha)$, $D = [\mathfrak{K} : k]$ et $\delta = \delta_k(\alpha)$. Soit C_0 un réel positif. Pour $r, s > 0$, on dira qu'un point algébrique α' vérifie l'hypothèse $(H(r, s))$ si α' n'est pas un point de torsion modulo les sous- T -modules de Φ , et si l'on a

$$(H(r, s)) \quad \hat{h}(\alpha') \leq \frac{1}{\delta_k(\alpha')} \left(\frac{(\log \log(3D))^s}{(C_0^2 \log(3D))^r} \right).$$

On définit aussi les paramètres suivants, où C_0 sera une constante choisie suffisamment grande de façon à ce que les inégalités qui suivent soient vérifiées.

$$\begin{aligned} L &= \left\lceil C_0^5 \delta \frac{(\log(3D))^3}{(\log \log(3D))^3} \right\rceil, & N &= q^{\left\lceil \frac{\log_q L}{d} \right\rceil + 1}, \\ T_0 &= \left\lceil C_0^8 \delta \frac{(\log(3D))^4}{(\log \log(3D))^5} \right\rceil, & T_{i+1} &= \left\lceil \frac{T_i \log \log(3D)}{C_0 \log(3D)} \right\rceil, \quad (i = 0, 1) \\ N_1^{(1)} &= \left\lceil \frac{(C_0^2 \log(3D))^{t^3(14d+3)}}{(\log \log(3D))^{t(7d+1)}} \right\rceil, & N_2^{(1)} &= \left\lceil \frac{(C_0^2 \log(3D))^{14t^4(2d+1)}}{(\log \log(3D))^{7t(2d+1)}} \right\rceil, \\ N_1^{(2)} &= \left\lceil \frac{(C_0^2 \log(3D))^{3t}}{(\log \log(3D))^t} \right\rceil, & N_2^{(2)} &= \left\lceil \frac{(C_0^2 \log(3D))^{14t^2}}{(\log \log(3D))^{7t}} \right\rceil, \end{aligned}$$

$$\mathcal{P}_j^{(i)} = \{1\} \cup \{a \in H_{N_j^{(i)}}(\Phi), \log(3D) \leq |a| \leq N_j^{(i)}\}.$$

7.2. Construction de la fonction auxiliaire

On applique la partie 6 dans un cadre plus restreint, où la dimension est 2, et où $E = k$. On choisit pour $i = 1$ ou 2, des exposants $r_i > 0$ et $s_i > 0$ pour lesquels on a

$$(45) \quad \left(N N_1^{(i)} N_2^{(i)} \right)^d \left(\frac{(\log \log(3D))^{s_i}}{(C_0^3 \log(3D))^{r_i}} \right) \leq C_0 \delta.$$

Ainsi, on prendra par exemple

$$\begin{aligned} r_1 &= t^4 d(42d + 17) + 3 & s_1 &= td(21d + 8) + 3 \\ r_2 &= 17t^2 d + 3 & s_2 &= 8td + 3 \end{aligned}$$

On a alors la proposition suivante.

Proposition 16. Soit $i \in \{1, 2\}$, on suppose que l'on a

$$\hat{h}(\alpha) \leq \frac{1}{\delta} \left(\frac{(\log \log(3D))^{s_i}}{(C_0^3 \log(3D))^{r_i}} \right).$$

Soit $\mu \in A$ irréductible et unitaire tel que $|\mu| = N$. Alors il existe un polynôme F appartenant à $A[\mathbf{X}, \mathbf{Y}] = A[X_1, X_2, Y_1, Y_2]$ non nul vérifiant $\deg_{\mathbf{X}} F \leq L$, $\deg_{\mathbf{Y}} F \leq L$, et tel que le polynôme $F_0(\mathbf{X}) = F(\mathbf{X}, \Phi_{\mu}(\mathbf{X}))$ s'annule au moins à l'ordre $T_2 + 1$ en $\Phi_{a_1 a_2}(\alpha)$ pour tout couple (a_1, a_2) de $\mathcal{P}_1^{(i)} \times \mathcal{P}_2^{(i)}$.

Preuve - On commence par construire une polynôme F dans $A[\mathbf{X}, \mathbf{Y}]$ non nul dont les degrés vérifient $\deg_{\mathbf{X}} F \leq L$, $\deg_{\mathbf{Y}} F \leq L$, et tel que le polynôme $F_0(\mathbf{X}) = F(\mathbf{X}, \Phi_{\mu}(\mathbf{X}))$ s'annule au moins à l'ordre $T_0 + 1$ en α . On est amené à résoudre un système linéaire $\mathcal{S}$ à $M = \binom{L+2}{2}^2$ inconnues et $\binom{T_0+2}{2}$ équations, à coefficients dans $\mathfrak{K} = k(\alpha)$ et dont on a majoré le rang sur k (ici $E = k$) dans le paragraphe 6. On note

$$\mathcal{E} = \{\mathbf{x} \in k^M, \mathcal{S}\mathbf{x} = 0\}$$

le k -espace vectoriel des solutions de $\mathcal{S}$. Il est de dimension $M - r$ où r désigne le rang de $\mathcal{S}$ sur le corps k .

Comme l'extension $k \hookrightarrow k(\alpha)$ est séparable, elle possède une clôture galoisienne G . On note $\sigma_1, \dots, \sigma_D$ les différents plongements de $k(\alpha)$ dans G . Ainsi, d'après le corollaire 3 de [Th], le système $\mathcal{S}$ possède une solution non nulle $\mathbf{X}_0$ dans k^M telle que :

$$h(\mathbf{X}_0) \leq \frac{1}{M-r} h(B) + 1,$$

où B est la matrice définie par bloc suivante

$$B = \begin{pmatrix} \sigma_1(\mathcal{S}) \\ \vdots \\ \sigma_D(\mathcal{S}) \end{pmatrix}$$

et où $h(B)$ désigne la hauteur (logarithmique) de l'espace engendré par les lignes de B , i.e. la hauteur du point de la Grassmannienne qui correspond à ce sous-espace. En effet, puisque l'extension $k \hookrightarrow k(\alpha)$ est séparable, les résultats de [SV] sont encore valables ici. Ainsi, si l'on note

$$\mathcal{G} = \{\mathbf{y} \in G^M, B\mathbf{y} = 0\},$$

alors on a $\dim_k(\mathcal{E}) = \dim_G(\mathcal{G}) = M - r$.

De plus, la hauteur $h(B)$ est aussi la hauteur d'une sous-matrice $\tilde{B}$ de dimension $r \times M$ extraite de B , de rang maximal. En majorant $h(\tilde{B})$ par la somme des hauteurs projectives de ses lignes $\tilde{B}_1, \dots, \tilde{B}_r$, on obtient la majoration suivante.

$$h(B) \leq r \max_{i=1, \dots, r} (h^{\text{proj}}(\tilde{B}_i))$$

Soit $\mathbf{X}_0 = \left(\frac{b_1}{b}, \dots, \frac{b_M}{b}\right) \in k^M$ la solution obtenue, où $b, b_1, \dots, b_M$ sont des éléments de A premiers entre eux. Alors on a les égalités suivantes

$$\begin{aligned} h(\mathbf{X}_0) &= h^{\text{proj}}(1, \mathbf{X}_0), \\ &= h^{\text{proj}}\left(1, \frac{b_1}{b}, \dots, \frac{b_M}{b}\right), \\ &= h^{\text{proj}}(b, b_1, \dots, b_M) \quad (\text{par la formule du produit}), \\ &= \max\{\deg b, \deg b_1, \dots, \deg b_M\} \quad (\text{car } (b, b_1, \dots, b_M) = 1). \end{aligned}$$

On note $\mathbf{Y}_0 = (b_1, \dots, b_M) \in A^M$, alors $\mathbf{Y}_0$ est aussi solution du système $\mathcal{S}$. De plus, comme $\mathbf{Y}_0 = b\mathbf{X}_0$, on a la majoration $h(\mathbf{Y}_0) \leq h(b) + h(\mathbf{X}_0)$. Ici, b est un élément de A , donc $h(b) = \deg(b)$, et d'après ce qui précède, on a $\deg(b) \leq h(\mathbf{X}_0)$, ainsi $h(\mathbf{Y}_0) \leq 2h(\mathbf{X}_0)$.

On utilise le paragraphe 6.1. où V est une $\bar{k}$ composante d'une k -variété V_0 passant par α et vérifiant

$$\deg_k(V_0)^{\text{codim} V_0} = \delta.$$

On note ν la dimension de cette variété, le rang du système est donc majoré par

$$C_6[k_V : k]T_0^{2-\nu} \deg(V)(|\mu|^d L)^\nu \leq C_6(\delta T_0)^{2-\nu}(|\mu|^d L)^\nu.$$

Finalement, on a montré qu'il existe un polynôme $F \in A[\mathbf{X}, \mathbf{Y}]$ non nul, vérifiant

$$\deg_{\mathbf{X}} F \leq L, \quad \deg_{\mathbf{Y}} F \leq L,$$

tel que $F_0(\mathbf{X})$ s'annule au moins à l'ordre $T_0 + 1$ en α . Par hypothèse, la hauteur $\hat{h}(\alpha)$ est suffisamment petite pour $\hat{h}(\Phi_\mu(\alpha))$ soit borné, on peut donc choisir F dont la hauteur est majorée de la façon suivante.

$$\begin{aligned} h(F) &\leq c_1 \frac{r}{M-r} \left(L + T_0 \log T_0 + T_0 \deg \mu \right), \\ &\leq c_2 \frac{(\delta T_0)^{2-\nu} |\mu|^{\nu d}}{L^{4-\nu}} \left(L + T_0 \log T_0 + T_0 \deg \mu \right), \\ &\leq c_3 \left(\frac{\delta T_0}{L^2} \right)^{2-\nu} \left(L + T_0 \log T_0 \right), \\ &\leq c_4 \frac{C_0^6 \delta (\log(3D))^3}{(\log \log(3D))^4}. \end{aligned}$$

On applique le lemme d'extrapolation au polynôme F et au point α . Soit $a_1 \in \mathcal{P}_1^{(i)}$, alors par hypothèse, on a la majoration

$$\hat{h}(\Phi_{a_1 \mu}(\alpha)) \leq C_0.$$

On montre ainsi que le polynôme F_0 s'annule en $\Phi_{a_1}(\alpha)$ à un ordre supérieur à

$$\frac{T_0 \deg a_1 - (h(F) + 2(C_0 + \Gamma(\Phi))L)}{\deg a_1 + c_\Phi \log T_0} \geq T_1 + 1$$

pour tout $a_1 \in \mathcal{P}_1^{(i)}$.

On applique alors à nouveau le lemme 5 au même polynôme F , et aux points $\Phi_{a_1}(\alpha)$ pour $a_1 \in \mathcal{P}_1^{(i)}$, et l'on obtient que le polynôme F_0 s'annule à un ordre supérieur à

$$\frac{T_1 \deg a_2 - (h(F) + 2(C_0 + \Gamma(\Phi))L)}{\deg a_2 + c_\Phi \log T_0} \geq T_2 + 1$$

en les points $\Phi_{a_1 a_2}(\alpha)$ pour tout $(a_1, a_2) \in \mathcal{P}_1^{(i)} \times \mathcal{P}_2^{(i)}$. $\square$

7.3. Construction d'un point de petit indice d'obstruction

Afin de pouvoir utiliser le lemme de zéros, on montre que la « plupart » des éléments de $\mathcal{P}_j^{(i)}$, ne sont pas dans $E(W)$ pour toute variété W dont on contrôle bien le degré. On aura besoin dans la preuve du lemme suivant, d'énoncés de géométrie apparaissant dans le paragraphe 3.

Lemme 8. *Soit W une k -variété, vérifiant*

$$\log \deg_k(W) \leq \left(\frac{C_0 \log(3D)}{\log \log(3D)} \right)^2.$$

Alors il existe une constante $c_5 > 0$, et des ensembles $\tilde{\mathcal{P}}_j^{(i)} \subset \mathcal{P}_j^{(i)}$ (pour $i, j = 1, 2$) contenant tous 1, tels que :

$$(4) \quad \forall (a_1, a_2) \in \tilde{\mathcal{P}}_1^{(i)} \times \tilde{\mathcal{P}}_2^{(i)}, \quad a_1 a_2 \notin E(W),$$

et tels que

$$\text{card}(\tilde{\mathcal{P}}_j^{(i)}) \geq c_5 \frac{(N_j^{(i)})^{1/t}}{\log N_j^{(i)}}.$$

Preuve - La preuve de [AD] s'adapte très bien ici ; par commodité pour le lecteur, on l'écrit malgré tout. On définit les ensembles $E_1^{(i)}$ et $E_2^{(i)}$ comme suit :

$$\begin{aligned} E_1^{(i)} &= E(W), \\ E_2^{(i)} &= \bigcup_{a_1 \in \mathcal{P}_1^{(i)}} E(\Phi_{a_1}(W)). \end{aligned}$$

D'après le point (i) de la proposition 13, si on pose $\tilde{\mathcal{P}}_j^{(i)} = \mathcal{P}_j^{(i)} \setminus E_j^{(i)}$, alors (4) est bien vérifiée. Il reste donc à minorer le cardinal des $\tilde{\mathcal{P}}_j^{(i)}$. Par construction des $\mathcal{P}_j^{(i)}$, et par hypothèse sur Φ , on a l'inégalité

$$\text{card}(\mathcal{P}_j^{(i)}) \geq c_6 \frac{(N_j^{(i)})^{1/t}}{\log N_j^{(i)}}.$$

On a d'une part les majorations suivantes (voir proposition 12).

$$\begin{aligned} \text{card} \left(A_{\text{irr}}^+ \cap E_1^{(i)} \right) &= \text{card} \left(A_{\text{irr}}^+ \cap E(W) \right) = \text{card} \left(E^+(W) \right), \\ &\leq C_1(\Phi) \log \deg_k(W), \\ &\leq C_1(\Phi) \left(\frac{C_0 \log(3D)}{\log \log(3D)} \right)^2, \\ &\leq \frac{1}{2} \text{card}(\mathcal{P}_1^{(i)}). \end{aligned}$$

D'autre part, par définition de $E_2^{(i)}$, on a

$$\text{card} \left(A_{\text{irr}}^+ \cap E_2^{(i)} \right) \leq N_1^{(i)} \max_{a_1 \in \mathcal{P}_1^{(i)}} \text{card} \left(A_{\text{irr}}^+ \cap E(\Phi_{a_1}(W)) \right).$$

D'après le point (i) du lemme 2, on a la majoration

$$\max_{a_1 \in \mathcal{P}_1^{(i)}} \deg(\Phi_{a_1}(W)) \leq \left(N_1^{(i)} \right)^{\text{ddim} W} \deg_k W.$$

On utilise maintenant la proposition 12 et l'hypothèse faite sur le degré de W , pour montrer

$$\begin{aligned} \max_{a_1 \in \mathcal{P}_1^{(i)}} \text{card} \left(A_{\text{irr}}^+ \cap E(\Phi_{a_1}(W)) \right) &\leq c_7 \left(\log \left(N_1^{(i)} \right) + \log \deg_k(W) \right), \\ &\leq c_8 \left(\frac{C_0 \log(3D)}{\log \log(3D)} \right)^2. \end{aligned}$$

En reportant dans l'inégalité ci-dessus, on obtient :

$$\text{card} \left(A_{\text{irr}}^+ \cap E_2^{(i)} \right) \leq c_9 N_1^{(i)} \left(\frac{C_0 \log(3D)}{\log \log(3D)} \right)^2 \leq \frac{c_6 \left(N_2^{(i)} \right)^{1/t}}{2 \log N_2^{(i)}} \leq \frac{1}{2} \text{card}(\mathcal{P}_2^{(i)}). \quad \square$$

On montre maintenant que, si la hauteur canonique de α est petite, on peut trouver $a \in A$ tel que l'indice d'obstruction de $\Phi_a(\alpha)$ est petit devant celui de α . Pour cela, on utilise le lemme de zéros; cependant afin d'obtenir un supplément galoisien, on doit l'appliquer à un autre polynôme que F_0 donné par la proposition 16. En effet, le polynôme $F_0(\mathbf{X}) = F(\mathbf{X}, \Phi_\mu(\mathbf{X}))$ définit des $\bar{k}$ -variétés de $\mathbb{G}_a^2$ qui peuvent ne pas être G.R. sur k . L'objectif est alors de construire, à partir de F_0 , un polynôme $\tilde{F}_0$, qui possède les mêmes propriétés que F_0 , mais dont les facteurs k -irréductibles sont séparables.

Lemme 9. *Soit $P_0 \in A[\mathbf{X}]$ irréductible s'annulant à l'ordre au moins $\tau_0 + 1$ en des points $\Phi_{a_1 a_2}(\alpha)$, et de degré $\leq L_0$. On suppose que P_0 n'est pas séparable sur k , et l'on note s le plus grand entier tel que $P_0(\mathbf{X}) = \tilde{P}_0(\mathbf{X}^{p^s})$. Alors, il existe $Q \in A[\mathbf{X}]$ tel que*

$$\deg Q \leq L_0/p^s, \quad h(Q) \leq h(P_0)/p^s$$

et s'annulant à l'ordre au moins $\left\lceil \frac{\tau_0}{p^s} \right\rceil + 1$ en les mêmes points $\Phi_{a_1 a_2}(\alpha)$.

Preuve - On écrit

$$P_0(\mathbf{X}) = (Q_0(\mathbf{X}))^{p^s} + T(Q_1(\mathbf{X}))^{p^s} + \dots + T^{p^s-1}(Q_{p^s-1}(\mathbf{X}))^{p^s}.$$

Si tous les $Q_i(\alpha)$ n'étaient pas nuls, alors T^{1/p^s} serait algébrique de degré $\leq p^s - 1$ sur $k(\alpha)$. Comme α est séparable sur k , le degré d'inséparabilité de T^{1/p^s} sur k serait strictement inférieur à p^s , ce qui n'est pas le cas. Ainsi, pour tout $i = 0, \dots, p^s - 1$, on a $Q_i(\alpha) = 0$.

On choisit i pour lequel $Q_i(\mathbf{X}) \neq 0$, et l'on note $Q = Q_i$. Il est clair que $\deg Q \leq L_0/p^s$ et que $h(Q) \leq h(P_0)/p^s$. De plus, $(P_0(\mathbf{X}))^{1/p^s}$ est un polynôme de $A[T^{1/p^s}][\mathbf{X}]$, on peut donc regarder ses dérivées divisées successives par rapport à $\mathbf{X}$. Soit $\tau'_0 p^s$ le premier multiple de p^s supérieur à $\tau_0 + 1$. On voit facilement que $\tau'_0 = \left\lceil \frac{\tau_0}{p^s} \right\rceil + 1$.

$$\begin{aligned} P_0(\Phi_{a_1 a_2}(\alpha) + e_\Phi(\mathbf{z})) &= \sum_{|\tau| \geq \tau_0 + 1} \Delta^{(\tau)} P_0(\Phi_{a_1 a_2}(\alpha)) \mathbf{z}^\tau, \\ &= \sum_{\tau'} \Delta^{(p^s \tau')} P_0(\Phi_{a_1 a_2}(\alpha)) \mathbf{z}^{p^s \tau'}, \\ &= \sum_{|\tau| \geq \tau'_0 + 1} \Delta^{(p^s \tau)} P_0(\Phi_{a_1 a_2}(\alpha)) \mathbf{z}^{p^s \tau}. \end{aligned}$$

$$\begin{aligned} (P_0(\Phi_{a_1 a_2}(\alpha) + e_\Phi(\mathbf{z})))^{1/p^s} &= \sum_{|\tau| \geq \tau'_0 + 1} (\Delta^{(p^s \tau)} P_0(\Phi_{a_1 a_2}(\alpha)))^{1/p^s} \mathbf{z}^\tau, \\ &= Q_0(\Phi_{a_1 a_2}(\alpha) + e_\Phi(\mathbf{z})) + T^{1/p^s} Q_1(\Phi_{a_1 a_2}(\alpha) + e_\Phi(\mathbf{z})) + \cdots \\ &\quad \cdots + T^{(p^s - 1)/p^s} Q_{p^s - 1}(\Phi_{a_1 a_2}(\alpha) + e_\Phi(\mathbf{z})), \\ &= \sum_{\tau} \left(\Delta^{(\tau)} Q_0(\Phi_{a_1 a_2}(\alpha)) + T^{1/p^s} \Delta^{(\tau)} Q_1(\Phi_{a_1 a_2}(\alpha)) + \cdots \right. \\ &\quad \left. \cdots + T^{(p^s - 1)/p^s} \Delta^{(\tau)} Q_{p^s - 1}(\Phi_{a_1 a_2}(\alpha)) \right) \mathbf{z}^\tau. \end{aligned}$$

Comme précédemment, on a $\Delta^{(\tau)} Q(\Phi_{a_1 a_2}(\alpha)) = 0$ pour $|\tau| \leq \tau'_0$, ce qui termine la preuve du lemme. $\square$

On décompose F_0 en produit de facteurs k -irréductibles, éventuellement répétés plusieurs fois.

$$F_0(\mathbf{X}) = P_1(\mathbf{X}) \cdots P_n(\mathbf{X})$$

Chacun des P_j s'annule à un ordre $\tau_j(a_1, a_2) \geq 0$ en $\Phi_{a_1 a_2}(\alpha)$. On applique le lemme 9 à chaque facteur P_j qui n'est pas séparable sur k , et l'on construit ainsi des puissances p^{s_j} et des polynômes $\tilde{P}_j$. On remplace alors dans le produit $F_0(\mathbf{X}) = P_1(\mathbf{X}) \cdots P_n(\mathbf{X})$ les P_j concernés par $\tilde{P}_j^{p^{s_j}}$. Les polynômes $\tilde{P}_j$ peuvent ne pas être séparables ; on recommence la même opération jusqu'à ne plus obtenir que des facteurs k -irréductibles, séparables sur k . Le produit ainsi construit est noté $\tilde{F}_0(\mathbf{X})$. L'ensemble algébrique qu'il définit n'est alors composé que de $\bar{k}$ -composantes G.R sur k , et on a les propriétés suivantes.

$$\deg(\tilde{F}_0) \leq L_0 \quad \text{et} \quad h(\tilde{F}_0) \leq h(F_0),$$

où $L_0 = (1 + |\mu|^d)L \leq (1 + q^d)L^2$, et $\tilde{F}_0$ s'annule aux mêmes points $\Phi_{a_1 a_2}(\alpha)$ que F_0 , et au même ordre au moins.

On montre maintenant la proposition suivante.

Proposition 17. *Soit $\alpha \in \mathbb{G}_a^2(\bar{k})$ séparable sur k , et qui n'est pas de torsion pour les sous- T -modules de Φ . Soit $i \in \{1, 2\}$. On suppose que l'on a*

$$\hat{h}(\alpha) \leq \frac{1}{\delta} \left(\frac{(\log \log(3D))^{s_i}}{(C_0^3 \log(3D))^{r_i}} \right).$$

Alors pour toute k -variété W vérifiant

$$\log \deg_k(W) \leq \left(\frac{C_0 \log(3D)}{\log \log(3D)} \right)^2,$$

il existe $l \notin E(W)$ tel que :

$$|l| \leq N_2^{(i)},$$

et pour lequel on a

$$\delta_k(\Phi_l(\alpha)) \leq \varepsilon_i \delta_k(\alpha),$$

$$\text{où } \varepsilon_1 \leq \left(\frac{(\log \log(3D))^{7d}}{(C_0^3 \log(3D))^{(t^2(14d+3)-3)}} \right) \text{ et } \varepsilon_2 < 1.$$

Preuve - On applique le lemme de zéros au polynôme $\tilde{F}_0(\mathbf{X})$ et aux ensembles $\tilde{\mathcal{P}}_j^{(i)}$ construits dans le lemme précédent : il fournit un indice $r = r^{(i)} \in \{1, 2\}$ et une $\bar{k}$ -variété $\bar{V}$ rencontrant Σ_{r+1} . On note

$$V = \bigcup_{\sigma \in \text{Aut}(\bar{k}/k)} \sigma(\bar{V}).$$

Si V est de dimension 0, alors V est de la forme $\{\sigma(\Phi_l(\alpha)), \sigma \in \text{Aut}(\bar{k}/k)\}$ qui, par hypothèse sur α , est réunion de $\bar{k}$ -composantes G.R. sur k . Si V est de dimension 1, alors elle est définie par l'un des facteurs k -irréductibles de $\tilde{F}_0$ qui est séparable. Ainsi, on a un supplément galoisien au lemme de zéros.

On a donc la majoration suivante

$$T_r^{\text{codim} V} \deg_k \left(\bigcup_{a \in \tilde{\mathcal{P}}_r^{(i)}} \Phi_a(V) \right) \leq \left(L_0 N_{r-1}^{(i)} \right)^{\text{codim} V},$$

en convenant que $N_0^{(i)} = 1$. En particulier, on a l'inclusion

$$V \subset \bigcup_{a \in \tilde{\mathcal{P}}_r} \Phi_a(V)$$

et ces ensembles algébriques sont de même dimension ; on a donc

$$\log \deg_k(V) \leq 2 \log \left(N_1^{(i)} L_0 \right) \leq c_{10} \log(3D).$$

Soit $\mathfrak{Q}_r^{(i)} = \tilde{\mathcal{P}}_r^{(i)} \setminus E(V)$. D'après la proposition 12, on a la minoration

$$\text{card}(\mathfrak{Q}_r^{(i)}) \geq c_{11} \frac{\left(N_r^{(i)} \right)^{1/t}}{\log N_r^{(i)}}.$$

Or, $\Phi_l(\alpha)$ n'est pas de torsion modulo les sous- T -modules de $(\mathbb{G}_a^2, \Phi)$, donc la composante $\bar{k}$ -irréductible de V passant par ce point ne peut pas être un translaté d'un sous- T -module par un point de torsion. Le point (ii) de la proposition 13 donne ici

$$T_r^{\text{codim} V} \text{card}(\mathfrak{Q}_r^{(i)}) \deg_k(V) \leq \left(L_0 N_{r-1}^{(i)} \right)^{\text{codim} V}.$$

On constate tout d'abord, que cette inégalité entraîne $r = 1$. En effet, si r valait 2, alors α appartiendrait à V et on aurait

$$\delta_k(\alpha) \leq \frac{L_0 N_1^{(i)}}{T_2 \left(\text{card}(\mathfrak{Q}_2^{(i)}) \right)^{1/2}} < \delta_k(\alpha).$$

Ainsi $r = 1$, et donc $\text{codim}(V) = 1$ et on obtient l'inégalité

$$T_1 \text{card}(\mathfrak{Q}_1^{(i)}) \deg_k(V)^{1/\text{codim} V} \leq L_0.$$

De plus, la variété V rencontre Σ_2 , donc il existe $l \in \tilde{\mathcal{P}}_2^{(i)}$, ($|l| \leq N_2^{(i)}$) pour lequel $\Phi_l(\alpha) \in V$.

$$\begin{aligned} \delta_k(\Phi_l(\alpha)) &\leq (\deg_k(V))^{1/\text{codim} V}, \\ &\leq \frac{L_0}{T_1 \text{card}(\mathfrak{Q}_1^{(i)})}, \\ &\leq \varepsilon_i \delta. \end{aligned}$$

□

7.4. La descente

La descente finale consiste à construire une suite de variétés passant par des translatés de α , et dont les degrés s'approchent des indices d'obstructions de ces points.

On désigne maintenant par $\mathcal{W}$ l'ensemble de triplets $(n, \mathbf{l}, \mathbf{V})$ où n est un élément de $\{0, 1, 2\}$, et où $\mathbf{l} = \emptyset$ si $n = 0$, $\mathbf{l} = (l_1) \in A$ si $n = 1$, et $\mathbf{l} = (l_1, l_2) \in A^2$ si $n = 2$. On suppose de plus que l'on a $0 \leq |l_i| \leq N_2^{(i)}$, et que $\mathbf{V} = (V_0, \dots, V_n)$ est un $(n+1)$ -uplet de k -variétés propres dont les $\bar{k}$ -composantes sont G.R. sur k et vérifiant :

- (i) $\alpha \in V_0$,
- (ii) pour $i = 1, n$: $l_i \notin E(V_{i-1})$ et $V_{i-1} \subset \Phi_{l_i}^{-1}(V_i)$,
- (iii) pour $i \in \{0, \dots, n\}$:
 - si $i = 0$, $\deg_k(V_i) = \deg_k(V_0) \leq \left(\left(N_2^{(1)} N_2^{(2)} \right)^d \delta_k(\alpha) \right)^{\text{codim} V_i}$,
 - si $i = 1$, $\deg_k(V_i) = \deg_k(V_1) \leq \left(\left(N_2^{(2)} \right)^d \delta_k(\Phi_{l_1}(\alpha)) \right)^{\text{codim} V_i}$,
 - si $i = 2$, $\deg_k(V_i) = \deg_k(V_2) \leq \left(\delta_k(\Phi_{l_1 l_2}(\alpha)) \right)^{\text{codim} V_i}$,
- (iv) pour $i \in \{1, n\}$:
 - si $i = 1$, $\delta_k(\Phi_{l_1}(\alpha)) \leq \varepsilon_i \delta_k(\alpha) = \varepsilon_1 \delta_k(\alpha)$,
 - si $i = 2$, $\delta_k(\Phi_{l_1 l_2}(\alpha)) \leq \varepsilon_i \delta_k(\Phi_{l_1}(\alpha)) = \varepsilon_2 \delta_k(\Phi_{l_1}(\alpha))$.

Puisque $\varepsilon_i < 1$, on remarque en particulier que, si cela a un sens, on a les majorations $\delta_k(\Phi_{l_1}(\alpha)) < \delta_k(\alpha)$, et $\delta_k(\Phi_{l_1 l_2}(\alpha)) < \delta_k(\Phi_{l_1}(\alpha))$.

On définit encore

$$(46) \quad \mathcal{W}_0 = \{(n, \mathbf{l}, \mathbf{V}) \in \mathcal{W}, \dim(V_0) < \dots < \dim(V_n)\}.$$

On montre dans un premier temps que $\mathcal{W}_0 \neq \mathcal{W}$, ainsi on pourra trouver $(n, \mathbf{l}, \mathbf{V})$ dans $\mathcal{W}$ pour lequel il existe un indice $i \in \{1, \dots, n\} \subset \{1, 2\}$ tel que $\dim(V_{i-1}) = \dim(V_i)$. Pour cela, on montre la proposition suivante.

Proposition 18. *Soit $\alpha \in \mathbb{G}_a^2(\bar{k})$ séparable sur k , et qui ne soit pas de torsion pour Φ . On suppose que :*

$$\hat{h}(\alpha) \leq \frac{1}{\delta} \left(\frac{(\log \log(3D))^V}{(C_0^3 \log(3D))^U} \right),$$

où $U = dt^4(42d + 17) + 3$ et $V = dt(21d + 8) + 2$. Alors $\mathcal{W}_0 \neq \mathcal{W}$.

On suit la preuve de [AD] et on introduit la même relation d'ordre total sur les suites finies de longueur au plus $m + 1$ d'entiers positifs ou nuls et strictement inférieurs à m . Soient $(v) = (v_0, \dots, v_j)$ et $(v') = (v'_0, \dots, v'_{j'})$ deux telles suites. On dira que :

$$(v) \preceq (v'),$$

si on a l'inégalité $(v_0, \dots, v_{\min(j, j')}) < (v'_0, \dots, v'_{\min(j, j')})$ pour l'ordre lexicographique, ou bien si $(v_0, \dots, v_{\min(j, j')}) = (v'_0, \dots, v'_{\min(j, j')})$ et $j \geq j'$.

Avant de commencer la preuve, on montre le lemme suivant.

Lemme 10. *Soit $m \geq 0$ un entier, $l_1, \dots, l_m$ des éléments de A non nuls ($l_0 = 1$), et $W_0, \dots, W_m$ des k -variétés propres de $\mathbb{G}_a^2$ dont les $\bar{k}$ -composantes sont G.R. sur k et telles que*

- $\alpha \in W_0$,
- $i = 1, \dots, m$, $W_{i-1} \subset \Phi_{l_i}^{-1}(W_i)$.

Soit $l_{m+1} \in A$ non nul. On note d_{m+1} la dimension d'une variété obstructrice de $\Phi_{l_1 \dots l_{m+1}}(\alpha)$. Alors, il existe un entier $m' \in \{0, \dots, m+1\}$ et une k -variété propre $Z_{m'}$ de degré sur k majoré par

$$|l_{m'+1} \dots l_{m+1}|^{d(2-d_{m+1})} \delta_k(\Phi_{l_1 \dots l_{m+1}}(\alpha))^{2-d_{m+1}} \deg_k(W_{m'})^{d_{m+1}},$$

et telle que

- $W_{m'-1} \subset \Phi_{l_{m'}}^{-1}(Z_{m'})$,
- si $m' \in \{0, \dots, m\}$ $\dim(Z_{m'}) = 0$,
- $(\dim W_0, \dots, \dim W_{m'-1}, \dim Z_{m'}) \preceq (\dim W_0, \dots, \dim W_m)$.

On a convenu dans cet énoncé que $\deg_k(W_{m+1}) = 1$ et que $W_{-1} = \{\sigma(\alpha), \sigma \in \text{Aut}(\bar{k}/k)\}$.

Preuve - On se donne une k -variété notée Z_{m+1} de dimension d_{m+1} passant par $\Phi_{l_1 \dots l_{m+1}}(\alpha)$ dont les $\bar{k}$ -composantes sont G.R. sur k et telle que

$$\deg_k(Z_{m+1}) = \delta_k(\Phi_{l_1 \dots l_{m+1}}(\alpha))^{2-d_{m+1}}.$$

En particulier, on l'inclusion

$$\{\sigma(\Phi_{l_1 \dots l_{m+1}}(\alpha)), \sigma \in \text{Aut}(\bar{k}/k)\} \subset Z_{m+1}.$$

On construit ensuite des variétés $Z_0, \dots, Z_m$ de la façon suivante.

Si $W_i \subset \Phi_{l_{i+1} \dots l_{m+1}}^{-1}(Z_{m+1})$, on pose $Z_i = W_i$.

Sinon, on pose $Z_i = \{\sigma(\Phi_{l_1 \dots l_i}(\alpha)), \sigma \in \text{Aut}(\bar{k}/k)\}$.

On peut maintenant choisir l'indice m' . Si pour $i = 0, \dots, m$ on a $W_i = Z_i$, on pose $m' = m + 1$, sinon, on choisit pour m' , le plus petit des indices i tels que $Z_i \subsetneq W_i$. Il reste à vérifier que $Z_{m'}$ convient. On remarque tout d'abord que nécessairement les $\bar{k}$ -composantes de $Z_{m'}$ sont G.R. sur k .

Si $m' = m + 1$ alors par construction, $W_m \subset \Phi_{l_{m+1}}^{-1}(Z_{m'})$, et les autres propriétés annoncées découlent de la construction de Z_{m+1} , et de la définition de l'ordre $\preceq$.

Si $m' \in \{0, \dots, m\}$, alors nécessairement la variété $W_{m'}$ est de dimension 1, et l'intersection $W_{m'} \cap \Phi_{l_{m'+1} \dots l_{m+1}}^{-1}(Z_{m+1})$ est de dimension 0, et contient $Z_{m'}$. Si Z_{m+1} est de dimension $d_{m+1} = 1$, alors en appliquant le lemme de Bezout sur $\bar{k}$ et en regroupant les $\bar{k}$ -composantes conjuguées (qui sont G.R. sur k), on obtient la majoration

$$\deg_k(Z_{m'}) \leq |l_{m'+1} \dots l_{m+1}|^{d(2-d_{m+1})} \delta_k(\Phi_{l_1 \dots l_{m+1}}(\alpha))^{2-d_{m+1}} \deg_k(W_{m'})^{d_{m+1}}.$$

Si $d_{m+1} = 0$ alors toutes les variétés Z_i sont de dimension 0 et s'écrivent

$$Z_i = \{\sigma(\Phi_{l_1 \dots l_i}(\alpha)), \sigma \in \text{Aut}(\bar{k}/k)\} \subset \Phi_{l_{i+1} \dots l_{m+1}}^{-1}(Z_{m+1}).$$

On en déduit l'inégalité suivante

$$\deg_k(Z_{m'}) \leq |l_{m'+1} \dots l_{m+1}|^{2d} \delta_k(\Phi_{l_1 \dots l_{m+1}}(\alpha))^2,$$

ce qui achève la preuve du lemme. □

Preuve de la proposition 18 - On voit tout d'abord que $\mathcal{W}_0 \neq \emptyset$. En effet, d'après le corollaire de la proposition 10, on peut trouver une k -variété propre V passant par α , dont les $\bar{k}$ -composantes sont G.R. sur k et vérifiant $\deg_k(V) = \delta_k(\alpha)^{\text{codim}(V)}$. Alors $(0, \emptyset, V)$ appartient à $\mathcal{W}_0$.

D'autre part, on place sur $\mathcal{W}_0$ une relation d'ordre en posant $(n, \mathbf{l}, \mathbf{W}) \preceq (n', \mathbf{l}', \mathbf{W}')$ si l'on a l'inégalité

$$(47) \quad (\dim W_i)_{i=0, \dots, n} \preceq (\dim W'_i)_{i=0, \dots, n'}.$$

Soit $(n, \mathbf{l}, \mathbf{W})$ un élément de $\mathcal{W}_0$. Les variétés W_i sont propres et strictement emboîtées, elles sont donc de dimension 0 ou 1. Par conséquent, les suites de dimensions apparaissant dans $\mathcal{W}_0$ sont parmi les trois suivantes.

$$(48) \quad (0, 1) \quad \preceq \quad (0) \quad \preceq \quad (1)$$

Ainsi, $\mathcal{W}_0$ possède (au moins) un élément minimal que l'on note $(n, \mathbf{l}, \mathbf{W})$ et pour lequel n vaut soit 0 soit 1. Si $n = 0$, on applique la proposition 17 à W_0 et α qui vérifie $(H(r_1, s_1))$. Dans ce cas, on a donc l'existence de $l_1 \notin E(W_0)$ tel que $|l_1| \leq N_2^{(1)}$, et

$$\delta_k(\Phi_{l_1}(\alpha)) \leq \varepsilon_1 \delta_k(\alpha).$$

Si $n = 1$, on applique cette même proposition à W_1 et $\Phi_{l_1}(\alpha)$. On constate tout d'abord que $\Phi_{l_1}(\alpha)$ vérifie $(H(r_2, s_2))$. En effet,

$$\begin{aligned} \hat{h}(\Phi_{l_1}(\alpha)) &= |l_1|^d \hat{h}(\alpha), \\ &\leq \left(N_2^{(1)}\right)^d C_0 \frac{1}{\delta} \left(\frac{(\log \log(3D))^V}{(C_0^3 \log(3D))^U} \right), \\ &\leq \frac{1}{\delta(\Phi_{l_1}(\alpha))} \left(\frac{(\log \log(3D))^{V-7td(2d+1)}}{(C_0^3 \log(3D))^{U-14t^4d(2d+1)}} \right), \\ &\leq \frac{1}{\delta(\Phi_{l_1}(\alpha))} \left(\frac{(\log \log(3D))^{s_2}}{(C_0^3 \log(3D))^{r_2}} \right). \end{aligned}$$

Ici on obtient $l_2 \notin E(W_2)$ tel que $|l_2| \leq N_2^{(2)}$, et

$$\delta_k(\Phi_{l_1 l_2}(\alpha)) \leq \varepsilon_2 \delta_k(\Phi_{l_1}(\alpha)).$$

On applique ensuite le lemme précédent à $(n, \mathbf{l}, \mathbf{W})$ et à l'élément l_{n+1} de A que l'on vient de construire. On en déduit l'existence de $n' \in \{0, \dots, n+1\} \subset \{0, 1, 2\}$ et d'une k -variété $Z_{n'}$ possédant les propriétés énoncées dans le lemme. Si l'on note

$$(n', \mathbf{l}', \mathbf{Z}) = (n', (l_1, \dots, l_{n'}), (W_0, \dots, W_{n'-1}, Z_{n'}))$$

on aura en particulier, la relation

$$(n', \mathbf{l}', \mathbf{Z}) \not\preceq (n, \mathbf{l}, \mathbf{W}),$$

ainsi $(n', \mathbf{l}', \mathbf{Z}) \notin \mathcal{W}_0$.

Pour terminer la preuve de la proposition 18, il reste donc à montrer que $(n', \mathbf{l}', \mathbf{Z})$ est bien dans $\mathcal{W}$. Les propriétés (i), (ii) et (iv) sont clairement vérifiées; on doit donc majorer convenablement le degré sur k de $Z_{n'}$, ceci à partir de l'inégalité

$$\deg_k(Z_{n'}) \leq |l_{n'+1} \cdots l_{n+1}|^{d(2-d_{n+1})} \delta_k(\Phi_{l_1 \dots l_{n+1}}(\alpha))^{2-d_{n+1}} \deg_k(W_{n'})^{d_{n+1}}.$$

Tout d'abord, si $n' = n+1$, la k -variété $Z_{n'}$ construite dans le lemme 10 vérifie

$$\deg_k(Z_{n'}) = \delta_k(\Phi_{l_1 \dots l_{n'}}(\alpha))^{\text{codim}(Z_{n'})}.$$

Par conséquent, dans ce cas, la propriété (iii) est clairement satisfaite. Il reste à traiter le cas où $n' \leq n$. En particulier, dans ce cas, la k -variété $Z_{n'}$ est de dimension 0 et $W_{n'}$ est de dimension 1. Comme n vaut soit 0 soit 1, trois possibilités apparaissent.

Premier cas : $n' = n = 0$

On obtient l'inégalité

$$\begin{aligned} \deg_k(Z_0) &\leq (|l_1|^d \delta_k(\Phi_{l_1}(\alpha)))^{2-d_{n+1}} \deg_k(W_0)^{d_{n+1}}, \\ &\leq \left(\left(N_2^{(1)}\right)^d \delta_k(\Phi_{l_1}(\alpha)) \right)^{2-d_{n+1}} \left(\left(N_2^{(1)} N_2^{(2)}\right)^d \delta_k(\alpha) \right)^{d_{n+1}}, \\ &\leq \left(\left(N_2^{(1)} N_2^{(2)}\right)^d \delta_k(\alpha) \right)^2, \end{aligned}$$

car par construction de l_1 , on a $\delta_k(\Phi_{l_1}(\alpha)) \leq \delta_k(\alpha)$.

Second cas : $n' = 0$ et $n = 1$

$$\begin{aligned} \deg_k(Z_0) &\leq (|l_1 l_2|^d \delta_k(\Phi_{l_1 l_2}(\alpha)))^{2-d_{n+1}} \deg_k(W_0)^{d_{n+1}}, \\ &\leq \left(\left(N_2^{(1)} N_2^{(2)} \right)^d \delta_k(\Phi_{l_1 l_2}(\alpha)) \right)^{2-d_{n+1}} \left(\left(N_2^{(1)} N_2^{(2)} \right)^d \delta_k(\alpha) \right)^{d_{n+1}}, \\ &\leq \left(\left(N_2^{(1)} N_2^{(2)} \right)^d \delta_k(\alpha) \right)^2, \end{aligned}$$

car ici encore, on a les inégalités $\delta_k(\Phi_{l_1 l_2}(\alpha)) \leq \delta_k(\Phi_{l_1}(\alpha)) \leq \delta_k(\alpha)$.

Troisième cas : $n' = n = 1$

$$\begin{aligned} \deg_k(Z_1) &\leq (|l_2|^d \delta_k(\Phi_{l_1 l_2}(\alpha)))^{2-d_{n+1}} \deg_k(W_1)^{d_{n+1}}, \\ &\leq \left(\left(N_2^{(2)} \right)^d \delta_k(\Phi_{l_1 l_2}(\alpha)) \right)^{2-d_{n+1}} \left(\left(N_2^{(2)} \right)^d \delta_k(\Phi_{l_1}(\alpha)) \right)^{d_{n+1}}, \\ &\leq \left(\left(N_2^{(2)} \right)^d \delta_k(\Phi_{l_1}(\alpha)) \right)^2. \end{aligned}$$

Ainsi, dans chacun des cas la propriété (iii) est bien satisfaite, par suite $(n', \mathbf{l}', \mathbf{Z})$ appartient à $\mathcal{W} \setminus \mathcal{W}_0$; la proposition 18 est donc établie. $\square$

7.5. Preuve du théorème principal

On termine cette démonstration en obtenant une contradiction. D'après ce qui précède, on peut trouver deux k -variétés V_{i-1} et V_i de même dimension, et telles qu'il existe $l_i \notin E(V_{i-1})$ pour lequel on a l'inclusion

$$V_{i-1} \subset \Phi_{l_i}^{-1}(V_i).$$

De plus, $\Phi_{l_1 \dots l_{i-1}}(\alpha) \in V_{i-1}$, et on a la majoration

$$\deg_k(V_i) \leq \left(\left(N_2^{(i+1)} N_2^{(2)} \right)^d \delta_k(\Phi_{l_1 \dots l_i}(\alpha)) \right)^{\text{codim} V_i}.$$

Or, il résulte de l'assertion (iii) de la proposition 13 que $\deg_k(V_{i-1}) \leq \deg_k(V_i)$.

Si i était égal à 2, alors on aurait

$$\begin{aligned} \delta_k(\Phi_{l_1}(\alpha)) &\leq (\deg_k(V_1))^{1/\text{codim} V_1} \leq (\deg_k(V_2))^{1/\text{codim} V_2}, \\ &\leq \delta_k(\Phi_{l_1 l_2}(\alpha)), \\ &\leq \varepsilon_2 \delta_k(\Phi_{l_1}(\alpha)) < \delta_k(\Phi_{l_1}(\alpha)), \end{aligned}$$

qui est impossible, on a donc $i = 1$.

$$\begin{aligned} \delta_k(\alpha) &\leq (\deg_k(V_0))^{1/\text{codim} V_0} \leq (\deg_k(V_1))^{1/\text{codim} V_1}, \\ &\leq \left(N_2^{(2)} \right)^d \delta_k(\Phi_{l_1}(\alpha)) \leq \varepsilon_1 \left(N_2^{(2)} \right)^d \delta_k(\alpha). \end{aligned}$$

Or, par choix des paramètres, on a $\varepsilon_1 \left(N_2^{(2)} \right)^d < 1$. L'inégalité précédente est donc fausse, ce qui donne la contradiction finale attendue, et achève la preuve du théorème C. $\square$

8 - Cas particuliers

8.1. Carré de Carlitz

Soit $(\mathbb{G}_a^2, \Phi) = (\mathbb{G}_a^2, C \times C)$ le T -module de dimension 2, produit de deux modules de Carlitz. Il est clair que dans ce cas, la matrice dominante de Φ_T est inversible, et que l'exponentielle associée à Φ est surjective. On sait de plus, que pour b dans A , les points de b -torsion de C sont les $e_c(\tilde{\pi}r/b)$ où $r \in A$, et où e_c désigne la fonction exponentielle associée à C . Les points de b -torsion de Φ sont donc les

$$\mathbf{x}_{r_1, r_2} = (e_c(\tilde{\pi}r_1/b), e_c(\tilde{\pi}r_2/b)),$$

où r_1, r_2 sont dans A . On détermine maintenant les points de b -torsion primitive.

$$\begin{aligned} \forall m \in A \quad \Phi_m(\mathbf{x}_{r_1, r_2}) = 0 &\iff \frac{mr_1}{b}, \frac{mr_2}{b} \in A, \\ &\iff b \mid (mr_1, mr_2) = m(r_1, r_2). \end{aligned}$$

Donc $\mathbf{x}_{r_1, r_2}$ est un point de b -torsion primitive si et seulement si on a $(b, r_1, r_2) = 1$. En particulier, si r_1 ou si r_2 est premier avec b , alors $\mathbf{x}_{r_1, r_2}$ est un point de b -torsion primitive. On notera $\Phi_{\text{prim}}[b]$ l'ensemble des points de b -torsion primitive.

Il est vu dans [Ca], que les k -isomorphismes du corps $k_b = k(e_c(\tilde{\pi}/b))$ sont les

$$\sigma_r : e_c(\tilde{\pi}/b) \longmapsto e_c(\tilde{\pi}r/b)$$

où $r \in A$ est premier avec b . Ainsi, les conjugués de $\mathbf{x}_{r_1, r_2}$ sont les $\mathbf{x}_{rr_1, rr_2}$ où $r \in A$ est premier avec b . En particulier, deux points de b -torsion primitive ne sont pas nécessairement conjugués sur k . Par exemple, soit $b = T(T+1)$. Les deux points $(e_c(\tilde{\pi}/T), e_c(\tilde{\pi}/(T+1)))$ et $(e_c(\tilde{\pi}/T(T+1)), e_c(\tilde{\pi}/T(T+1)))$ ne seront jamais image l'un de l'autre par l'un des isomorphismes σ_r .

Cependant, si $b \in A$, et si $u \in A$ est premier à b , et de degré strictement plus petit que celui de b , alors pour tout point $\mathbf{x}_{r_1, r_2}$ de b -torsion primitive, le point

$$\Phi_u(\mathbf{x}_{r_1, r_2}) = \sigma_u(\mathbf{x}_{r_1, r_2})$$

est un point de b -torsion primitive conjugué de $\mathbf{x}_{r_1, r_2}$. Il reste à vérifier que les $\Phi_u(\mathbf{x}_{r_1, r_2})$ sont distincts quand u parcourt l'ensemble des éléments de A premiers avec b , de degré strictement plus petit que celui de b . En effet, comme $(b, r_1, r_2) = 1$, alors pour tout $u, v \in A$ on a l'équivalence suivante

$$\Phi_u(\mathbf{x}_{r_1, r_2}) = \Phi_v(\mathbf{x}_{r_1, r_2}) \iff u - v \in bA.$$

En particulier, à chaque $u \in A$ irréductible et unitaire, ne divisant pas b et de degré strictement inférieur à $\deg(b)$, correspond un conjugué de tout point de b -torsion primitive. Or, il existe $\kappa > 0$ tel que

$$\text{card}\{u \in A_{\text{irr}}^+, \deg u < \deg b\} \geq \frac{\kappa|b|}{\log(3|b|)}.$$

Or, il y a au plus $\log_q |b|$ éléments de A irréductibles et unitaires qui divisent b . Par conséquent, $(\mathbb{G}_a^2, \Phi)$ vérifie l'hypothèse (Gal 1). De plus, soit $v \in A$ premier avec b et soient $\Phi_u(\mathbf{x}_{r_1, r_2})$ et $\Phi_{u'}(\mathbf{x}_{r_1, r_2})$ deux conjugués de $\mathbf{x}_{r_1, r_2}$ vérifiant

$$\Phi_v(\Phi_u(\mathbf{x}_{r_1, r_2})) = \Phi_v(\Phi_{u'}(\mathbf{x}_{r_1, r_2})).$$

Alors $\Phi_v(\Phi_{u-u'}(\mathbf{x}_{r_1, r_2}))$ est nul, et donc b divise $v(u - u')$. Comme v et b sont premiers entre eux, on a aussi $b|(u - u')$ et par conséquent l'égalité

$$\Phi_u(\mathbf{x}_{r_1, r_2}) = \Phi_{u'}(\mathbf{x}_{r_1, r_2}).$$

Ainsi, Φ_v est bien une permutation de la classe de conjugaisons sur k , de tout point de b -torsion primitive. Et donc $(\mathbb{G}_a^2, \Phi)$ vérifie aussi l'hypothèse (Gal 2).

On s'intéresse maintenant à l'hypothèse (H). Soit G un sous-groupe algébrique connexe de $\mathbb{G}_a^2(\bar{k})$, pour lequel il existe un élément a de A non constant, tel que $\Phi_a(G) \subset G$. D'après la proposition du paragraphe 7.3 de [Hu] (page 53), G est une $\bar{k}$ -variété, puisque $\Phi_a(G)$ et G ont même dimension, on a l'égalité

$$\Phi_a(G) = G.$$

Alors, d'après le lemme 4 de [De1], comme $(\mathbb{G}_a^2, \Phi)$ est produit direct de modules de Drinfeld, cela entraîne que G est le translaté d'un sous- T -module de $(\mathbb{G}_a^2, \Phi)$. Mais G est un groupe, donc il est lui-même ce sous- T -module. Ainsi, $(\mathbb{G}_a^2, \Phi)$ vérifie l'hypothèse (H).

Enfin, d'après la proposition 2.4 de [Ha], l'hypothèse $(\mathcal{H}_{\nu_0})$ est vérifiée pour tout $\nu_0 \in A$ irréductible et unitaire. Toutes les conditions sont donc réunies pour obtenir le corollaire suivant du théorème C.

Corollaire 1. *Soit $(\mathbb{G}_a^2, C \times C)$ le T -module de dimension 2, produit de deux modules de Carlitz. On note $\hat{h}_1$ sa hauteur canonique associée. Alors, il existe une constante $C'_0 > 0$ telle que pour tout $\alpha \in \mathbb{G}_a^2(\bar{k})$ séparable de degré D sur k , et qui n'est pas de torsion pour les sous- T -modules de $C \times C$, on ait la minoration*

$$\hat{h}_1(\alpha) \geq \frac{C'_0}{D^{1/2}} \frac{(\log \log(3D))^{31}}{(\log(3D))^{62}}.$$

8.2. Carré de module de Drinfeld de rang 2

Dans ce paragraphe, $(\mathbb{G}_a^2, \varphi \times \varphi)$ est le carré d'un module de Drinfeld de rang 2 à multiplications complexes.

$$\varphi_T = T\mathcal{F}^0 + a_1\mathcal{F} + a_2\mathcal{F}^2.$$

Ainsi, il existe $\tau_0 \in \bar{k}$ quadratique et entier sur k , tel que $R_\Lambda = A[\tau_0]$. L'endomorphisme φ se prolonge à R_Λ . On note $k(\varphi_\tau)$ l'extension de k engendrée par les coefficients de φ_τ . Soit (w_1, w_2) une base du réseau Λ associé à φ ; on pose $\eta = w_2/w_1$. Les nombres $\tau_0 w_1$ et $\tau_0 w_2$ étant dans Λ , on peut écrire

$$\begin{aligned} \tau_0 &= r + s\eta, \\ \tau_0 \eta &= r' + s'\eta, \end{aligned}$$

où r, s, r' et s' sont des éléments de A .

Ces deux équations donnent en particulier l'égalité

$$s\eta^2 + (r - s')\eta - r' = 0.$$

Ainsi η est aussi quadratique sur k . On pose alors $\tau = s\eta$. Comme $\tau_0 = r + \tau$, on a encore $R_\Lambda = A[\tau]$. On note enfin $w = w_1/s$, alors la base (w_1, w_2) est aussi la base $(sw, \tau w)$.

Soit $b \in A$, et z un point de b -torsion primitive de φ . Il s'écrit donc

$$z = e_\varphi((b_1sw + b_2\tau w)/b) = \varphi_{b_1s + \tau b_2}(e_\varphi(w/b)),$$

où $(b_1, b_2) \in A^2$ vérifie $(b, b_1, b_2) = 1$, et où e_φ désigne la fonction exponentielle associée à φ . Comme pour le carré de Carlitz, on est amené à trouver des conjugués de $z_0 = e_\varphi(w/b)$ sur $k(\varphi_\tau)$. On écrit pour cela $a_2 = \lambda/\mu \in k$ où $\lambda, \mu \in A$ sont premiers entre eux, et on définit les ensembles suivants

$$(49) \quad \begin{aligned} H(\varphi) &= \{\nu \in A_{\text{irr}}^+, (\nu, s\lambda\mu) = 1, \varphi_\nu(X) \equiv X^{q^{2 \deg \nu}} \pmod{\nu}\}, \\ G(\varphi) &= \{\nu \in H(\varphi), \mathcal{O}_\nu(k(\varphi_\tau))/(\nu\mathcal{O}_\nu(k(\varphi_\tau))) \subset \mathbb{F}_{q^{2 \deg \nu}}\}. \end{aligned}$$

On impose alors à φ de vérifier la minoration suivante

$$(50) \quad \exists \kappa_0 > 0, \quad \exists t > 1, \quad \forall m \in \mathbb{N} \setminus \{0, 1\}, \quad \text{card} \{\nu \in G(\varphi), |\nu| \leq m\} \geq \frac{\kappa_0 m^{1/t}}{\log m}.$$

Le nombre $z_0 = e_\varphi(w/b)$ est une racine de $\varphi_{sb}(X)$, il est donc séparable sur $k(\varphi_\tau)$. De plus, pour tout $u \in H(\varphi)$, z_0 est entier sur A_u . Soit alors $P \in \mathcal{O}(k(\varphi_\tau))[X]$ un polynôme minimal de z_0 . On va montrer que si $u \in G(\varphi)$ est premier avec b , alors $P(\varphi_u(z_0)) = 0$, ainsi $\varphi_u(z_0)$ et z_0 seront bien conjugués sur $k(\varphi_\tau)$ donc sur k . Quitte à multiplier P par une constante, on peut supposer que $P \in \mathcal{O}_u(k(\varphi_\tau))[X]$ est unitaire.

Comme z_0 est racine de $\varphi_{sb}(X)$, le polynôme $P(X)$ divise $\varphi_{sb}(X)$. Ainsi, il existe un polynôme $h(X) \in \mathcal{O}_u(k(\varphi_\tau))[X]$ pour lequel on a

$$\varphi_{sb}(X) = h(X)P(X).$$

D'autre part, $\varphi_u(z_0)$ est racine de $\varphi_{sb}(X)$, donc s'il n'annule pas $P(X)$, alors il annule $h(X)$. Par conséquent, il existe $g(X) \in \mathcal{O}_u(k(\varphi_\tau))[X]$ vérifiant

$$h \circ \varphi_u(X) = g(X)P(X).$$

Comme $\mathcal{O}_u(k(\varphi_\tau))/(\nu\mathcal{O}_u(k(\varphi_\tau)))$ est contenu dans $\mathbb{F}_{q^{2 \deg(u)}}$ et comme u appartient à $H(\varphi)$, modulo u on a l'égalité

$$(h(X))^{q^{2 \deg u}} \equiv P(X)g(X) \pmod{u}.$$

Soit alors θ une racine de $P(X)$ modulo u , c'est aussi une racine de $h(X)$ modulo u . Par suite, c'est une racine double de $\varphi_{sb}(X)$. Or, $\varphi'_{sb}(X) = sb$ n'a pas de racine modulo u , donc φ_{sb} n'a pas de racine double modulo u . Ainsi, nécessairement on a $P(\varphi_u(z_0)) = 0$.

Sachant que si $\mathbf{z} = (z_1, z_2)$ est un point de b -torsion primitive pour Φ alors $k(\varphi_\tau)(\mathbf{z})$ est un sous-corps de $k(\varphi_\tau)(z_0)$, on montre facilement le lemme suivant par récurrence.

Lemme 11. Soient $b \in A$ et $\mathbf{z} = (z_1, z_2)$ un point de b -torsion primitive pour $\Phi = \varphi \times \varphi$. Alors, pour tout $u \in A$ produit d'éléments de $G(\varphi)$ premiers avec b , le point

$$\Phi_u(\mathbf{z}) = (\varphi_u(z_1), \varphi_u(z_2))$$

est un conjugué sur $k(\varphi_\tau)$ de $\mathbf{z}$.

Comme pour le carré de Carlitz, pour obtenir l'hypothèse (Gal 1), il suffit de minorer le cardinal de l'ensemble

$$G_{|b|}(\varphi) = \{\nu_0 \in G(\varphi), \text{ tel que } |\nu_0| \leq |b|\}.$$

D'après les travaux de M.L. Brown [B], on sait que dans le cas où φ est à multiplications complexes, on a

$$\exists \kappa > 0, \quad \forall m \in \mathbb{N} \setminus \{0, 1\}, \quad \text{card}(H_m(\varphi)) \geq \frac{\kappa m}{\log \log(3m)}.$$

Ainsi, l'hypothèse de Fermat est bien vérifiée, et sous la condition (50), le T -module $\Phi = \varphi \times \varphi$ satisfait aussi la condition (Gal 1). De plus, d'après le lemme 11, si $v \in A$ est premier avec b et est produit d'éléments de $G(\varphi)$, alors pour tout point $\mathbf{x}$ de b -torsion primitive, $\mathbf{x}$ et $\mathbf{y} = \Phi_v(\mathbf{x})$ sont conjugués sur k . Par conséquent s'il existe $\sigma \in \text{Aut}(\bar{k}/k)$ tel que

$$\Phi_v(\mathbf{x}) = \Phi_v(\sigma(\mathbf{x})),$$

alors $\mathbf{y} = \sigma(\mathbf{y})$ et donc $\mathbf{x} = \sigma(\mathbf{x})$.

Ainsi Φ_v est une permutation de la classe de conjugaison du point $\mathbf{x}$. L'hypothèse (Gal 2) n'est donc pas vérifiée telle qu'elle est écrite, mais on peut reprendre la démonstration du théorème C en remplaçant les ensembles

$$\mathcal{P}_j^{(i)} = \{1\} \cup \{a \in H_{N_j}(\Phi), \log(3D) \leq |a| \leq N_j^{(i)}\}$$

par les ensembles

$$\{1\} \cup \{a \in G_{N_j}(\varphi), \log(3D) \leq |a| \leq N_j^{(i)}\}.$$

En effet, d'une part les nombres a et b auxquels on applique les propositions 12 et 13 seront toujours des produits d'éléments de $G(\varphi)$, et d'autre part, si T n'est pas dans $G(\varphi)$, on peut le remplacer dans la preuve de la proposition 12 par un élément u_0 fixé dans $G(\varphi)$.

Enfin, l'hypothèse (H) se vérifie de la même façon que pour $C \times C$ dans le paragraphe précédent. Toutes les conditions sont donc réunies pour obtenir le corollaire suivant.

Corollaire 2. Soit $(\mathbb{G}_a^2, \varphi \times \varphi)$ le carré d'un module de Drinfeld de rang 2 à multiplications complexes. On note $\hat{h}_2$ sa hauteur canonique associée. On suppose que l'on a

$$\exists \kappa_0 > 0, \quad \exists t > 1, \quad \forall m \in \mathbb{N} \setminus \{0, 1\}, \quad \text{card} \{u \in G(\varphi), |u| \leq m\} \geq \frac{\kappa_0 m^{1/t}}{\log m},$$

où l'ensemble $G(\varphi)$ a été défini précédemment.

Alors, il existe une constante $C_0'' > 0$ telle que pour tout $\alpha \in \mathbb{G}_a^2(\bar{k})$ séparable de degré D sur k , et qui n'est pas de torsion pour les sous- T -modules de $\varphi \times \varphi$, on ait la minoration

$$\hat{h}_2(\alpha) \geq \frac{C_0''}{D^{1/2}} \frac{(\log \log(3D))^{100t+2}}{(\log(3D))^{202t^4+3}}.$$

8.3. Puissance tensorielle de Carlitz

On considère dans cette partie des T -modules plus généraux que ceux définis dans l'introduction. Soient $n \geq 1$ et $d \geq 1$ deux entiers, et soit E une extension finie de k . On appellera T -module de dimension n , de degré d , défini sur E , tout couple $(\mathbb{G}_a^n, \Phi)$ où Φ est un homomorphisme injectif d'anneaux vérifiant

$$\Phi : \begin{cases} A & \longrightarrow & \text{End}_E(\mathbb{G}_a^n) \\ T & \longmapsto & \Phi_T = a_0 \mathcal{F}^0 + \dots + a_d \mathcal{F}^d \end{cases}$$

où les a_i ($i = 0, \dots, d$) sont des matrices $n \times n$ à coefficients dans E avec $a_d \neq 0$, et où $\mathcal{F}$ est l'endomorphisme de Frobenius sur $\mathbb{G}_a^n$:

$$\mathcal{F} : (x_1, \dots, x_n) \longmapsto (x_1^q, \dots, x_n^q).$$

La seule différence avec la première définition est que l'on ne suppose plus ici, que T est la seule valeur propre de a_0 . Cette hypothèse a permis en particulier d'alléger la démonstration du lemme 5. Néanmoins, ce résultat est encore valable dans certains cas, notamment celui où a_0 n'a que T^n comme valeur propre. Ici, on s'intéresse à un T -module particulier, induit par la puissance tensorielle de Carlitz.

On rappelle tout d'abord la définition de la puissance tensorielle du module de Carlitz.

$$C^{\otimes n} : T \longmapsto \begin{pmatrix} T & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & T \end{pmatrix} \mathcal{F}^0 + \begin{pmatrix} 0 & \dots & \dots & 0 \\ \vdots & & & \vdots \\ 0 & & & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix} \mathcal{F}^1$$

Le T -module induit $(\mathbb{G}_a^n, \Phi^{(n)})$ est alors défini par l'égalité $\Phi_T^{(n)} = C_{T^n}^{\otimes n}$. La matrice dominante de $\Phi_T^{(n)}$ est inversible, et T^n est la seule valeur propre de a_0 . Ainsi, a_0 s'écrit $a_0 = T^n I_n + N$ où N est une matrice nilpotente. La preuve du lemme 5, s'adapte ici sans problème si l'on pose $[m] = T^{nq^m} - T^n$ au lieu de $T^{q^m} - T$. On obtient ainsi une fonction exponentielle dont les coefficients de Taylor ont une estimation du même ordre que celle donnée dans le lemme 5.

Avant de s'intéresser aux hypothèses galoisiennes, on rappelle le lemme élémentaire suivant.

Lemme 12. *Soit K un corps et L une extension finie de K de degré r . Soit $a(T)$ un polynôme irréductible de $K[T]$. Si le degré de $a(T)$ est premier avec r , alors $a(T)$ reste irréductible dans $L[T]$.*

Pour $b \in A$ non nul, G.W. Anderson et D.S. Thakur ont montré dans [AnT] les deux propositions suivantes.

- (1) Pour tout $u \in A$ tel que $(u, b) = 1$, $C_{u^2}^{\otimes 2}$ est la restriction à l'ensemble des points de b -torsions pour $C^{\otimes 2}$ d'un élément de $\text{Gal}(k^{\text{sep}}/k)$.
- (2) Pour tout $u \in A_{\text{irr}}^+$, on a $C_{u^2}^{\otimes 2}(X_1, X_2) \equiv (X_1^{q^{\deg u}}, X_2^{q^{\deg u}}) \pmod{u}$.

On fixe désormais $p = 2$ et $q = 2^r$ où $r \in \mathbb{N} \setminus \{0\}$. Pour tout $u(T) \in \mathbb{F}_2[T]$, $u^2(T)$ est égal à $u(T^2)$. Ainsi, pour tout $u \in \mathbb{F}_2[T]$ premier avec b , $\Phi_{u(T)}^{(2)} = C_{u(T^2)}^{\otimes 2}$ est la restriction à l'ensemble des points de b -torsions pour $\Phi^{(2)}$ d'un élément de $\text{Gal}(k^{\text{sep}}/k)$. De plus, il est clair que pour tout point $\mathbf{z}$ de b -torsion primitive, si l'on a $\Phi_u^{(2)}(\mathbf{z}) = \Phi_v^{(2)}(\mathbf{z})$ alors b divise $u - v$. Or, d'après le lemme 12, tout élément de $\mathbb{F}_2[T]$ irréductible et de degré premier avec r reste irréductible dans $A = \mathbb{F}_q[T] = \mathbb{F}_{2^r}[T]$. Par conséquent, comme pour le carré de Carlitz, tout point de b -torsion primitive possède au moins $|b|^{C(\Phi)}$ conjugués sur k , où $C(\Phi)$ peut être pris égal à $1/2r$.

La proposition (2) ci-dessus donne de plus pour tout $u(T) \in \mathbb{F}_2[T] \cap A_{\text{irr}}^+$, la congruence suivante

$$\Phi_{u(T)}^{(2)}(X_1, X_2) \equiv (X_1^{q^{\deg u}}, X_2^{q^{\deg u}}) \pmod{u}.$$

On définit alors l'ensemble suivant

$$G_m(\Phi^{(2)}) = \{\nu \in \mathbb{F}_2[T] \cap A_{\text{irr}}^+, (\mathcal{H}_\nu) \text{ vérifiée et } |\nu| \leq m\}.$$

Comme pour le carré de modules de Drinfeld à multiplications complexes, l'hypothèse (Gal 2) n'est pas vérifiée. Cependant, le lemme 12 joint à la proposition (2) donnent une minoration de l'ensemble $G_m(\Phi^{(2)})$:

$$\exists C > 0, \quad \forall m \in \mathbb{N} \setminus \{0, 1\}, \quad \text{card}(G_m(\Phi^{(2)})) \geq \frac{Cm^{1/r}}{\log m}.$$

Si $b \in A$ alors pour tout $u \in G_m(\Phi^{(2)})$ premier avec b , $\Phi_u^{(2)}$ est une permutation de la classe de conjugaison sur k de tout point de b -torsion primitive. Comme précédemment, la preuve du théorème C s'adapte en modifiant les ensembles $\mathcal{P}_j^{(i)}$.

Malheureusement, à ce jour, l'hypothèse (H) n'est pas connue pour les puissances tensorielles $C^{\otimes n}$. On obtient donc le corollaire « conditionnel » suivant.

Corollaire 3. *Soit $(\mathbb{G}_a^2, \Phi^{(2)})$ le T -module induit par la puissance tensorielle de Carlitz $(\mathbb{G}_a^2, C^{\otimes 2})$. On note $\hat{h}_3$ sa hauteur canonique associée. On suppose que la caractéristique du corps $k = \mathbb{F}_q(T)$ est égale à 2, et que $q = 2^r$. Si $(\mathbb{G}_a^2, \Phi^{(2)})$ vérifie l'hypothèse (H), alors il existe une constante $\widetilde{C}_0 > 0$ telle que pour tout $\alpha \in \mathbb{G}_a^2(\bar{k})$ séparable de degré D sur k , et qui n'est pas de torsion pour les sous- T -modules de $\Phi^{(2)}$, on ait*

$$\hat{h}_3(\alpha) \geq \frac{\widetilde{C}_0}{D^{1/2}} \frac{(\log \log D)^{29r+2}}{(\log D)^{59r^4+3}}.$$

Annexe : un lemme de zéros

On montre dans cette annexe un lemme de zéros qui, lorsqu'on ne tient pas compte de la multiplicité, donne une meilleure majoration du degré de la variété construite que celle donnée dans le paragraphe 5. On note comme précédemment $\deg(V)$ le degré sur $\bar{k}$ d'un ensemble algébrique V . Soit Φ un T -module de dimension n défini sur une extension finie E de k , soient $\alpha = (\alpha_1, \dots, \alpha_n)$ un point de $\mathbb{G}_a^n(\bar{k})$, et $N_1, \dots, N_n$ des entiers non nuls. Pour $j = 1, \dots, n$ on fixe aussi des ensembles $\mathcal{P}_j$ tels que :

$$1 \in \mathcal{P}_j \subset \{a \in A, \deg a \leq N_j\}.$$

On définit encore :

$$\begin{aligned} \Sigma_j &= \{\Phi_{a_j \dots a_n}(\alpha), (a_j, \dots, a_n) \in \mathcal{P}_j \times \dots \times \mathcal{P}_n\}, \quad \text{si } j = 1, \dots, n, \\ \Sigma_{n+1} &= \{\alpha\}. \end{aligned}$$

Ainsi, pour $j = 1, \dots, n$ et $a \in \mathcal{P}_j$, on a l'inclusion

$$\Phi_a(\Sigma_{j+1}) \subset \Sigma_j.$$

Pour $j = 2, \dots, n$, on note enfin $\mathcal{Q}_j = \{a_1 \dots a_{j-1}, a_i \in \mathcal{P}_i\}$.

On se propose de montrer le résultat suivant.

Proposition. *Soit $F \in E[X_1, \dots, X_n]$ un polynôme non nul de degré $\leq L$, s'annulant sur Σ_1 . Il existe un entier $r \in \{1, \dots, n\}$ et une E -variété algébrique V propre de $\mathbb{G}_a^n(\bar{E})$ rencontrant Σ_{r+1} et de codimension $\leq r$, telle que l'on ait*

$$\deg \left(\bigcup_{a \in \mathcal{P}_r} \Phi_a(V) \right) \leq L(N_1 \dots N_{r-1} L)^{\text{codim} V - 1}.$$

Preuve - On commence la preuve comme le font F. Amoroso et S. David dans [AD]. Pour ne pas alourdir les notations, comme eux on écrira encore F son homogénéisé

$$X_0^{\deg F} F \left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0} \right),$$

et α le point projectif $(1, \alpha_1, \dots, \alpha_n)$. On considère les ensembles algébriques projectifs $(\mathcal{X}_j)_{j=1, \dots, n+1}$ définis comme suit :

$$\mathcal{X}_1 = Z(F(\mathbf{X})) = \{(x_0 : \dots : x_n) \in \mathbb{P}_n(\bar{E}), F(x_0 : \dots : x_n) = 0\},$$

$$\mathcal{X}_j = \bigcap_{a \in \mathcal{Q}_j} Z(F \circ \Phi_a(\mathbf{X})), \quad \text{pour } j = 2, \dots, n+1.$$

On a alors $\forall a \in \mathcal{P}_j, \forall j = 1, \dots, n, \quad \Phi_a(\mathcal{X}_{j+1}) \subset \mathcal{X}_j$.

Pour $j = 1, \dots, n$, on note $\mathcal{Y}_j$ la réunion des E -composantes isolées de $\mathcal{X}_j$ rencontrant Σ_j . Le polynôme F s'annule sur Σ_1 , donc $\Sigma_j \subset \mathcal{X}_j$. Ainsi $\mathcal{Y}_j$ n'est pas vide. De plus, pour $a \in \mathcal{P}_j$ et pour $j = 1, \dots, n$, l'inclusion suivante a lieu.

$$\Phi_a(\mathcal{Y}_{j+1}) \subset \mathcal{Y}_j.$$

Car si V est une composante isolée de $\mathcal{X}_{j+1}$ rencontrant Σ_{j+1} , alors d'une part on a $\Phi_a(V) \subset \mathcal{X}_j$, et d'autre part $\Phi_a(V) \cap \Sigma_j$ n'est pas vide. Donc $\Phi_a(V)$ est contenue dans une E -composante de $\mathcal{X}_j$ rencontrant Σ_j .

Puisque les ensembles $\mathcal{P}_j$ contiennent l'élément 1, on a les inclusions

$$\mathcal{Y}_{n+1} \subset \mathcal{Y}_n \subset \dots \subset \mathcal{Y}_1.$$

Par le principe des tiroirs, il existe donc un indice r , que l'on choisit maximal, pour lequel on a $\dim \mathcal{Y}_r = \dim \mathcal{Y}_{r+1} = d$ et aussi $n - d \leq r$. Soit V une E -composante de dimension d de $\mathcal{Y}_{j+1}$, et $W = \bigcup_{a \in \mathcal{P}_r} \Phi_a(V) \subset \mathcal{Y}_r$ (car $\Phi_a(\mathcal{Y}_{r+1}) \subset \mathcal{Y}_r$).

Pour terminer la preuve du lemme de zéros, on montre le résultat suivant.

Lemme. *Soit $s \in \{1, \dots, n - d\}$. Alors il existe un ensemble algébrique $\mathcal{Z}_s$ défini sur E , équidimensionnel, de dimension $n - s$, contenant W , et dont toutes les composantes E -irréductibles rencontrent Σ_r , telle que l'on ait*

$$\deg(\mathcal{Z}_s) \leq L(N_1 \dots N_{r-1} L)^{s-1}.$$

Preuve - On procède par récurrence sur s .

Pour $s = 1$:

Soit F_1 un diviseur de F tel que $F = F_1 \times G$, où G est de degré maximal pour lequel on ait

$$\forall x \in \Sigma_r, \quad G(x) \neq 0.$$

Ainsi le polynôme F_1 est produit des facteurs E -irréductibles de F qui s'annulent au moins en un élément de Σ_r . Il est homogène. On choisit $\mathcal{Z}_1 = Z(F_1)$. Il est clair que $\dim(\mathcal{Z}_1) = n - 1$, que $\mathcal{Z}_1$ contient $\mathcal{Y}_r$, donc aussi W , et que ses composantes E -irréductibles rencontrent Σ_r .

Soit $s < n - d$ pour lequel le lemme est vérifié.

On décompose $\mathcal{Z}_s = \mathcal{Z}'_1 \cup \dots \cup \mathcal{Z}'_l$ où les $\mathcal{Z}'_i$ sont E -irréductibles. On sait que

$$\dim(\mathcal{Z}'_i) = \dim(\mathcal{Z}_s) = n - s > d = \dim(\mathcal{Y}_r).$$

De plus, chaque $\mathcal{Z}'_i$ rencontre Σ_r , donc, par définition de $\mathcal{Y}_r$, l'ensemble algébrique $\mathcal{Z}'_i$ n'est pas contenu dans $\mathcal{X}_r = \bigcap_{a \in \mathcal{Q}_r} Z(F \circ \Phi_a(\mathbf{X}))$, ce qui s'écrit encore :

$$\forall i = 1, \dots, l, \quad \exists a_i \in \mathcal{Q}_r, \quad \mathcal{Z}'_i \not\subset Z(F \circ \Phi_{a_i}(\mathbf{X})).$$

On note $S_i = \mathcal{Z}'_i \cap Z(F \circ \Phi_{a_i}(\mathbf{X}))$. L'ensemble algébrique $\bigcup_{i=1}^l S_i$ est équidimensionnel, on prend pour $\mathcal{Z}_{s+1}$ la réunion des composantes E -irréductibles de $\bigcup_{i=1}^s S_i$, qui rencontrent Σ_r .

Alors Z_{s+1} est clairement équidimensionnelle de dimension $n - s - 1$. De plus, le théorème de Bezout donne les inégalités

$$\begin{aligned} \deg(S_i) &\leq \deg(Z'_i) \deg(F \circ \Phi_{a_i}(\mathbf{X})), \\ &\leq \deg(Z'_i) \times N_1 \dots N_{r-1} L. \end{aligned}$$

On a donc les majorations successives suivantes

$$\begin{aligned} \deg Z_{s+1} &\leq \sum_{i=1}^l \deg S_i, \\ &\leq N_1 \dots N_{r-1} L \left(\sum_{i=1}^l \deg(Z'_i) \right), \\ &\leq N_1 \dots N_{r-1} L \times \deg(Z_s), \\ &\leq L(N_1 \dots N_{r-1} L)^s. \end{aligned}$$

Il reste à montrer l'inclusion $W \subset Z_{s+1}$. En effet, $W = \bigcup_{a \in \mathcal{P}_r} \Phi_a(V)$ est une union de E -composantes de $\mathcal{Y}_r$, de même dimension d . Par construction de $\mathcal{Y}_r$, chacune de ces composantes rencontre Σ_r . Or on a :

$$\bigcup_{i=1}^l S_i = \bigcup_{i=1}^l \left(\mathcal{Z}'_i \cap Z(F \circ \Phi_{a_i}(\mathbf{X})) \right) \supset \bigcup_{i=1}^l (\mathcal{Z}'_i \cap W) \supset \left(\bigcup_{i=1}^l \mathcal{Z}'_i \right) \cap W = W.$$

Ainsi chaque composante de W est contenue dans une composante de $\bigcup_{i=1}^n S_i$ rencontrant Σ_r . Donc W est inclus dans Z_{s+1} . □

Pour terminer la preuve du lemme de zéros, on utilise le lemme précédent en prenant $s = n - d$. Alors, $W \subset Z_{n-d}$, et ces deux variétés ont même dimension d . Ainsi, on a les majorations

$$\deg(W) \leq \deg(Z_{n-d}) \leq L(N_1 \dots N_{r-1} L)^{n-d-1},$$

d'où le résultat annoncé. □

On remarque qu'en général, on n'a pas de supplément galoisien à cette proposition, car les composantes $\overline{E}$ -irréductibles des E -variétés W et Z_{n-d} peuvent ne pas être géométriquement réduites sur E . Cependant, comme dans la preuve du théorème C, lorsque la dimension est égale à 2 et quand α et F sont séparables sur E , on obtient une majoration du degré sur E de la E -variété W .

Références

- [AD] F. Amoroso et S. David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math. **513** (1999), 145-179.
- [An] G.W. Anderson, *t-motives*, Duke Math. J. **53** (1986), n° 2, 457-502.
- [AnT] G.W. Anderson et D.S. Thakur, *Tensor powers of the Carlitz module and zeta values*, Ann. of Math. (2) **132** (1990), n° 1, 159-191.
- [ADR] M. Ably, L.Denis et F. Recher, *Transcendance de l'invariant modulaire en caractéristique finie*, Math. Z. **231** (1999), n° 1, 75-89.
- [Ba] S. Bae, *On the modular equation for Drinfeld modules of rank 2*, J. Number Theory **42** (1992), n° 2, 123-133.
- [BS et al.] K. Barré-Sirieix, G. Diaz, F. Gramain et G. Philibert, *Une preuve de la conjecture de Mahler-Manin*, Invent. Math. **124** (1996), 1-9.
- [BGR] Bosch-Güntzer-Remmert, *Non Archimedean Analysis*, Springer (1984).
- [B1] V. Bosser, *Minorations de formes linéaires de logarithmes pour les modules de Drinfeld*, J. Number Theory **75** (1999), n° 2, 279-323.
- [B2] V. Bosser, Thèse.
- [B] M.L. Brown, *Singular moduli and supersingular moduli of Drinfeld modules*, Invent. Math. **110** (1992), n° 2, 419-439.
- [Br] W.D. Brownawell, *The algebraic independence of certain numbers related by the exponential function*, J. Number Theory **6** (1974), 22-31.
- [Ca] L. Carlitz, *The arithmetic of polynomials in Galois field*, Amer. J. Math. **54** (1932), 39-50.
- [C] M. Chardin, *Majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique*, Bull. Soc. Math. France **117** (1989), n° 3, 305-318.
- [Ch] G.V. Chudnovsky, *Contributions to the theory of transcendental numbers*, Math. Surveys and Monographs, A.M.S. **19** (1984), 355-383.
- [De1] L. Denis, *Géométrie diophantienne sur les modules de Drinfeld*, The arithmetic of function fields, Proceedings of the workshop at the Ohio State University, D. Goss, D.R. Hayes, M.I. Rosen eds, Walter de Gruyter, (1992), 285-302.
- [De2] L. Denis, *Hauteur canoniques et modules de Drinfeld*, Math. Ann. **294** (1992), n° 2, 213-223.
- [De3] L. Denis, *Théorème de Baker et modules de Drinfeld*, J. Number Theory **43** (1993), n° 2, 203-215.
- [De4] L. Denis, *Indépendance algébrique et exponentielle de Carlitz*, Acta Arith. **LXIX.1** (1995), 75-89.
- [De5] L. Denis, *Problème de Lehmer en caractéristique finie*, Comp. Math. **98** (1995), n° 2, 167-175.
- [De6] L. Denis, *Lemmes de multiplicités et T-modules*, Michigan Math. Journal **43** (1996), n° 1, 67-79.
- [De7] L. Denis, *Indépendance algébrique en caractéristique 2*, J. Number Theory **66** (1997), n° 1, 183-200.
- [DH] S. David et M. Hindry, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type CM*, J. Reine Angew. Math. **529** (2000), 1-74.
- [D] S. Dion, *Théorème de Brownawell-Waldschmidt en caractéristique finie*, Ann. Fac. Sci. Toulouse Math. **9** (2000), n° 1, 71-90.

- [Do] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arithmetica **34** (1979), n° 4, 391-401.
- [EH] D. Eisenbud et M. Hochster, *A Nullstellensatz with nilpotents and Zariski's main lemma on holomorphic functions*, J. of Algebra **58** (1979), 157-161.
- [Ge1] E.U. Gekeler, *Drinfeld-Moduln und modulare Formen über rationalen Funktionkörpern* Dissertation. Rheinische Friedrich-Wilhelms-Universität, Bonn 1979. Bonner Mathematische Schriften **119**.
- [Ge2] E.U. Gekeler, *Über Drinfeldsche Modulkurven vom Hecke-Typ*, Comp. Math. **57** (1986), n° 2, 219-236.
- [Ge3] E.U. Gekeler, *Drinfeld modular curves*, Lecture Notes in Math. Springer-Verlag (1986).
- [Ge4] E.U. Gekeler, *A product expansion for the discriminant function of Drinfeld modules of rank two*, J. Number Theory **21** (1985), n° 2, 135-140.
- [Ge5] E.U. Gekeler, *On the coefficients on Drinfeld modular forms*, Invent. Math. **93** (1988), n° 3, 667-700.
- [Ge6] E.U. Gekeler, *On the de Rham isomorphism for Drinfeld modules*, J. Reine Angew. Math. **401** (1989), 188-208.
- [Ge7] E.U. Gekeler, *Quasi periodic functions and Drinfeld modular forms*, Comp. Math. **69** (1989), n° 3, 277-293.
- [Ha] D.R. Hayes, *Explicit class field theory for rational function fields*, Trans. Am. Math. Soc. **189** (1974), 77-91.
- [Hi] M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), n° 3, 575-603.
- [Hs] L.C. Hsia, *On the coefficients of modular polynomials for Drinfeld modules*, J. Number Theory **72** (1998), n° 2, 236-256.
- [Hu] J.E. Humphreys, *Linear Algebraic Groups*, Grad. Texts in Math. Springer Verlag, New-York Heideberg Berlin (1975).
- [L1] S. Lang, *Elliptic Functions*, Addison-Wesley **21** (1973).
- [L2] S. Lang, *Introduction to algebraic geometry*, Interscience tracts in pure and applied mathematics **5** (1958).
- [La] M. Laurent, *Minoration de la hauteur de Néron-Tate*, Bertin M.-J. (ed.) Seminar on number theory, Paris 1981-1982 (Prog. in Math. **38**, 137-151) Bosto Basel Stuttgart, Birkhäuser 1983.
- [M] R. Müller, *Algebraische Unabhängigkeit der Werte gewisser Lückenreihen in nicht-archimedisch bewerteten Körpern*, Results Math. **24** (1993), n° 3-4, 288-297.
- [Na] M. Nagata, *Local rings*, Interscience tracts in pure and applied mathematics **13** (1962).
- [N1] Y. Nesterenko, *Modular functions and transcendence problems*, C.R. Acad. Sci. Paris **322** (1996), n° 10, 909-914.
- [N2] Y. Nesterenko, *Modular functions and transcendence questions*, Mat. Sb. **187**, (1996), n° 9, 65-96 (russian); English translation in Sb. Math. **187**, (1996), n° 9, 1319-1348.
- [P1] P. Philippon, *Lemmes de zéros dans les groupes algébriques commutatifs*, Bull. Soc. Math. France **114** (1986), n° 3, 355-383.
- [P2] P. Philippon, *Nouveaux lemmes de zéros dans les groupes algébriques commutatifs*, Rocky Mountain J. Math. **26** (1996), n° 3, 1069-1088.
- [P3] P. Philippon, *Indépendance algébrique et K-fonctions*, J. Reine Angew. Math. **497**, (1998), 1-15.

- [SV] T. Struppeck et J. Vaaler, *Inequalities for heights of algebraic subspaces and the Thue-Siegel principle*, Analytic Number Theory, proceedings of a conference in honor to Paul T. Bateman, Prog. in Math. **85** (1990), 493-528.
- [T1] A. Thiery, *Indépendance algébrique de périodes et quasi-périodes de modules de Drinfeld*, The Arithmetic of Functions Fields, Proceedings, Workshop at Ohio State University (1992), 265-284.
- [T2] A. Thiery, *Théorème de Lindemann-Weierstrass pour les modules de Drinfeld*, Comp. Math. **95** (1995), n° 1, 1-42.
- [Th] J.L. Thunder, *Siegel's lemma for function fields*, Mich. Math. J. **42** (1995), n° 1, 147-162.
- [Tu1] R. Tubbs, *Algebraic groups and small transcendence degree, I*, J. Number Theory **25** (1987), n° 3, 279-307.
- [Tu2] R. Tubbs, *Algebraic groups and small transcendence degree, II*, J. Number Theory **35** (1990), n° 2, 109-127.
- [Wa] M. Waldschmidt, *Solution du huitième problème de Schneider*, J. Number Theory **5** (1973), 191-202.
- [W] A. Weil, *Foundations of algebraic geometry*, Am. Math. Soc. Colloquium Publications Vol. XXIX. (1946).
- [Y1] J. Yu, *Transcendence Theory over function fields*, Duke Math. J. **52** (1985), 517-527.
- [Y2] J. Yu, *Analytic homomorphisms into Drinfeld Modules*, Ann. of Math. **145** (1997), 215-233.
- [ZS] Zariski-Samuel, *Commutative Algebra*, Vol I et II, The University Series in Higher Mathematics.

Résumé. Ce travail consiste en l'examen de quelques problèmes diophantiens en caractéristique non nulle. Plus particulièrement, on s'est attaché à la résolution de problèmes de transcendance, d'indépendance algébrique et intéressé au problème de Lehmer. Le premier résultat obtenu est l'analogue du théorème de Brownawell-Waldschmidt pour les modules de Drinfeld. Il répond en particulier à l'analogue du huitième problème de Schneider. Dans une seconde partie, on s'est intéressé au théorème de Nesterenko. Ici, la caractéristique positive a constitué un obstacle majeur à l'obtention d'un lemme de multiplicité. Néanmoins, la méthode des Stéphanois jointe à l'estimation de hauteurs de nouveaux polynômes modulaires a conduit à un résultat de transcendance de valeurs de fonctions modulaires. Enfin, l'objet de la troisième partie est le problème de Lehmer relatif aux T -modules. Il existe sur ces objets une hauteur canonique dont la construction est similaire à celle de la hauteur de Néron-Tate pour les variétés abéliennes. Pour certains T -modules, on démontre une minoration de la hauteur de points algébriques séparables et non de torsion, semblable à celles obtenues par F. Amoroso, S. David et M. Hindry pour les puissances du groupe multiplicatif et pour les variétés abéliennes.

Diophantine analysis and Drinfeld modules.

Abstract. In this work, we enter upon diophantine problems in positive characteristic. In particular, we are interested in transcendence and algebraic independence questions, and in Lehmer's problem. The first result we obtain is the analogue for Drinfeld modules of the Brownawell-Waldschmidt's theorem. Particularly, this gives a proof of the analogue of the eighth Schneider's problem. In a second part, we are interested in the Nesterenko's theorem. The positive characteristic stands here in the way of getting a zero estimate. Nevertheless, the Stéphanois' method joined to an estimate of the height of new modular polynomials, bring us to a transcendence result for values of modular functions. Finally, the purpose of the third part is Lehmer's problem for T -modules. On these objects we have a height similar to the Néron-Tate height for abelian varieties. For some T -modules, we obtain a lower bound for the height of algebraic, separable and non-torsion points like to those obtained by F. Amoroso, S. David and M. Hindry for powers of the multiplicative group, and for abelian varieties.