

# COMPOSITIO MATHEMATICA

A. THIERY

## **Théorème de Lindemann-Weierstrass pour les modules de Drinfeld**

*Compositio Mathematica*, tome 95, n° 1 (1995), p. 1-42

[http://www.numdam.org/item?id=CM\\_1995\\_\\_95\\_1\\_1\\_0](http://www.numdam.org/item?id=CM_1995__95_1_1_0)

© Foundation Compositio Mathematica, 1995, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

## **Théorème de Lindemann-Weierstrass pour les modules de Drinfeld**

A. THIERY

*Université de Caen Département de Math, Esplanade de la paix, 14032 Caen*

Received 2 February 1993; accepted in final form 7 November 1993

**Abstract.** Let  $\phi$  a  $\mathbb{F}_q[T]$  Drinfeld module, with rank  $d > 0$  and whose coefficients are algebraic over  $\mathbb{F}_q(T)$ . We denote  $\Lambda$  and  $e_\Lambda$  the lattice and the exponential function associated with  $\phi$ ,  $\Omega$  the complex multiplication ring of  $\Lambda$ , and  $d_1 = \text{rank}_{\mathbb{F}_q[T]} \Omega$ . Let  $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{F}_q(T)}$  linearly independent over  $\Omega$ . We denote  $t$  the transcendence degree over  $\mathbb{F}_q(T)$  of the extension generated by  $e_\Lambda(\alpha_1), \dots, e_\Lambda(\alpha_n)$ . Then the following inequality holds

$$td \geq nd_1.$$

This result is an analogous for Drinfeld modules of the Lindemann-Weierstrass theorem.

### **1. Introduction**

On sait depuis les travaux de Jing Yu (voir [Y<sub>2</sub>]), que les fonctions exponentielles attachées aux modules de Drinfeld ont des propriétés de transcendance analogues à celles de la fonction exponentielle classique. Il est donc naturel de se poser la question de l'indépendance algébrique. Pour cela, il faut utiliser des outils puissants tels que le critère d'indépendance algébrique de P. Philippon (voir [P<sub>1</sub>]), ou le lemme de zéros de Jing Yu (voir [Y<sub>1</sub>]), qui est lui-même une version en caractéristique positive d'un lemme de zéros de P. Philippon (voir [P<sub>2</sub>]).

Le but de cet article est donc de donner un équivalent en caractéristique non nulle du célèbre théorème de Lindemann-Weierstrass. Ce théorème dit ceci.

**THEOREME DE LINDEMANN-WEIERSTRASS.** *Soient  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$  algébriques sur  $\mathbb{Q}$  et linéairement indépendants sur  $\mathbb{Q}$ ; alors les nombres  $e^{\alpha_1}, \dots, e^{\alpha_n}$  sont algébriquement indépendants sur  $\mathbb{Q}$ .*

Fixons d'abord quelques notations.

Soient  $p$  un nombre premier,  $q$  une puissance de  $p$ . Le corps fini à  $q$  éléments sera noté  $\mathbb{F}_q$ . On note  $A = \mathbb{F}_q[T]$ ,  $k = \mathbb{F}_q(T)$ . On munit  $k$  de la valuation  $v(x) = \deg_T(x)$ . Soit  $k_\infty = \mathbb{F}_q(\left(\frac{1}{T}\right))$  le complété de  $k$  pour cette valuation, et  $C$  un complété d'une clôture algébrique de  $k_\infty$  sur laquelle on

a prolongé  $v$ . On rappelle que  $C$  est algébriquement clos et on note  $\bar{k}$  la clôture algébrique de  $k$  dans  $C$ . Le Frobénius  $x \rightarrow x^q$  sera noté  $\tau$ .

Soit  $\phi: A \rightarrow \bar{k}\{\tau\}$  un module de Drinfeld de rang  $d > 0$ . On note  $\Lambda$  et  $e_\Lambda$  le réseau et la fonction exponentielle associés à  $\phi$ , et  $\Omega$  l'anneau des multiplications complexes de  $\Lambda$ . On pose  $d_1 = \text{rang}_A \Omega$ .

Le théorème principal est le suivant.

**THEOREME.** *Soient  $\alpha_1, \dots, \alpha_n \in \bar{k}$  linéairement indépendants sur  $\Omega$ . On note  $t$  le degré de transcendance sur  $\mathbb{F}_q(T)$  de l'extension engendrée par  $e_\Lambda(\alpha_1), \dots, e_\Lambda(\alpha_n)$ . On a alors l'inégalité suivante*

$$td \geq nd_1.$$

**REMARQUE.** Le cas  $A = \mathbb{F}_q[T]$  n'est pas restrictif. En effet, un module de Drinfeld pour un anneau  $A$  quelconque peut être considéré comme un module sur un sous-anneau de  $A$  de la forme  $\mathbb{F}_q[T]$ . (La dimension de  $A$  sur  $\mathbb{F}_q[T]$  étant alors nécessairement finie si  $\phi \neq 0$ .)

En prenant le cas particulier où  $\phi$  est le module de Carlitz, c'est-à-dire  $\phi_T = T\tau^0 - \tau$ , on a  $A = \Omega$  et  $d = d_1 = 1$ . On note  $e_C$  l'exponentielle de Carlitz. Le théorème entraîne immédiatement le corollaire suivant, qui est un analogue parfait du théorème de Lindemann-Weierstrass.

**COROLLAIRE.** *Soient  $\alpha_1, \dots, \alpha_n \in \bar{k}$  linéairement indépendants sur  $A$ ; alors les nombres  $e_C(\alpha_1), \dots, e_C(\alpha_n)$  sont algébriquement indépendants sur  $k$ .*

## 2. Semi-résultant

Les semi-résultants ont été introduits par G. V. Chudnovsky. On peut obtenir certaines estimations pour la caractéristique 0 qui utilisent assez fortement le corps des nombres complexes (voir [C]). Pour le cas qui m'intéresse, c'est-à-dire la caractéristique  $p$ , il faut reprendre les théorèmes pour en donner une version ultramétrique, qui est généralement plus simple.

Pour tout  $P \in C[X]$ , on pose

$$v(P) = \max \left\{ v(p_i) \mid P(X) = \sum_{i=1}^n p_i X^i \right\}.$$

On rappelle le résultat bien connu: pour tout  $P, Q \in C[X]$  on a  $v(PQ) = v(P) + v(Q)$ .

DEFINITION-RAPPEL. Soient  $P, Q \in C[X]$ , on pose

$$P(X) = P_0 X^m + \dots + P_m = P_0(X - t_1) \dots (X - t_m).$$

$$Q(X) = Q_0 X^n + \dots + Q_n = Q_0(X - u_1) \dots (X - u_n).$$

On rappelle l'égalité classique:

$$P_0^n Q_0^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (t_i - u_j) = \begin{vmatrix} P_0 & \dots & P_m & & \\ & \ddots & & \ddots & \\ & & P_0 & \dots & P_m \\ Q_0 & \dots & Q_n & & \\ & \ddots & & \ddots & \\ & & Q_0 & \dots & Q_n \end{vmatrix},$$

(voir [L]). Cette valeur commune est appelée résultant de  $P$  et  $Q$ , notée  $\text{Res}(P, Q)$ . Je rappelle également l'inégalité classique suivante.

LEMME 1. Pour tout  $\theta \in C$

$$v(\text{Res}(P, Q)) \leq (n-1)v(P) + (m-1)v(Q) + \max\{v(Q(\theta)) + v(P), v(P(\theta)) + v(Q)\}.$$

(voir [L]).

Nous allons passer maintenant à la partie principale de ce paragraphe.

DEFINITION. Soient  $P, Q \in C[X] - \{0\}$ ; on pose

$$P(X) = P_0(X - t_1) \dots (X - t_m)$$

$$Q(X) = Q_0(X - u_1) \dots (X - u_n).$$

On appelle semi-résultant de  $P$  et  $Q$ , noté  $r(P, Q)$ ,

$$r(P, Q) = P_0^n Q_0^m \prod_{\{(i,j) | t_i \neq u_j\}} (t_i - u_j).$$

Le semi-résultant n'est donc jamais nul.

Les lemmes suivants montrent que le semi-résultant a des propriétés analogues au résultant.

LEMME 2. Soient  $P, Q \in C[X] - \{0\}$ , on note

$$P(X) = P_0 X^m + \dots + P_m$$

$$Q(X) = Q_0 X^n + \dots + Q_n.$$

Alors

$$r(P, Q) \in \mathbb{F}_p[P_0, \dots, P_m, Q_0, \dots, Q_n],$$

avec

$$\deg_{P_0, \dots, P_m} r(P, Q) \leq n$$

$$\deg_{Q_0, \dots, Q_n} r(P, Q) \leq m.$$

DEMONSTRATION. Soit  $l$  le cardinal de l'ensemble

$$\{(i, j) \in [1, m] \times [1, n] \mid t_i \neq u_j\}$$

avec  $t_i, u_j$  les racines de  $P, Q$  comme précédemment. On a alors

$$r(P, Q) = P_0^n Q_0^m \sum_{\substack{J \subset [1, m] \times [1, n] \\ \text{Card } J = l}} \prod_{(i, j) \in J} (t_i - u_j).$$

Posons  $R(\lambda) = P_0^n Q_0^m \prod_{i=1}^m \prod_{j=1}^n (\lambda - (t_i - u_j))$ , alors  $r(P, Q) = (-1)^l \times$  coefficient d'ordre  $mn - l$  de  $R(\lambda)$ .

De plus  $R(\lambda) = \text{Res}(P(X + \lambda), Q(X))$ . Or

$$\begin{aligned} P(X + \lambda) &= \sum_{i=0}^m P_{m-i}(X + \lambda)^i \\ &= \sum_{i=0}^m \left( P_{m-i} \sum_{k=0}^i \binom{i}{k} X^k \lambda^{i-k} \right) \\ &= \sum_{k=0}^m \left( \sum_{i=k}^m \binom{i}{k} P_{m-i} \lambda^{i-k} \right) X^k. \end{aligned}$$

D'où

$$R(\lambda) = \begin{vmatrix} P_0 & \cdots & \sum_{i=k}^m \binom{i}{k} P_{m-i} \lambda^{i-k} & \cdots & \sum_{i=0}^m \lambda^i P_{m-i} & \cdots \\ \cdots & & & & & \cdots \\ & & P_0 & \cdots & \cdots & \cdots \sum_{i=0}^m \lambda^i P_{m-i} \\ Q_0 & \cdots & \cdots & \cdots & Q_n & \cdots \\ \cdots & & & & & \cdots \\ & & Q_0 & \cdots & \cdots & \cdots Q_n \end{vmatrix}$$

Le résultat annoncé en découle immédiatement. □

LEMME 3. Soient  $P, Q \in C[X] - \{0\}$ . Posons  $P = P_1 P_2$  et  $Q = Q_1 Q_2$  avec  $P_2, Q_2$  unitaires et  $P_1, Q_1$  premiers entre eux. On note  $m = \deg_X P, n = \deg_X Q$ , alors pour tout  $\theta \in C$

$$v(r(P, Q)) \leq (n - 1)v(P) + (m - 1)v(Q) + \max\{v(P_1(\theta)) + v(Q) + v(P_2), v(Q_1(\theta)) + v(P) + v(Q_2)\}.$$

DEMONSTRATION. Quitte à renuméroter les racines de  $P$  et  $Q$ , on a

$$P_1 = P_0(X - t_1) \cdots (X - t_\mu) \quad P_2 = (X - t_{\mu+1}) \cdots (X - t_m)$$

$$Q_1 = Q_0(X - u_1) \cdots (X - u_\nu) \quad Q_2 = (X - u_{\nu+1}) \cdots (X - u_n).$$

Par définition le semi-résultant vaut

$$r(P, Q) = P_0^n Q_0^m \prod_{\{(i,j) | t_i \neq u_j\}} (t_i - u_j).$$

Les polynômes  $P_1$  et  $Q_1$  étant premiers entre eux, pour tout  $i \leq \mu, j \leq \nu$  on a  $t_i \neq u_j$ . En définissant  $E = \{(i, j) | (i > \mu \text{ ou } j > \nu) \text{ et } t_i \neq u_j\}$ ,

$$r(P, Q) = P_0^{n-\nu} Q_0^{m-\mu} P_0^\nu Q_0^\mu \prod_{\substack{i \leq \mu \\ j \leq \nu}} (t_i - u_j) \prod_{(i,j) \in E} (t_i - u_j)$$

$$= P_0^{n-\nu} Q_0^{m-\mu} \text{Res}(P_1, Q_1) \prod_{(i,j) \in E} (t_i - u_j).$$

D'après le lemme 1,

$$v(\text{Res}(P_1, Q_1)) \leq (\nu - 1)v(P_1) + (\mu - 1)v(Q_1)$$

$$+ \max\{v(P_1(\theta)) + v(Q_1), v(Q_1(\theta)) + v(P_1)\}.$$

Séparons  $E$  en trois parties disjointes.

$$E_1 = \{(i, j) | t_i \neq u_j, i \leq \mu \text{ et } j > \nu\}$$

$$E_2 = \{(i, j) | t_i \neq u_j, i > \mu \text{ et } j \leq \nu\}$$

$$E_3 = \{(i, j) | t_i \neq u_j, i > \mu \text{ et } j > \nu\}.$$

En développant, on trouve que  $\prod_{(i,j) \in E_1} (t_i - u_j)$  est une somme de monômes de degré inférieur à  $n - \nu$  en  $t_i, i \leq \mu$  et de degré inférieur à  $\mu$  en  $u_j, j > \nu$ . Or, en

utilisant la formule,  $v(AB) = v(A) + v(B)$  pour tout  $A, B \in C[X]$ , on obtient facilement

$$v\left(\frac{P_1}{P_0}\right) = \sum_{i=1}^{\mu} \max\{0, v(t_i)\}$$

$$v(Q_2) = \sum_{j=\nu+1}^n \max\{0, v(u_j)\}.$$

D'où

$$v\left(\prod_{(i,j) \in E_1} (t_i - u_j)\right) \leq (n - \nu)v\left(\frac{P_1}{P_0}\right) + \mu v(Q_2).$$

De même,

$$v\left(\prod_{(i,j) \in E_2} (t_i - u_j)\right) \leq (m - \mu)v\left(\frac{Q_1}{Q_0}\right) + \nu v(P_2)$$

$$v\left(\prod_{(i,j) \in E_3} (t_i - u_j)\right) \leq (n - \nu)v(P_2) + (m - \mu)v(Q_2).$$

En additionnant toutes ces inégalités et en utilisant  $v(P) = v(P_1) + v(P_2)$ , on obtient le résultat annoncé.  $\square$

### 3. Critère d'indépendance algébrique

Dans cette section on énonce un critère d'indépendance algébrique dû à P. Philippon (voir [P<sub>1</sub>]), qui ne concerne que les extensions transcendentes pures, et on l'étend grâce au semi-résultant.

Dans cette partie le degré d'un polynôme par rapport à plusieurs variables est défini comme le degré total du polynôme par rapport à ces variables.

**THEOREME 1.** *Soient  $n$  un entier strictement positif et  $c(n) \geq 1$ ; on se donne quatre fonctions  $d, t, s$  et  $r$  croissantes de  $\mathbb{N}$  à valeurs dans les réels  $\geq 1$  telles que*

$$(i) \text{ pour tout } k \in \mathbb{N}, d(k) \leq t(k) \text{ et } \lim_{k \rightarrow \infty} t(k) = \lim_{k \rightarrow \infty} \frac{s(k)}{t(k)d(k)^n} = +\infty,$$

$$(ii) \text{ pour tout } k \in \mathbb{N}, s(k)^{n+2} \geq c(n)t(k+1)d(k+1)^n(s(k)^{n+1} + r(k+1)^{n+1}).$$

*Alors, si  $c(n)$  est assez grand, pour toutes fonctions  $d, t, s, r$  comme ci-dessus*

et tout  $(\theta_1, \dots, \theta_n) \in C^n$  on a la propriété suivante: il n'existe pas de suite  $(I_k = (P_{1,k}, \dots, P_{m(k),k}))_{k \geq k_0}$  d'idéaux de  $A[X_1, \dots, X_n]$  dont l'ensemble des zéros dans  $\{z \in C^n \mid \max v(z_i - \theta_i) \leq -r(k)\}$  soit de cardinal fini et tel que pour tout  $k \geq k_0$  on ait

- (i)  $\max_{1 \leq i \leq m(k)} \{\deg_{X_1, \dots, X_n}(P_{i,k})\} \leq d(k)$
- (ii)  $\max_{1 \leq i \leq m(k)} \{\deg_T(P_{i,k})\} \leq t(k)$
- (iii)  $-\infty < \max_{1 \leq i \leq m(k)} \{v(P_{i,k}(\theta_1, \dots, \theta_n))\} \leq -s(k)$ .

Le critère ci-dessus ne convient que pour les extensions transcendentes pures. Il faut donc le généraliser. Pour cela, j'utilise le semi-résultant.

Soit  $n$  un entier strictement positif, on se donne quatre fonctions  $D, T, S$  et  $R$  croissantes de  $\mathbb{N}$  à valeurs dans les réels  $> 0$  telles que

- (i)  $D \ll T \ll R$  et  $\lim_{k \rightarrow \infty} T(k) = \lim_{k \rightarrow \infty} \frac{S(k)}{T(k)D(k)^n} = +\infty$
- (ii)  $S(k)^{n+2} \gg T(k+1)D(k+1)^n(S(k)^{n+1} + R(k+1)^{n+1})$
- (iii) il existe  $c_0 > 0$  tel que pour tout  $k, R(k) \geq c_0 S(k)$ .

Soient  $\alpha \in C$  entier sur  $\mathbb{F}_q[T]$ ,  $\theta_1, \dots, \theta_n \in C$  fixés et

$$M(T, T_1, X_1, \dots, X_{n+1})$$

un polynôme à coefficients dans  $\mathbb{F}_q$ , unitaire en  $X_{n+1}$ . Pour tout  $\theta'_1, \dots, \theta'_n \in C$  on choisit  $\theta'_{n+1} \in C$  vérifiant

$$M[T, \alpha, \theta'_1, \dots, \theta'_n, \theta'_{n+1}] = 0.$$

**THEOREME 2.** Avec les notations précédentes, il n'existe pas de suite de famille de polynômes,  $F_k$ , définie pour  $k \geq k_0$

$$F_k = \{P_{k,\theta'_1, \dots, \theta'_n} \in \mathbb{F}_q[T, T_1, X_1, \dots, X_{n+1}] \mid 1 \leq i \leq n, v(\theta_i - \theta'_i) \leq -R(k)\},$$

tel que pour tout  $(\theta'_1, \dots, \theta'_n)$  vérifiant  $v(\theta_i - \theta'_i) \leq -R(k)$  on ait

$$-\infty < v(P_{k,\theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n, \theta'_{n+1})) \leq -S(k)$$

$$\deg_{T, T_1} P_{k,\theta'_1, \dots, \theta'_n} \leq T(k)$$

$$\deg_{X_1, \dots, X_{n+1}} P_{k,\theta'_1, \dots, \theta'_n} \leq D(k).$$

**DEMONSTRATION.** Supposons qu'une telle suite existe. On va se ramener à une extension transcendante pure. Commençons par éliminer  $\theta'_{n+1}$ . Le



polynôme  $M(T, \alpha, \theta'_1, \dots, \theta'_n, X) \in C[X]$  est unitaire en  $X$  donc non nul. De même le polynôme  $P_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n, X) \in C[X]$  prend une valeur non nulle en  $\theta'_{n+1}$ , donc il n'est pas nul. D'après le lemme 2, il existe un polynôme  $Q_{k, \theta'_1, \dots, \theta'_n} \in \mathbb{F}_q[T, T_1, X_1, \dots, X_n]$  tel que

$$\begin{aligned} & Q_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n) \\ &= r(M(T, \alpha, \theta'_1, \dots, \theta'_n, X), P_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n, X)), \end{aligned}$$

et

$$\begin{aligned} \deg_{T, T_1} Q_{k, \theta'_1, \dots, \theta'_n} &\leq \deg_{X_{n+1}}(M)T(k) + D(k) \deg_{T, \alpha}(M) \\ \deg_{X_1, \dots, X_n} Q_{k, \theta'_1, \dots, \theta'_n} &\leq \deg_{\theta_{n+1}}(M)D(k) + D(k) \deg_{\theta'_1, \dots, \theta'_n}(M). \end{aligned}$$

Comme  $T \gg D$ , il existe  $c_1$  tel que

$$\begin{aligned} \deg_{T, T_1} Q_{k, \theta'_1, \dots, \theta'_n} &\leq c_1 T(k) \\ \deg_{X_1, \dots, X_n} Q_{k, \theta'_1, \dots, \theta'_n} &\leq c_1 D(k). \end{aligned}$$

On note

$$P_1 = X - \theta'_{n+1}, P_2 = \frac{M(T, \alpha, \theta'_1, \dots, \theta'_n, X)}{X - \theta'_{n+1}}$$

qui est un polynôme unitaire et

$$Q_1 = P_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n, X), Q_2 = 1.$$

Ainsi les polynômes  $P_1$  et  $Q_1$  sont premiers entre eux. Le lemme 3 nous donne

$$\begin{aligned} & v(Q_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n)) \\ &\leq (\deg_X(M(T, \alpha, \theta'_1, \dots, \theta'_n, X)) - 1)v(P_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n, X)) \\ &\quad + (\deg_X(P_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n, X)) - 1)v(M(T, \alpha, \theta'_1, \dots, \theta'_n, X)) \\ &\quad + v(P_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n, \theta'_{n+1})) + v(M(T, \alpha, \theta'_1, \dots, \theta'_n, X)). \end{aligned}$$

Donc il existe  $c_2 > 0$  tel que

$$v(Q_{k, \theta'_1, \dots, \theta'_n}(T, \alpha, \theta'_1, \dots, \theta'_n)) \leq c_2(T(k) + D(k)) - S(k).$$

Or

$$\lim_{k \rightarrow \infty} \frac{S(k)}{T(k)D(k)^n} = +\infty,$$

d'où  $S \gg T$ , et comme  $T \gg D$ , il existe  $c_3 > 0$  tel que

$$v(Q_{k,\theta_1,\dots,\theta_n}(T, \alpha, \theta'_1, \dots, \theta'_n)) \leq -c_3 S(k).$$

Maintenant que nous avons éliminé  $\theta'_{n+1}$ , il ne reste plus qu'à éliminer  $\alpha$ . On procède d'une façon analogue. Soit  $R \in A[X]$  un polynôme unitaire tel que

$$R(\alpha) = 0.$$

Comme précédemment il existe  $R_{k,\theta_1,\dots,\theta_n} \in \mathbb{F}_q[T, X_1, \dots, X_n]$  tel que

$$R_{k,\theta_1,\dots,\theta_n}(T, \theta'_1, \dots, \theta'_n) = r(Q_{k,\theta_1,\dots,\theta_n}(T, X, \theta'_1, \dots, \theta'_n), R(T, X))$$

et

$$\deg_T(R_{k,\theta_1,\dots,\theta_n}) \leq \deg_X(R) c_1 T(k) + c_1 T(k) \deg_T(R)$$

$$\deg_{X_1,\dots,X_n}(R_{k,\theta_1,\dots,\theta_n}) \leq \deg_X(R) c_1 D(k) + c_1 T(k) \deg_{X_1,\dots,X_n}(R).$$

Or  $\deg_{X_1,\dots,X_n}(R) = 0$ , donc il existe  $c_4 > 0$  tel que

$$\deg_T(R_{k,\theta_1,\dots,\theta_n}) \leq c_4 T(k)$$

$$\deg_{X_1,\dots,X_n}(R_{k,\theta_1,\dots,\theta_n}) \leq c_4 D(k).$$

En posant

$$P_1 = X - \alpha, Q_2 = \frac{R}{X - \alpha} \quad \text{et} \quad Q_1 = Q_{k,\theta_1,\dots,\theta_n}(T, X, \theta'_1, \dots, \theta'_n), Q_2 = 1,$$

on peut appliquer le lemme 3; il existe donc une constante  $c_5 > 0$  tel que

$$v(R_{k,\theta_1,\dots,\theta_n}(T, \theta'_1, \dots, \theta'_n)) \leq -c_5 S(k).$$

Soit  $I_k$  l'idéal de  $\mathbb{F}_q[T, X_1, \dots, X_n]$  engendré par les  $R_{k,\theta_1,\dots,\theta_n}(T, X_1, \dots, X_n)$ ,  $v(\theta'_i - \theta_i) \leq -R(k)$ . Comme  $R_{k,\theta_1,\dots,\theta_n}(T, \theta'_1, \dots, \theta'_n)$  est égal à un semi-résultant, il est non nul. L'idéal  $I_k$  n'a donc pas de zéros dans la boule de centre  $(\theta_1, \dots, \theta_n)$  et de rayon  $-R(k)$ .

Soit  $c_6 > 0$  tel que  $c_6 \geq \max\{v(\theta_i) \mid 1 \leq i \leq n\}$ . Comme  $R(k) \geq 0$ , pour tout  $(\theta'_1, \dots, \theta'_n)$  tel que  $v(\theta_i - \theta'_i) \leq -R(k)$  alors  $v(\theta'_i) \leq \max\{v(\theta_i), v(\theta_i - \theta'_i)\} \leq c_6$ .  
Donc

$$\begin{aligned} & v(R_{k,\theta_1,\dots,\theta_n}(T, \theta_1, \dots, \theta_n)) \\ &= v(R_{k,\theta_1,\dots,\theta_n}((T, \theta'_1, \dots, \theta'_n) + (0, \theta_1 - \theta'_1, \dots, \theta_n - \theta'_n))) \\ &\leq \max\{-c_5 S(k), -R(k) + T(k) + c_6(D(k) - 1)\}. \end{aligned}$$

Or  $R(k) \geq c_0 S(k)$ , donc il existe  $c_7 > 0$  tel que

$$v(R_{k,\theta_1,\dots,\theta_n}(T, \theta_1, \dots, \theta_n)) \leq -c_7 S(k).$$

On pose alors  $d(k) = c_8 D(k)$  avec  $c_8 \geq c_4$  et de telle sorte que  $d(k) \geq d(k_0) \geq 1$ ,  $t(k) = c_4 T(k)$ ,  $r(k) = R(k)$  et  $s(k) = c_7 S(k)$ . Donc il existe  $k_1$  tel que les fonctions  $d(k)$ ,  $t(k)$ ,  $r(k)$ ,  $s(k)$ ,  $k \geq k_1$  vérifient les conditions du critère de Philippon.

Pour tout  $k \geq k_1$ , j'extraie de la famille

$$\{R_{k,\theta_1,\dots,\theta_n}(T, X_1, \dots, X_n) \mid v(\theta'_i - \theta_i) \leq -R(k)\}$$

une famille génératrice finie de l'idéal  $I_k$ , on obtient alors une contradiction avec le critère de Philippon.  $\square$

#### 4. Lemme de Siegel

Soit  $\alpha$  entier sur  $A = F_q[T]$  de degré  $\delta$ . L'anneau  $B = A[\alpha]$  est donc un  $A$  module libre de rang  $\delta$  admettant pour base  $1, \alpha, \dots, \alpha^{\delta-1}$ .

DEFINITION. Pour tout  $x \in B$ , il existe un unique  $(a_0, \dots, a_{\delta-1}) \in A^\delta$  tel que

$$x = \sum_{i=0}^{\delta-1} a_i \alpha^i.$$

On appelle taille de  $x$ , notée  $t(x)$ , le nombre

$$t(x) = \max\{\deg_T(a_i) \mid 0 \leq i \leq \delta - 1\}.$$

Cette taille dépend du choix de  $\alpha$  tel que  $B = A[\alpha]$ .

On a alors les propriétés suivantes.

PROPRIETES. (1) Pour tout  $x, y \in B$ ,  $t(x + y) \leq \max\{t(x), t(y)\}$ .

(2) Pour tout  $a, x \in A \times B$ ,  $t(ax) = t(a) + t(x)$ .

Il existe  $c_9 \geq 0$  tel que pour tout  $n \in \mathbb{N}$  et tout  $(x_1, \dots, x_n) \in B^n$  on ait

(3)  $t(x_1 \cdots x_n) \leq t(x_1) + \dots + t(x_n) + c_9(n - 1)$ .

DEMONSTRATION. Seule la dernière propriété est non triviale. Par récurrence, il suffit de la montrer au rang 2.

Soient  $x, y \in B$

$$x = \sum_{i=0}^{\delta-1} a_i \alpha^i, \quad y = \sum_{i=0}^{\delta-1} b_i \alpha^i.$$

Donc

$$xy = \sum_{\substack{0 \leq i \leq \delta-1 \\ 0 \leq j \leq \delta-1}} a_i b_j \alpha^{i+j}.$$

La première propriété nous donne:

$$t(xy) \leq \max\{t(a_i b_j \alpha^{i+j}) \mid 0 \leq i \leq \delta - 1, 0 \leq j \leq \delta - 1\}.$$

De la deuxième propriété on déduit  $t(a_i b_j \alpha^{i+j}) = t(a_i) + t(b_j) + t(\alpha^{i+j})$ .  
D'où

$$t(xy) \leq t(x) + t(y) + \max\{t(\alpha^i) \mid 0 \leq i \leq 2(\delta - 1)\}. \quad \square$$

Maintenant que nous avons défini une taille sur l'anneau  $B$ , il est possible de donner une estimation des solutions de systèmes linéaires homogènes à coefficients dans  $B$ .

THEOREME 3 ("lemme de Siegel"). Soient  $a_{i,j} \in B$ ,  $1 \leq i \leq n$ ,  $1 \leq j \leq m$  et  $t \in \mathbb{N}$  tels que pour tout  $i, j$  on ait  $t(a_{i,j}) \leq t$ . On suppose  $n > \delta m$ . Il existe alors  $x_1, \dots, x_n \in A$  non tous nuls tels que

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

$$t(x_i) = \deg_T(x_i) \leq \frac{m\delta}{n - m\delta} t.$$

DEMONSTRATION. Soit  $t_1 \in \mathbb{N}$ . Notons  $E$  l'ensemble défini par

$$E = \{(x_1, \dots, x_n) \in A^n \mid t(x_i) \leq t_1\}.$$

Le cardinal de  $E$  vaut donc  $q^{n(t_1 + 1)}$ .

Soit  $L$  l'application linéaire définie de  $A^n$  dans  $B^m$  par

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

Donc  $L(E) \subset F = \{(y_1, \dots, y_m) \in B^m \mid t(y_j) \leq t + t_1\}$ . Le cardinal de  $F$  vaut donc  $q^{m\delta(t+t_1+1)}$ .

Si  $n(t_1 + 1) > m\delta(t + t_1 + 1)$  alors il existe deux éléments distincts de  $E$  qui ont même image par  $L$ . Donc leur différence, qui appartient aussi à  $E$  car  $E$  est un groupe, s'envoie sur 0 par  $L$ . Pour avoir une solution non triviale au système linéaire, il suffit donc que l'on ait  $n(t_1 + 1) > m\delta(t + t_1 + 1)$ , ce qui équivaut à

$$t_1 + 1 > \frac{m\delta}{n - m\delta} t.$$

Donc  $t_1 = \left\lceil \frac{m\delta}{n - m\delta} t \right\rceil$  convient. □

## 5. Préliminaires arithmétiques

Dans cette partie, je montre que certaines hypothèses techniques sont non restrictives et je calcule des suites de dénominateurs pour certaines fonctions. Il s'agit là essentiellement d'un léger raffinement de la notion de  $E_q$  fonctions de Jing Yu (voir [Y<sub>2</sub>]).

Soit  $\phi : A \rightarrow \bar{k}\{\tau\}$  un module de Drinfeld de rang  $d > 0$ . On note  $\Lambda$  et  $e_\Lambda$  le réseau et la fonction exponentielle associés à  $\phi$ , et  $\Omega$  l'anneau des multiplications complexes de  $\Lambda$ . On pose  $d_1 = \text{rang}_A \Omega$ .

Soient  $\alpha_1, \dots, \alpha_n \in \bar{k}$  linéairement indépendants sur  $\Omega$ . Nous sommes intéressés par le degré de transcendance sur  $k$  de l'extension engendrée par  $e_\Lambda(\alpha_1), \dots, e_\Lambda(\alpha_n)$ .

Soit  $k_1$  une extension finie de  $k$  contenant  $\alpha_1, \dots, \alpha_n$  ainsi que les coefficients de  $\phi_\gamma$  pour tout  $\gamma \in \Omega$ . On note  $p^{i_s}$  le degré d'inséparabilité de  $k_1$  sur  $k$  et  $k_s$  la sous-extension séparable maximale. Par le théorème de l'élément primitif, il existe  $\alpha \in k_s$ , que l'on peut prendre entier sur  $A$ , tel que

$$k_s = k[\alpha].$$

On note  $B = A[\alpha]$ . Ce n'est, en général, pas la clôture intégrale de  $A$  dans  $k_s$  mais pour tout  $x \in k_s$  il existe  $a \in A - \{0\}$  tel que

$$ax \in B.$$

Pour tout  $1 \leq i \leq n$ ,  $\alpha_i^{p^i} \in k_s$ . Il existe donc  $a_i \in A - \{0\}$  tel que  $a_i \alpha_i^{p^i} \in B$ . Or il existe un multiple non nul de  $a_i$  qui soit une puissance  $p^i$ -ième dans  $A$ . Notons le  $b_i^{p^i}$ . On a alors

$$(b_i \alpha_i)^{p^i} \in B.$$

De plus  $e_\Lambda(b_i \alpha_i) = \phi_{b_i}(e_\Lambda(\alpha_i))$ . On ne change donc pas le degré de transcendance en remplaçant  $\alpha_i$  par  $b_i \alpha_i$ . Par ailleurs, il est trivial que les  $b_i \alpha_i$  sont linéairement indépendants sur  $\Omega$ . Pour la démonstration du théorème, il n'y a donc pas de restriction à supposer

$$\alpha_i^{p^i} \in B.$$

Soient  $\gamma_1, \dots, \gamma_{d_1} \in \Omega$  linéairement indépendants sur  $A$ . Comme précédemment, en remplaçant  $\gamma_i$  par  $a_i \gamma_i$  avec  $a_i \in A - \{0\}$ , on peut supposer

$$\gamma_i^{p^i} \in B.$$

Soit  $a \in A - \{0\}$  et  $\psi$  le module de Drinfeld homomorphe à  $\phi$  défini par

$$\text{pour tout } b \in A, \quad \psi_b(z) = \frac{1}{a} \phi_b(az).$$

Notons  $\Lambda'$  et  $e_{\Lambda'}$  le réseau et la fonction exponentielle associés à  $\psi$ . On a alors

$$e_{\Lambda'}(z) = \frac{1}{a} e_\Lambda(az) = \frac{1}{a} \phi_a(e_\Lambda(z))$$

$$\Lambda' = \frac{\Lambda}{a}.$$

Donc l'anneau des endomorphismes de  $\Lambda'$  est égal à  $\Omega$ , et le degré de transcendance sur  $k$  du corps  $k(e_{\Lambda'}(\alpha_1), \dots, e_{\Lambda'}(\alpha_n))$  est aussi égal à  $t$ . On ne modifie donc pas le problème en changeant  $\phi$  en  $\psi$ .

De plus, pour tout  $\gamma \in \Omega$ , le morphisme de module de Drinfeld  $\psi_\gamma$  associé à l'endomorphisme de réseau  $\gamma$  vaut

$$\psi_\gamma(z) = \frac{1}{a} \phi_\gamma(az).$$

Donc, en prenant  $a \in A - \{0\}$  tel que pour tout  $c$ , coefficient de  $\phi_T$ ,

$\phi_{\gamma_1}, \dots, \phi_{\gamma_d}$ , on ait  $ac^{p^{i_1}} \in B$ , on peut supposer que les coefficients de  $\psi_T^{p^{i_1}}, \psi_{\gamma_1}^{p^{i_1}}, \dots, \psi_{\gamma_d}^{p^{i_1}}$  appartiennent à  $B$ .

Il n'y a donc pas de restrictions à supposer qu'il existe  $\gamma_1, \dots, \gamma_d \in \Omega$  linéairement indépendants sur  $A$  tel que les coefficients de  $\phi_T^{p^{i_1}}, \phi_{\gamma_1}^{p^{i_1}}, \dots, \phi_{\gamma_d}^{p^{i_1}}$  appartiennent à  $B$ .

On munit  $B$  de la taile  $t$  définie au paragraphe 4.

LEMME 4. On note  $e_\Lambda = \sum_{i \in \mathbb{N}} e_i \tau^i$ . Pour tout  $m > 0$ , on définit

$$D_m = (T^{q^m} - T)(T^{q^{m-1}} - T)^q \dots (T^q - T)^{q^{m-1}},$$

et  $D_0 = 1$ , alors pour tout  $m \in \mathbb{N}$

$$(D_m e_m)^{p^{i_1}} \in B,$$

et il existe  $c_{10}$  tel que pour tout  $m \in \mathbb{N}$  on ait

$$t((D_m e_m)^{p^{i_1}}) \leq c_{10} m q^m.$$

DEMONSTRATION. L'équation fonctionnelle  $e_\Lambda(Tz) = \phi_T(e_\Lambda(z))$  nous donne la relation de récurrence

$$e_m(T^{q^m} - T) = \sum_{j=1}^d b_j e_{m-j}^{q^j},$$

où  $\phi_T = \sum_{j=1}^d b_j \tau^j$ . On a donc

$$e_m D_m = \sum_{j=1}^d b_j (D_{m-j} e_{m-j})^{q^j} (T^{q^{m-1}} - T)^q \dots (T^{q^{m-j+1}} - T)^{q^{j-1}}.$$

On en déduit par une récurrence immédiate que  $(D_m e_m)^{p^{i_1}} \in B$  et aussi

$$t((e_m D_m)^{p^{i_1}}) \leq \max_{1 \leq j \leq d} \{t(b_j^{p^{i_1}} ((D_{m-j} e_{m-j})^{p^{i_1}})^{q^j}) + (j-1)q^m p^{i_1}\}.$$

Soit  $c_{11} \geq \max_{1 \leq j \leq d} \{t(b_j^{p^{i_1}}) + c_9 q^j\}$ . On fait l'hypothèse de récurrence suivante

$$t((D_m e_m)^{p^{i_1}}) \leq c_{11} \sum_{i=0}^m q^i + p^{i_1} m q^m.$$

On choisit  $c_{11}$  assez grand pour qu'elle soit vérifiée pour  $m \leq d$ . On suppose

la relation vraie au rang  $m$ . En utilisant les propriétés multiplicatives de la taille, on a

$$t((D_{m+1}e_{m+1})^{p^{i_1}}) \leq \max_{1 \leq j \leq d} \{c_{11} + q^j t((D_{m+1-j}e_{m+1-j})^{p^{i_1}}) + (j-1)q^{m+1}p^{i_1}\}.$$

Or pour tout  $1 \leq j \leq d$

$$\begin{aligned} & c_{11} + q^j t((D_{m-j}e_{m-j})^{p^{i_1}}) + (j-1)q^{m+1}p^{i_1} \\ & \leq c_{11} + q^j \left( c_{11} \sum_{i=0}^{m+1-j} q^i + p^{i_1}(m+1-j)q^{m+1-j} \right) + (j-1)q^{m+1}p^{i_1} \\ & \leq c_{11} + c_{11} \sum_{i=j}^{m+1} q^i + p^{i_1}mq^{m+1} \\ & \leq c_{11} \sum_{i=0}^{m+1} q^i + p^{i_1}(m+1)q^{m+1}. \end{aligned}$$

L'hypothèse de récurrence est donc vraie au rang  $m+1$ . En remarquant que

$$\sum_{i=0}^{m+1} q^i = \frac{q^{m+2} - 1}{q - 1},$$

on a le résultat annoncé. □

On note  $\Omega_1$  le sous  $A$  module de  $\Omega$  qui a pour base  $(\gamma_1, \dots, \gamma_{d_1})$ . Pour tout  $\gamma \in \Omega_1$ , les coefficients de  $\phi_\gamma^{p^{i_1}}$ , considéré comme polynôme, appartient à  $B$ . On peut donc définir la taille de  $\phi_\gamma^{p^{i_1}}$  comme étant le maximum de la taille de ses coefficients. Dans la suite nous aurons besoin de l'estimation suivante.

LEMME 5. *Il existe  $c_{12}$  tel que pour tout  $\gamma = \sum_{i=1}^{d_1} a_i \gamma_i \in \Omega_1$ ,  $a_i \in A$  on ait*

$$t(\phi_\gamma^{p^{i_1}}) \leq c_{12} q^{d \max\{\deg_T(a_i)\}}.$$

DEMONSTRATION. Soit  $c_{13} \geq 0$  tel que

$$t(\phi_T^{p^{i_1}}) \leq c_{13}.$$

Comme  $\phi_{T^n} = \phi_T \circ \phi_{T^{n-1}}$ , on a

$$t(\phi_{T^n}^{p^{i_1}}) \leq c_{13} + q^d t(\phi_{T^{n-1}}^{p^{i_1}}) + c_9 q^d.$$



Posons  $c_{14} = c_{13} + c_9 q^d$ ; par une récurrence immédiate on a

$$t(\phi_{T^n}^{p^{i_1}}) \leq c_{14} \sum_{i=0}^{n-1} q^{id}.$$

Or

$$c_{14} \sum_{i=0}^{n-1} q^{id} = c_{14} \frac{q^{nd} - 1}{q^d - 1} \leq c_{15} q^{nd}.$$

Soit  $a \in A$ , écrivons

$$a = \sum_{i=0}^n a_i T^i \quad \text{avec } a_i \in \mathbb{F}_q.$$

Alors

$$\begin{aligned} t(\phi_a^{p^{i_1}}) &= t\left(\sum_{i=0}^n a_i^{p^{i_1}} \phi_{T^i}^{p^{i_1}}\right) \\ &\leq \max_{0 \leq i \leq n} \{t(a_i^{p^{i_1}} \phi_{T^i}^{p^{i_1}})\} \\ &\leq \max \{t(\phi_{T^i}^{p^{i_1}}) \mid 0 \leq i \leq n \text{ et } a_i \neq 0\} \\ &\leq c_{15} q^{d \deg_T(a)}. \end{aligned}$$

Soit  $\gamma = \sum_{i=1}^{d_1} a_i \gamma_i \in \Omega_1$ , avec  $a_i \in A$ . On a alors

$$t(\phi_\gamma^{p^{i_1}}) \leq \max_{1 \leq i \leq d_1} \{t(\phi_{a_i \gamma_i}^{p^{i_1}})\}.$$

Or  $\phi_{a_i \gamma_i} = \phi_{a_i} \circ \phi_{\gamma_i}$  et  $\deg_r \phi_{a_i} = d \deg_T(a_i)$ . En prenant  $c_{16} \geq \max_{1 \leq i \leq d_1} \{t(\phi_{\gamma_i}^{p^{i_1}})\}$ , on a

$$\begin{aligned} t(\phi_{a_i \gamma_i}^{p^{i_1}}) &\leq t(\phi_{a_i}^{p^{i_1}}) + q^{d \deg_T(a_i)} t(\phi_{\gamma_i}^{p^{i_1}}) + c_9 q^{d \deg_T(a_i)} \\ &\leq (c_{15} + c_{16} + c_9) q^{d \deg_T(a_i)}. \end{aligned}$$

D'où  $t(\phi_\gamma^{p^{i_1}}) \leq (c_{15} + c_{16} + c_9) q^{d \max\{\deg_T(a_i)\}}$ . □

Nous aurons également besoin des deux lemmes suivants.

**LEMME 6.** Soit  $m_1, \dots, m_n, m \in \mathbb{N}$  tel que  $q^{m_1} + \dots + q^{m_n} \leq q^m$  alors

$$D_{m_1} \cdots D_{m_n} \text{ divise } D_m.$$

Il existe une constante  $c_{17}$  tel que pour tout  $m_1, \dots, m_n, m \in \mathbb{N}$  comme précédemment on ait

$$t((D_m e_{m_1} \cdots e_{m_n})^{p^{i_1}}) \leq c_{17} m q^m.$$

DEMONSTRATION. Par définition

$$D_m = \prod_{j=1}^m (T^{q^j} - T)^{q^{m-j}}.$$

D'où

$$\prod_{i=1}^n D_{m_i} = \prod_{i=1}^n \prod_{j=1}^{m_i} (T^{q^j} - T)^{q^{m_i-j}} = \prod_{j=1}^{\max\{m_i\}} (T^{q^j} - T) \sum_{i=1}^n q^{m_i-j}.$$

On voit alors facilement que  $D_{m_1} \cdots D_{m_n}$  divise  $D_m$ . Comme  $\deg_T(D_m) = m q^m$ , on a de plus  $\sum_{i=1}^n m_i q^{m_i} \leq m q^m$ .

Soit  $P \in \mathbb{F}_q[T]$  tel que  $D_m = P D_{m_1} \cdots D_{m_n}$ ; on a donc  $\deg_T(P) \leq m q^m$ . On a alors

$$\begin{aligned} t((D_m e_{m_1} \cdots e_{m_n})^{p^{i_1}}) &\leq \deg_T(P^{p^{i_1}}) + \sum_{i=1}^n t((D_{m_i} e_{m_i})^{p^{i_1}}) + c_9(n-1) \\ &\leq p^{i_1} m q^m + c_{10} \sum_{i=1}^n m_i q^{m_i} + c_9(n-1) \\ &\leq p^{i_1} m q^m + c_{10} m q^m + c_9(n-1). \end{aligned}$$

La majoration  $n \leq q^m$  donne le résultat. □

LEMME 7. Soient  $(\theta_1, \dots, \theta_n, \theta_{n+1}) \in C^{n+1}$  et  $M \in C[X_1, \dots, X_n, X_{n+1}]$  unitaire en  $X_{n+1}$  tel que

$$M(\theta_1, \dots, \theta_n, \theta_{n+1}) = 0.$$

Alors il existe deux constantes  $c_{18} > 0$  et  $R_0 \geq 0$ , ne dépendant que des  $\theta_i$  et de  $M$ , telles que pour tout  $R \geq R_0$  et tout  $(\theta'_1, \dots, \theta'_n) \in C^n$ ,  $v(\theta_i - \theta'_i) \leq -R$ , alors il existe  $\theta'_{n+1} \in C$  vérifiant

$$v(\theta_{n+1} - \theta'_{n+1}) \leq -c_{18} R$$

$$M(\theta'_1, \dots, \theta'_n, \theta'_{n+1}) = 0.$$

DEMONSTRATION. Soit  $c_{19} > 0$  tel que

$$c_{19} \geq \max\{v(M(X_1, \dots, X_n, X_{n+1})), v(\theta_1), \dots, v(\theta_{n+1})\}.$$

Pour tout  $R \geq 0$  et  $(\theta'_1, \dots, \theta'_n) \in C^n$ ,  $v(\theta_i - \theta'_i) \leq -R$ ,

$$M(\theta'_1, \dots, \theta'_n, \theta_{n+1}) = M((\theta_1, \dots, \theta_n, \theta_{n+1}) + (\theta'_1 - \theta_1, \dots, \theta'_n - \theta_n, 0)).$$

Comme  $M(\theta_1, \dots, \theta_n, \theta_{n+1}) = 0$ , alors

$$v(M(\theta'_1, \dots, \theta'_n, \theta_{n+1})) \leq -R + c_{19} \deg_{X_1, \dots, X_{n+1}}(M).$$

Posons

$$M(\theta'_1, \dots, \theta'_n, X) = \prod_{i=1}^D (X - r_i),$$

donc

$$M(\theta'_1, \dots, \theta'_n, \theta_{n+1}) = \prod_{i=1}^D (\theta_{n+1} - r_i).$$

On en déduit facilement qu'il existe  $i_0$  tel que

$$v(\theta_{n+1} - r_{i_0}) \leq \frac{-R + c_{19} \deg_{X_1, \dots, X_n}(M)}{D}.$$

On pose alors  $\theta'_{n+1} = r_{i_0}$ . □

## 6. Démonstration du théorème

**THEOREME.** Soient  $\alpha_1, \dots, \alpha_n \in \bar{k}$  linéairement indépendants sur  $\Omega$ . On note  $t$  le degré de transcendance sur  $\mathbb{F}_q(T)$  de l'extension engendrée par  $e_\Lambda(\alpha_1), \dots, e_\Lambda(\alpha_n)$ . On a alors l'inégalité

$$td \geq nd_1.$$

DEMONSTRATION. On prend  $k_1, k_s, \alpha, B, \alpha_1, \dots, \alpha_n, \phi_T, \phi_{\gamma_1}, \dots, \phi_{\gamma_d}$ , vérifiant les conditions techniques non restrictives du paragraphe 5.

Soit  $L = k_s(e_\Lambda(\alpha_1), \dots, e_\Lambda(\alpha_n))$  et  $\theta_1, \dots, \theta_t$  une base de transcendance de  $L$  sur  $k_s$ . Soit  $p^{i_2}$  le degré d'inséparabilité de  $L$  sur  $k_s(\theta_1, \dots, \theta_t)$  et  $L_s$  la

sous-extension séparable maximale. Comme  $L_s$  est une extension finie de  $k_s(\theta_1, \dots, \theta_t)$ , il existe  $\theta_{t+1} \in L_s$  tel que

$$L_s = k_s(\theta_1, \dots, \theta_t)[\theta_{t+1}].$$

Le corps des fractions de  $B[\theta_1, \dots, \theta_t]$  étant égal à  $k_s(\theta_1, \dots, \theta_t)$ , on peut choisir  $\theta_{t+1}$  entier sur  $B[\theta_1, \dots, \theta_t]$ .

Soit  $i_3 = \max\{i_1, i_2\}$ . Comme  $p^{i_3}$  divise  $q^{i_3}$ , pour tout  $1 \leq i \leq n$  on a

$$e_\Lambda(\alpha_i)^{q^{i_3}} \in L_s.$$

On note  $\Delta \in B[\theta_1, \dots, \theta_t] - \{0\}$  un dénominateur commun aux  $e_\Lambda(\alpha_i)^{q^{i_3}}$ , c'est-à-dire pour tout  $1 \leq i \leq n$

$$\Delta e_\Lambda(\alpha_i)^{q^{i_3}} \in B[\theta_1, \dots, \theta_t][\theta_{t+1}].$$

Supposons  $td < nd_1$ , alors il existe  $\varepsilon > 0$  tel que

$$t(d + 2\varepsilon) < nd_1 - 4\varepsilon.$$

*Construction d'une fonction auxiliaire*

Pour tout  $m \in \mathbb{N}$ , on définit les fonctions  $x, y$  par

$$x = m(\log_q \log_q(m))^{-\varepsilon}$$

$$y = (\log_q \log_q(m))^{2\varepsilon}.$$

On fixe  $h \in \mathbb{N}$  tel que  $h\varepsilon > nd_1 - 4\varepsilon$ .

LEMME 8. *Il existe une constante  $c_{20}$  et  $m_0 \in \mathbb{N}$  tel que pour tout  $m \geq m_0$  alors il existe  $P_m$  non nul appartenant à  $A[X_1, \dots, X_h, Y_1, \dots, Y_h]$  vérifiant*

$$\deg_{X_1, \dots, X_h} P_m \leq x$$

$$\deg_{Y_1, \dots, Y_h} P_m \leq y$$

$$t(P_m) \leq c_{20} m \log_q(m) (\log_q \log_q(m))^{-h\varepsilon},$$

et tel que la fonction  $f_m$  définie par

$$f_m(z_1, \dots, z_h) = P_m(z_1^{q^{i_3}}, \dots, z_h^{q^{i_3}}, e_\Lambda(z_1)^{q^{i_3}}, \dots, e_\Lambda(z_h)^{q^{i_3}})$$

s'annule à l'ordre  $m$  en 0.

DEMONSTRATION. Soit  $P \in A[X_1, \dots, X_h, Y_1, \dots, Y_h]$  tel que

$$\deg_{X_1, \dots, X_h} P \leq x$$

$$\deg_{Y_1, \dots, Y_h} P \leq y.$$

On pose

$$P(x_1, \dots, x_h, y_1, \dots, y_h) = \sum_{\substack{\bar{k} \in \mathbb{N}^h \\ \bar{l} \in \mathbb{N}^h}} P_{\bar{k}, \bar{l}} x_1^{k_1} \cdots x_h^{k_h} y_1^{l_1} \cdots y_h^{l_h},$$

et  $e_\Lambda(z) = \sum_{j \in \mathbb{N}} e_j z^{q^j}$ . Soit  $f(z_1, \dots, z_h) = P(z_1^{q^{i_3}}, \dots, z_h^{q^{i_3}}, e_\Lambda(z_1)^{q^{i_3}}, \dots, e_\Lambda(z_h)^{q^{i_3}})$ . Ainsi on a

$$f(z_1, \dots, z_h) = \sum_{\substack{\bar{k} \in \mathbb{N}^h \\ \bar{l} \in \mathbb{N}^h}} P_{\bar{k}, \bar{l}} z_1^{k_1 q^{i_3}} \cdots z_h^{k_h q^{i_3}} \prod_{i=1}^h \left( \sum_{j \in \mathbb{N}} e_j^{q^{i_3}} z_i^{q^{j+i_3}} \right)^{l_i}.$$

Or

$$\left( \sum_{j \in \mathbb{N}} e_j^{q^{i_3}} z_i^{q^{j+i_3}} \right)^{l_i} = \sum_{n \in \mathbb{N}} \left( \sum_{q^{j_1+i_3} + \dots + q^{j_{l_i}+i_3} = n} e_{j_1}^{q^{i_3}} \cdots e_{j_{l_i}}^{q^{i_3}} \right) z_i^n.$$

Fixons  $\bar{N} \in \mathbb{N}^h$ . Le coefficient de taylor en  $z_1^{N_1} \cdots z_h^{N_h}$  de la fonction  $f$  vaut donc

$$\sum_{\substack{\bar{k} \in \mathbb{N}^h \\ \bar{l} \in \mathbb{N}^h}} P_{\bar{k}, \bar{l}} \left( \sum_{\bar{k} q^{i_3} + \bar{n} = \bar{N}} \prod_{i=1}^h \left( \sum_{q^{j_1+i_3} + \dots + q^{j_{l_i}+i_3} = n_i} e_{j_1}^{q^{i_3}} \cdots e_{j_{l_i}}^{q^{i_3}} \right) \right).$$

Pour que la fonction  $f$  s'annule à l'ordre  $m$ , il suffit donc de résoudre un système linéaire de  $\binom{m+h}{h}$  équations à  $\binom{[x]+h}{h} \binom{[y]+h}{h}$  inconnues, les inconnues étant les coefficients de  $P$ .

Comme  $p^{i_3}$  divise  $q^{i_3}$ , le lemme 6 nous dit que  $D_{[\log_q(m)]+1}^{hq^{i_3}}$  est un dénominateur commun aux coefficients du système, notés  $c_{i,j}$ . De plus ce lemme nous permet d'affirmer l'existence d'une constante  $c_{2,1}$  indépendante de  $m$  tel que

$$t(D_{[\log_q(m)]+1}^{hq^{i_3}} c_{i,j}) \leq c_{2,1} m \log_q(m).$$

Or

$$\binom{m+h}{h} \leq \frac{(m+h)^h}{h!} \quad \text{et} \quad \binom{[x]+h}{h} \geq \frac{[x]^h}{h!} \geq \frac{(m(\log_q \log_q(m))^{-\varepsilon} - 1)^h}{h!}.$$

De même

$$\binom{[y] + h}{h} \geq \frac{((\log_q \log_q(m))^{2\varepsilon} - 1)^h}{h!}.$$

Les conditions du théorème 3 sont donc remplies pour  $m \geq m_0$ . On peut alors affirmer qu'il existe un polynôme  $P_m$  tel que

$$\begin{aligned} t(P_m) &\leq \frac{\binom{m+h}{h}^\delta}{\binom{[x]+h}{h} \binom{[y]+h}{h} - \binom{m+h}{h}^\delta} c_{21} m \log_q(m) \\ &\leq c_{20} m \log_q(m) (\log_q \log_q(m))^{-h\varepsilon}. \end{aligned}$$

et  $P_m$  vérifie les autres conditions du lemme 8. □

A partir de maintenant on fixe une suite  $P_m$ ,  $m \geq m_0$  ayant les propriétés du lemme 8.

*Lemme de zéros*

On définit deux nouvelles fonctions de  $m$ , notées  $N$  et  $m'$ ,

$$\begin{aligned} q^N &= \log_q \log_q(m) \\ m' &= m (\log_q \log_q(m))^{-nd_1 + 4\varepsilon}. \end{aligned}$$

Pour tout  $(\alpha'_1, \dots, \alpha'_n) \in C^n$  et  $k$  réel  $> 0$ , on définit  $\Gamma_1(k)$  et  $\Gamma_2(k)$  par

$$\begin{aligned} \Gamma_1(k) &= \left\{ \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_1}} a_{i,j} \gamma_j \alpha_i \mid a_{i,j} \in A, \deg_T(a_{i,j}) \leq k \right\} \\ \Gamma_2(k) &= \left\{ e_\Lambda \left( \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_1}} a_{i,j} \gamma_j \alpha'_i \right) \mid a_{i,j} \in A, \deg_T(a_{i,j}) \leq k \right\}. \end{aligned}$$

Les  $\alpha_i$  étant linéairement indépendants sur  $\Omega$ , on a

$$\text{Card } \Gamma_1(k) = q^{nd_1((k+1))}.$$

Cela entraîne aussi que la définition suivante est cohérente.

$$\Gamma(k) = \left\{ (x_1, \dots, x_h, y_1, \dots, y_h) \left| \begin{array}{l} x_l = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_i}} a_{i,j,l} \gamma_j \alpha_i, \\ y_l = e_\Lambda \left( \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_i}} a_{i,j,l} \gamma_j \alpha_i \right) a_{i,j,l} \in A, \deg_T(a_{i,j,l}) \leq k \end{array} \right. \right\}.$$

On a de plus

$$\text{Card } \Gamma(k) = \text{Card } \Gamma_1(k)^h \geq q^{hnd, k}.$$

LEMME 9. *Il existe  $m_1 \geq m_0$  ayant la propriété suivante: pour tout  $m \geq m_1$  et tout  $(\alpha'_1, \dots, \alpha'_n) \in C^n$ , il existe  $(x_1, \dots, x_h, y_1, \dots, y_h) \in \Gamma(N)$  tel que la fonction*

$$P_m((x_1 + z_1)^{q^{i_3}}, \dots, (x_h + z_h)^{q^{i_3}}, (y_1 + e_\Lambda(z_1))^{q^{i_3}}, \dots, (y_h + e_\Lambda(z_h))^{q^{i_3}})$$

*ne s'annule pas à l'ordre  $2hm' + 1$  en 0.*

DEMONSTRATION. Supposons que pour tout  $(x_1, \dots, x_h, y_1, \dots, y_h) \in \Gamma(N)$  la fonction

$$P_m((x_1 + z_1)^{q^{i_3}}, \dots, (x_h + z_h)^{q^{i_3}}, (y_1 + e_\Lambda(z_1))^{q^{i_3}}, \dots, (y_h + e_\Lambda(z_h))^{q^{i_3}})$$

s'annule avec un ordre  $\geq 2hm' + 1$  en 0.

Notons  $d_x, d_y$  les degrés de  $P_m$  en  $X_1, \dots, X_n$  et  $Y_1, \dots, Y_n$ . D'après le lemme de zéros multihomogène de Jing Yu (voir [Y<sub>1</sub>]), il existe un sous  $\mathbb{F}_p[T]$  module propre  $G$  de  $C^{2h}$  tel que

$$\binom{m' + r(G)}{r(G)} \frac{\text{Card } \Gamma(N - 2h + 1)}{\text{Card } \Gamma(N - 2h + 1) \cap G} H(G, q^{i_3} d_x, q^{i_3} d_y) \leq C_1 (q^{i_3} d_x)^h (q^{i_3} d_y)^h,$$

où  $C_1$  est une constante qui ne dépend que de  $\Lambda$  et de  $h$ , tandis que  $H(G, q^{i_3} d_x, q^{i_3} d_y)$  est la partie multihomogène de plus haut degré du polynôme de Hilbert-Samuel de la variété  $G$  et  $r(G)$  est la codimension analytique de l'image réciproque  $G$  par l'application

$$F: (z_1, \dots, z_h) \rightarrow (z_1, \dots, z_h, e_\Lambda(z_1), \dots, e_\Lambda(z_h)).$$

Supposons dans un premier temps  $d_x$  et  $d_y$  non nuls.

(a) Estimation de  $\binom{m' + r(G)}{r(G)}$

Le réseau  $\Lambda$  étant de rang  $d > 0$ , il n'est homomorphe à 0 que pour le morphisme nul. Donc il existe  $G_1$  et  $G_2$ , sous  $\mathbb{F}_p[T]$  modules de  $C^h$  pour l'action triviale et pour l'action associée à  $\phi$ , respectivement, tel que

$$G = G_1 \times G_2,$$

(voir [D]).

D'après la classification des sous-modules (voir l'appendice),  $G_1$  est un sous  $C$  espace vectoriel de  $C^h$ ;  $T_{G_2}$ , l'espace tangent à  $G_2$ , est rationnel sur  $\Omega$  et

$$G_2 = \exp(T_{G_2})$$

$$\dim G_2 = \dim T_{G_2},$$

avec  $\exp(z_1, \dots, z_h) = (e_{\Lambda}(z_1), \dots, e_{\Lambda}(z_h))$ . On en déduit que

$$F^{-1}(G) = G_1 \cap \exp^{-1}(G_2) = G_1 \cap (T_{G_2} + \Lambda^h).$$

Soit

$$S: \sum_{i=1}^h \gamma_{i,j} z_i = 0, \quad 1 \leq j \leq h - \dim T_{G_2},$$

un système d'équations de  $T_{G_2}$  à coefficients dans  $\Omega$ . Soit  $r \in \mathbb{R}$  tel que

$$r < \min\{v(\lambda) \mid \lambda \in \Lambda - \{0\}\} - \max\{v(\gamma_{i,j}) \mid 1 \leq i \leq h, 1 \leq j \leq h - \dim T_{G_2}\}.$$

Pour tout  $z \in B(0, r) \cap (T_{G_2} + \Lambda^h)$ , écrivons  $z = g + \lambda$  avec  $g \in T_{G_2}$  et  $\lambda \in \Lambda^h$ . Comme  $g \in \ker S$ ,

$$S(z) = S(\lambda).$$

Or  $S(\lambda) \in \Lambda^{h - \dim T_{G_2}}$ , et, par le choix de  $r$ , cela implique

$$S(\lambda) = 0,$$

et donc  $z \in T_{G_2}$ . L'inclusion réciproque étant triviale, cela montre

$$B(0, r) \cap (T_{G_2} + \Lambda^h) = B(0, r) \cap T_{G_2}.$$

Donc  $B(0, r) \cap F^{-1}(G) = B(0, r) \cap (G_1 \cap T_{G_2})$  et la dimension analytique de  $F^{-1}(G)$  vaut alors  $\dim(G_1 \cap T_{G_2})$ . D'où

$$r(G) \geq h - \min\{\dim G_1, \dim G_2\}.$$



Donc

$$\binom{m' + r(G)}{r(G)} \geq \binom{m' + h - \min\{\dim G_1, \dim G_2\}}{r(G)}.$$

Or, pour  $m$  assez grand,  $h \leq m'/2$ , d'où

$$r(G) \leq \frac{m' + h - \min\{\dim G_1, \dim G_2\}}{2}$$

et donc

$$\binom{m' + r(G)}{r(G)} \geq \binom{m' + h - \min\{\dim G_1, \dim G_2\}}{h - \min\{\dim G_1, \dim G_2\}} \geq \frac{m'^{(h - \min\{\dim G_1, \dim G_2\})}}{h!}$$

(b) *Estimation de  $H(G, q^{i_3}d_x, q^{i_3}d_y)$*

On a d'après [P<sub>2</sub>]

$$H(G, q^{i_3}d_x, q^{i_3}d_y) = \frac{(\dim G)!}{(\dim G_1)!(\dim G_2)!} \deg G_1 \deg G_2 (q^{i_3}d_x)^{\dim G_1} (q^{i_3}d_y)^{\dim G_2}.$$

Donc  $H(G, q^{i_3}d_x, q^{i_3}d_y) \geq (q^{i_3}d_x)^{\dim G_1} (q^{i_3}d_y)^{\dim G_2}$ .

(c) *Estimation de  $\text{Card}(\Gamma(N - 2h + 1) \cap G)$*

Il est trivial que

$$\text{Card}(\Gamma(N - 2h + 1) \cap G) \leq \text{Card}(\Gamma_1(N - 2h + 1)^h \cap G_1).$$

Par la méthode du pivot de Gauss, il existe  $i_1, \dots, i_{\dim G_1}$  tel que la projection  $\Pi$

$$\Pi: \begin{cases} C^h \rightarrow C^{\dim G_1} \\ (z_1, \dots, z_h) \rightarrow (z_{i_1}, \dots, z_{i_{\dim G_1}}) \end{cases}$$

induit un isomorphisme entre  $G_1$  et  $C^{\dim G_1}$ . Or  $x \in \Gamma_1(N - 2h + 1)^h \cap G_1$  implique  $\Pi(x) \in \Gamma_1(N - 2h + 1)^{\dim G_1}$ . D'où

$$\text{Card}(\Gamma_1(N - 2h + 1)^h \cap G_1) \leq q^{nd_1(N - 2h + 3) \dim G_1}.$$

En réunissant toutes ces inégalités, on obtient, en divisant par  $d_x^{\dim G_1} d_y^{\dim G_2}$ ,

$$\frac{m'^{(h - \min\{\dim G_1, \dim G_2\})}}{h!} \frac{q^{nd_1 h(N - 2h + 1)}}{q^{nd_1(N - 2h + 3) \dim G_1}} \leq C_1 (q^{i_3}d_x)^{h - \dim G_1} (q^{i_3}d_y)^{h - \dim G_2}.$$

En tenant compte du fait que  $d_x \leq x$  et  $d_y \leq y$ , on obtient

$$m^{(h - \min\{\dim G_1, \dim G_2\})} (\log_q \log_q(m))^{((-nd_1 + 4\epsilon)(h - \min\{\dim G_1, \dim G_2\}) + nd_1(h - \dim G_1))} \\ \leq h! q^{nd_1(2h^2 + 2h)} q^{2hi_3} C_1 m^{(h - \dim G_1)} (\log_q \log_q(m))^{(-\alpha(h - \dim G_1) + 2\alpha(h - \dim G_2))}.$$

Cas 1.  $\dim G_2 < \dim G_1$ . Alors l'exposant de  $m$  à droite est strictement inférieur à celui de gauche. Donc pour  $m \geq m_2$ , avec  $m_2$  ne dépendant pas des  $\alpha'_i$ , ce cas là est impossible.

Cas 2.  $\dim G_1 \leq \dim G_2$ , l'équation implique

$$(\log_q \log_q(m))^{\alpha(3(h - \dim G_1) - 2(h - \dim G_2))} \leq h! q^{nd_1(2h^2 + 2h)} q^{2hi_3} C_1.$$

Comme  $G$  est un sous module propre,  $\dim G_1 < h$  et donc

$$3(h - \dim G_1) - 2(h - \dim G_2) \geq h - \dim G_1 > 0.$$

On en déduit qu'il existe  $m_3$  qui ne dépend pas des  $\alpha'_i$  tel que pour tout  $m \geq m_3$  ce cas soit impossible.

Reste à traiter les deux cas  $d_x = 0$  ou  $d_y = 0$ .

Si  $d_x = 0$  alors  $d_y \neq 0$  sinon  $P_m$  serait nul. De plus  $P_m$  est alors un polynôme en  $Y_1, \dots, Y_h$  tel que pour tout  $(y_1, \dots, y_h) \in \Gamma_2(N)^h$  la fonction

$$P_m((y_1 + e_\Lambda(z_1))^{q^{i_3}}, \dots, (y_h + e_\Lambda(z_h))^{q^{i_3}})$$

s'annule à l'ordre  $2hm' + 1$  en 0.

On applique le lemme de zéros de Jing-Yu à  $C^h$  muni de l'action associée à  $\phi$ . Il existe  $G \subset C^h$  sous  $F_p[T]$  module propre tel que

$$\left( \frac{2m' + r(G)}{r(G)} \right) \frac{\text{Card } \Gamma_2(N - h + 1)^h}{\text{Card } \Gamma_2(N - h + 1)^h \cap G} H(G, q^{i_3} d_y) \leq C_2 (q^{i_3} d_y)^h$$

où  $r(G)$  est la codimension analytique de  $\exp^{-1}(G)$  et  $C_2$  une constante qui ne dépend que de  $\Lambda$  et de  $h$ .

Par des considérations analogues à celles du paragraphe précédent, on a

$$\frac{(2m')^{h - \dim G}}{h!} \leq C_2 (q^{i_3} d_y)^{h - \dim G}.$$

D'où

$$(2m)^{h - \dim G} \leq h! q^{hi_3} C_2 (\log_q \log_q(m))^{(nd_1 - 2\epsilon)(h - \dim G)}.$$

Comme  $\dim G < h$ , il existe  $m_4$  ne dépendant pas des  $\alpha'_i$  tel que pour tout  $m \geq m_4$  ce soit impossible.

Si  $d_y = 0$  alors  $d_x \neq 0$  sinon  $P_m$  serait nul. De plus  $P_m$  est alors un polynôme en  $X_1, \dots, X_h$  tel que pour tout  $(x_1, \dots, x_h) \in \Gamma_1(N)^h$  la fonction

$$P_m((x + z_1)^{q^{i_3}}, \dots, (x_h + z_h)^{q^{i_3}})$$

s'annule à l'ordre  $2hm' + 1$  en 0.

On applique le lemme de zéros de Jing-Yu à  $C^h$  muni de l'action triviale. Il existe  $G \subset C^h$  sous  $\mathbb{F}_p[T]$  module propre, c'est-à-dire un sous espace vectoriel de  $C^h$ , tel que

$$\binom{2m' + r(G)}{r(G)} \frac{\text{Card } \Gamma_1(N - h + 1)^h}{\text{Card } \Gamma_1(N - h + 1)^h \cap G} H(G, q^{i_3} d_x) \leq C_3 (q^{i_3} d_x)^h$$

où  $r(G)$  est la codimension de  $G$  et  $C_3$  une constante qui ne dépend que de  $h$ .

Par des considérations analogues à celles du paragraphe précédent, on a

$$\frac{(2m')^{h - \dim G}}{h!} \frac{q^{nd_1 h(N-h+1)}}{q^{nd_1(N-h+3)\dim G}} \leq C_3 (q^{i_3} d_x)^{h - \dim G}.$$

En utilisant les définitions de  $N$ ,  $m'$  et  $x$ , on a

$$2^{h - \dim G} (\log_q \log_q(m))^{3d(h - \dim G)} \leq C_3 h! q^{h^2} q^{nd_1(h^2 + 2h)}.$$

Comme  $\dim G < h$ , il existe  $m_5$  ne dépendant pas des  $\alpha'_i$  tel que pour tout  $m \geq m_5$  ce soit impossible.

On a alors le résultat en prenant  $m_1 \geq \max\{m_0, m_2, m_3, m_4, m_5\}$ . □

### Application du critère d'indépendance algébrique

LEMME 10. Il existe  $c_{22}$  tel que pour tout  $m \geq m_0$  et tout  $m'_1, \dots, m'_h \in \mathbb{N}$  vérifiant

$$m'_1 + \dots + m'_h \leq 2hm' + 1,$$

alors il existe  $P_{m, m'_1, \dots, m'_h} \in B[X_1, \dots, X_n, Y_1, \dots, Y_h]$  tel que

$$\deg_{X_1, \dots, X_n} P_{m, m'_1, \dots, m'_h} \leq x$$

$$\deg_{Y_1, \dots, Y_h} P_{m, m'_1, \dots, m'_h} \leq y$$

$$i(P_{m, m'_1, \dots, m'_h}) \leq c_{22} m \log_q(m) (\log_q \log_q(m))^{-nd_1 + 4\epsilon}$$

et pour tout  $(x_1, \dots, x_h, y_1, \dots, y_h) \in C^{2h}$  le coefficient d'ordre  $m'_1, \dots, m'_h$ , noté  $C_{m'_1, \dots, m'_h}$ , de la fonction

$$P_m((x_1 + z_1)^{q^{i_3}}, \dots, (x_h + z_h)^{q^{i_3}}, (y_1 + e_\Lambda(z_1))^{q^{i_3}}, \dots, (y_h + e_\Lambda(z_h))^{q^{i_3}})$$

vérifie la relation

$$(D_{[\log_q(2hm') + 1] + 1})^{hq^{i_3}} C_{m'_1, \dots, m'_h} = P_{m, m'_1, \dots, m'_h}(x_1^{q^{i_3}}, \dots, x_h^{q^{i_3}}, y_1^{q^{i_3}}, \dots, y_h^{q^{i_3}}). \quad (1)$$

DEMONSTRATION. Ecrivons

$$\begin{aligned} & P_m((x_1 + z_1)^{q^{i_3}}, \dots, (x_h + z_h)^{q^{i_3}}, (y_1 + e_\Lambda(z_1))^{q^{i_3}}, \dots, (y_h + e_\Lambda(z_h))^{q^{i_3}}) \\ &= \sum_{\bar{k}, \bar{j} \in \mathbb{N}^h} P_{\bar{k}, \bar{j}} \prod_{i=1}^h (x_i^{q^{i_3}} + z_i^{q^{i_3}})^{k_i} \prod_{i=1}^h (y_i^{q^{i_3}} + e_\Lambda(z_i)^{q^{i_3}})^{l_i}. \end{aligned}$$

On a de plus

$$(x_i^{q^{i_3}} + z_i^{q^{i_3}})^{k_i} = \sum_{j=0}^{k_i} \binom{k_i}{j} x_i^{q^{i_3}(k_i - j)} z_i^{q^{i_3}j}.$$

En posant  $q^{-\infty} = 0$ , on a

$$y_i^{q^{i_3}} + e_\Lambda(z_i)^{q^{i_3}} = \sum_{r \in \mathbb{N} \cup \{-\infty\}} e_{r,i}^{q^{i_3}} z_i^{q^{i_3} + j},$$

où  $e_{-\infty, i} = y_i$  et  $e_{r,i} = e_r$  pour tout  $r > 0$ . Donc

$$(y_i^{q^{i_3}} + e_\Lambda(z_i)^{q^{i_3}})^{l_i} = \sum_{n_i \in \mathbb{N}} \left( \sum_{q^{i_3}(q^{r_1} + \dots + q^{r_{l_i}}) = n_i} e_{r_1, i}^{q^{i_3}} \dots e_{r_{l_i}, i}^{q^{i_3}} \right) z_i^{n_i}.$$

Le coefficient d'ordre  $m'_1, \dots, m'_h$  vaut donc

$$\sum_{\bar{k}, \bar{j} \in \mathbb{N}^h} P_{\bar{k}, \bar{j}} \left( \sum_{\bar{n} + \bar{j}q^{i_3} = (m'_1, \dots, m'_h)} \prod_{i=1}^h \binom{k_i}{j_i} x_i^{q^{i_3}(k_i - j_i)} \prod_{i=1}^h \left( \sum_{q^{i_3}(q^{r_1} + \dots + q^{r_{l_i}}) = n_i} e_{r_1, i}^{q^{i_3}} \dots e_{r_{l_i}, i}^{q^{i_3}} \right) \right).$$

Il existe donc un polynôme  $P_{m, m'_1, \dots, m'_h}$  vérifiant la relation (1). En tenant compte des conditions imposées à  $P_m$  par le lemme 8 et en utilisant le lemme 6, il existe une constante  $c_{23}$  telle que

$$\deg_{x_1, \dots, x_h} P_{m, m'_1, \dots, m'_h} \leq x$$

$$\deg_{y_1, \dots, y_h} P_{m, m'_1, \dots, m'_h} \leq y$$

$$t(P_{m, m'_1, \dots, m'_h}) \leq t(P_m) + c_{23} m' \log_q(m').$$

Or

$$t(P_m) \leq c_{20} m \log_q(m) (\log_q \log_q(m))^{-h\varepsilon}$$

$$m' \log_q(m') \sim m \log_q(m) (\log_q \log_q(m))^{-nd_1 + 4\varepsilon}.$$

Comme  $h\varepsilon > nd_1 - 4\varepsilon$ , on a le résultat. □

On convient pour tout

$$P \in C[X], \left( \sum_{i=1}^n P_i X_i \right)^{*q^{i_3}} = \sum_{i=1}^n P_i^{q^{i_3}} X_i.$$

Alors pour tout  $\alpha'_1, \dots, \alpha'_n \in C$  et  $(x_1, \dots, x_h, y_1, \dots, y_h) \in \Gamma(N)$ , c'est-à-dire pour

$$x_l = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_1}} a_{i,j,l} \gamma_j \alpha_i \quad \text{et} \quad y_l = e_\Lambda \left( \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_1}} a_{i,j,h} \gamma_j \alpha_i \right),$$

le polynôme  $Q(X_1, \dots, X_n)$  égal à

$$P_{m,m'_1, \dots, m'_h} \left( \left( \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_1}} a_{i,j,1} \gamma_j \alpha_i \right)^{q^{i_3}}, \dots, \left( \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_1}} a_{i,j,h} \gamma_j \alpha_i \right)^{q^{i_3}} \right),$$

$$\times \left( \sum_{i=1}^n \phi(\Sigma_{j=1}^{d_1} a_{i,j,1} \gamma_j) \right)^{*q^{i_3}} (X_i), \dots, \left( \sum_{i=1}^n \phi(\Sigma_{j=1}^{d_1} a_{i,j,h} \gamma_j) \right)^{*q^{i_3}} (X_i)$$

vérifie la relation

$$Q(e_\Lambda(\alpha'_1)^{q^{i_3}}, \dots, e_\Lambda(\alpha'_n)^{q^{i_3}}) = (D_{[\log_q(2hm' + 1)] + 1})^{hq^{i_3}} C_{m'_1, \dots, m'_h}.$$

Soit  $c_{24} = \max\{\deg_r(\phi_{\gamma_i}) \mid 1 \leq i \leq d_1\}$ , on a alors

$$\deg_{X_1, \dots, X_n} Q \leq yq^{dN + c_{24}}.$$

Donc il existe  $c_{25}$  tel que

$$\deg_{X_1, \dots, X_n} Q \leq c_{25} (\log_q \log_q(m))^{d + 2\varepsilon}.$$

En utilisant les lemmes 5 et 10, on a de plus

$$t(Q) \leq c_{22} m \log_q(m) (\log_q \log_q(m))^{-nd_1 + 4\varepsilon}$$

$$+ x(q^{i_3} N + \max\{t((\alpha_i \gamma_j)^{q^{i_3}})\}) + \frac{q^{i_3}}{p^{i_1}} y c_{12} q^{dN} + c_9 \left( x + \frac{q^{i_3}}{p^{i_1}} y \right).$$

Il existe donc  $c_{26}$  tel que

$$t(Q) \leq c_{26} m \log_q(m) (\log_q \log_q(m))^{-nd_1 + 4\epsilon}.$$

Soit  $M \in B[X_1, \dots, X_t][X]$  unitaire en  $X$  tel que

$$M[\theta_1, \dots, \theta_t][\theta_{t+1}] = 0.$$

Soit  $R_0$  comme au lemme 7; pour tout  $(\theta'_1, \dots, \theta'_t) \in B((\theta_1, \dots, \theta_t), -R_0)$ , on choisit  $\theta'_{t+1}$  comme étant une racine de  $M(\theta'_1, \dots, \theta'_t)[X] = 0$  ayant la propriété d'être la plus proche de  $\theta_{t+1}$ . Le lemme 7 nous donne alors pour tout  $R \geq R_0$  et  $(\theta'_1, \dots, \theta'_t) \in B((\theta_1, \dots, \theta_t), -R)$

$$v(\theta'_{t+1} - \theta_{t+1}) \leq -c_{18}R.$$

Soit  $\Delta$  le dénominateur commun aux  $e_\Lambda(\alpha_i)^{q^{i3}}$  défini plus haut. Comme  $\Delta(\theta_1, \dots, \theta_t) \neq 0$ , il existe  $R_1 \geq R_0$  tel que pour tout

$$(\theta'_1, \dots, \theta'_t) \in B((\theta_1, \dots, \theta_t), -R_1)$$

$$\Delta(\theta'_1, \dots, \theta'_t) \neq 0.$$

Soit  $R(m) = m \log_q(m)$ , il existe donc  $m_6 \geq m_1$  tel que pour tout  $m \geq m_6$  on ait

$$R(m) \geq R_1.$$

Pour tout  $1 \leq i \leq t$ , il existe  $P_i \in B[X_1, \dots, X_{t+1}]$  tel que

$$\Delta(\theta_1, \dots, \theta_t) e_\Lambda(\alpha_i)^{q^{i3}} = P_i(\theta_1, \dots, \theta_t, \theta_{t+1}).$$

Pour tout  $m \geq m_6$  et  $(\theta'_1, \dots, \theta'_t) \in B((\theta_1, \dots, \theta_t), -R(m))$  on choisit  $\alpha'_i$  vérifiant la relation

$$\Delta(\theta'_1, \dots, \theta'_t) e_\Lambda(\alpha'_i)^{q^{i3}} = P_i(\theta'_1, \dots, \theta'_t, \theta'_{t+1}).$$

On prendra  $\alpha'_i = \alpha_i$  si  $\theta'_i = \theta_i$ .

Le lemme 9 nous assure qu'il existe  $(x_1, \dots, x_h, y_1, \dots, y_h) \in \Gamma(N)$  tel que la fonction

$$P_m((x + z_1)^{q^{i3}}, \dots, (x_h + z_h)^{q^{i3}}, (y_1 + e_\Lambda(z_1))^{q^{i3}}, \dots, (y_h + e_\Lambda(z_h))^{q^{i3}})$$

ne s'annule pas à l'ordre  $2hm' + 1$  en 0. Donc il existe  $m'_1, \dots, m'_h$  avec

$m'_1 + \dots + m'_h \leq 2hm' + 1$ , et  $a_{i,j,l} \in A$ ,  $\deg_T(a_{i,j,l}) \leq N$  tel que

$$Q(e_\Lambda(\alpha'_1)^{q^{i_3}}, \dots, e_\Lambda(\alpha'_n)^{q^{i_3}}) \neq 0.$$

On pose alors

$$\begin{aligned} & Q_{m,\theta_1,\dots,\theta_t}(X_1, \dots, X_t) \\ &= \Delta(X_1, \dots, X_t)^{\lfloor c_{25}(\log_q \log_q(m))^{d+2\epsilon} \rfloor + 1} Q\left(\frac{P_1(X_1, \dots, X_t)}{\Delta(X_1, \dots, X_t)}, \dots, \frac{P_n(X_1, \dots, X_t)}{\Delta(X_1, \dots, X_t)}\right). \end{aligned}$$

En particulier,

$$\begin{aligned} & Q_{m,\theta_1,\dots,\theta_t}(\theta'_1, \dots, \theta'_{t+1}) \\ &= \Delta(\theta'_1, \dots, \theta'_t)^{\lfloor c_{25}(\log_q \log_q(m))^{d+2\epsilon} \rfloor + 1} Q(e_\Lambda(\alpha'_1)^{q^{i_3}}, \dots, e_\Lambda(\alpha'_n)^{q^{i_3}}) \neq 0. \end{aligned}$$

De plus,  $Q_{m,\theta_1,\dots,\theta_t} \in B[X_1, \dots, X_{t+1}]$  et il existe  $c_{27}$  tel que

$$\begin{aligned} \deg_{X_1, \dots, X_{t+1}} Q_{m,\theta_1, \dots, \theta_t} &\leq c_{27} (\log_q \log_q(m))^{d+2\epsilon} \\ t(Q_{m,\theta_1, \dots, \theta_t}) &\leq c_{27} m \log_q(m) (\log_q \log_q(m))^{-nd_1 + 4\epsilon}. \end{aligned}$$

Pour majorer les  $v(Q_{m,\theta_1,\dots,\theta_t}(\theta'_1, \dots, \theta'_{t+1}))$ , on utilise le lemme de Schwarz, ce lemme dit ceci:

**LEMME DE SCHWARZ.** *Soit  $f \in k[[X_1, \dots, X_h]]$  une série entière en  $h$  variables, partout convergente. Pour  $r \in \mathbb{R}$ , notons*

$$\begin{aligned} M(f, r) &= \max\{v(f(z_1, \dots, z_h)) \mid v(z_i) \leq r\} \\ &= \max\{v(c_{m_1, \dots, m_h}) + r(m_1 + \dots + m_h)\}, \end{aligned}$$

avec  $f(z_1, \dots, z_h) = \sum_{m_1, \dots, m_h \in \mathbb{N}} c_{m_1, \dots, m_h} z_1^{m_1} \dots z_h^{m_h}$ . Si  $f$  s'annule à l'ordre  $m$  en 0 alors pour tout  $R \geq r$

$$M(f, r) \leq m(r - R) + M(f, R).$$

Pour vérifier la cohérence de la double définition de  $M(f, r)$  et le lemme de Schwarz, voir [A].

Par le lemme 10, on a

$$\begin{aligned} & Q_{m,\theta_1,\dots,\theta_t}(\theta_1, \dots, \theta_{t+1}) \\ &= \Delta(\theta_1, \dots, \theta_t)^{\lfloor c_{25}(\log_q \log_q(m))^{d+2\epsilon} \rfloor + 1} D_{\lfloor \log_q(2hm' + 1) \rfloor + 1}^{hq^{i_3}} C_{m'_1, \dots, m'_h}, \end{aligned}$$

avec  $C_{m'_1, \dots, m'_h}$  le coefficient d'ordre  $m'_1, \dots, m'_h$  de la fonction

$$g_m(z_1, \dots, z_h) = P_m((x_1 + z_1)^{q^{i_3}}, \dots, (x_h + z_h)^{q^{i_3}}, (e_\Lambda(x_1 + z_1))^{q^{i_3}}, \dots, (e_\Lambda(x_h + z_h))^{q^{i_3}})$$

avec  $m'_1 + \dots + m'_h \leq 2hm' + 1$ , où  $x_i$  a été défini plus haut.

Pour une distance ultramétrique, tous les points d'une boule sont aussi centre de cette boule. On en déduit donc

$$M(g_m, r) = M(f_m, r).$$

dès que  $r \geq N + \max\{v(\alpha_i \gamma_j)\}$  et  $f_m$  la fonction définie au lemme 8. Soit  $m_7 \geq m_6$  tel que pour tout  $m \geq m_7$ ,  $N + \max\{v(\alpha_i \gamma_j)\} \geq 0$ . On pose

$$r = N + \max\{v(\alpha_i \gamma_j)\}.$$

On a donc pour tout  $R \geq r$

$$v(C_{m'_1, \dots, m'_h}) \leq m(r - R) + M(f_m, R).$$

Or  $e_\Lambda$  est d'ordre de croissance inférieur à  $d$  (voir [Y<sub>2</sub>]), donc, il existe  $c_{28}$  tel que pour tout  $R$

$$M(e_\Lambda, R) \leq c_{28} q^{(d+\varepsilon)R}.$$

Donc

$$M(f_m, R) \leq q^{i_3}(xR + c_{28} y q^{(d+\varepsilon)R}) + t(P_m) \max\{0, (\delta - 1)v(\alpha)\}.$$

En prenant  $R = \log_q(m)/d + \varepsilon$ , alors  $R > r$ , si  $m \geq m_8 \geq m_7$ , et il existe donc  $c_{29} > 0$  tel que pour tout  $m \geq m_8$

$$v(C_{m'_1, \dots, m'_h}) \leq -c_{29} m \log_q(m).$$

On en déduit immédiatement qu'il existe  $c_{30} > 0$  tel que pour tout  $m \geq m_8$

$$v(Q_{m, \theta_1, \dots, \theta_t}(\theta_1, \dots, \theta_{t+1})) \leq -c_{30} m \log_q(m).$$

Or

$$\begin{aligned} & Q_{m, \theta_1, \dots, \theta_t}(\theta'_1, \dots, \theta'_{t+1}) \\ &= Q_{m, \theta_1, \dots, \theta_t}(\theta_1 + (\theta'_1 - \theta_1), \dots, \theta_{t+1} + (\theta'_{t+1} - \theta_{t+1})). \end{aligned}$$



Comme  $v(\theta_i - \theta'_i) \leq -\min\{1, c_{18}\}m \log_q(m)$  et que la valuation des coefficients de  $Q_m \ll m \log_q(m)$ , on a

$$v(Q_{m, \theta_1, \dots, \theta_t}(\theta'_1, \dots, \theta'_{t+1})) \leq -c_{31}m \log_q(m).$$

En posant

$$R(m) = m \log_q(m)$$

$$S(m) = m \log_q(m)$$

$$T(m) = c_{27}m \log_q(m)(\log_q \log_q(m))^{-nd_1 + 4\varepsilon} + \delta$$

$$D(m) = c_{25}(\log_q \log_q(m))^{2\varepsilon + d},$$

on peut appliquer le théorème 2, car  $t(d + 2\varepsilon) < nd_1 - 4\varepsilon$  entraîne

$$\lim_{n \rightarrow \infty} \frac{S(m)}{T(m)D(m)^t} = +\infty. \quad \square$$

### Appendice: classification des sous-modules

La première classification des sous-modules d'une puissance d'un module de Drinfeld apparaît dans le cours de troisième cycle de M. Waldschmidt en 89. La démonstration en est malheureusement incomplète. Dans sa thèse, L. Denis donne également une classification un peu différente. Ce paragraphe est consacré à la démonstration de la version donnée par M. Waldschmidt.

Soit  $p$  un nombre premier,  $q$  une puissance de  $p$  et  $C$  un corps de caractéristique  $p$  algébriquement clos et complet pour une valuation  $v$ . Le Frobenius  $x \rightarrow x^q$  sera noté  $\tau$ .

Soit  $A \subset C$  un anneau contenant  $\mathbb{F}_q$ ; on suppose qu'il existe  $x \in A$  tel que  $v(x) > 0$ . Soit  $\phi: A \rightarrow C\{\tau\}$  un module de Drinfeld de rang  $d$  sur  $\mathbb{F}_q[x]$ . On note  $\Lambda$  et  $e_\Lambda$  le réseau et la fonction exponentielle associée à  $\phi$ , et  $R$  l'anneau des multiplications complexes de  $\Lambda$ .

Soit  $n \in \mathbb{N}$ . Pour tout  $(x_1, \dots, x_n) \in C^n$  on note

$$\exp(x_1, \dots, x_n) = (e_\Lambda(x_1), \dots, e_\Lambda(x_n)).$$

De plus, on définit l'action de  $A$  par

$$a * (x_1, \dots, x_n) = (\phi_a(x_1), \dots, \phi_a(x_n)), \text{ pour tout } a \in A.$$

On remarque que  $a * \exp(x_1, \dots, x_n) = \exp(ax_1, \dots, ax_n)$ .

DEFINITION. On appelle sous  $A$  module de  $C^n$  tout sous-groupe additif algébrique connexe stable par l'action de  $A$ .

DEFINITION. Soit  $H$  un sous  $A$  module de  $C^n$ . On appelle espace tangent à  $H$ , noté  $T_H$ , le sous-espace vectoriel de  $C^n$  défini par

$$T_H = \{(x_1, \dots, x_n) \in C^n \mid \text{pour tout } z \in C \exp(zx_1, \dots, zx_n) \in H\}.$$

Le théorème principal de ce paragraphe est le suivant.

THEOREME. Les applications  $\text{Exp}$  et  $T$ , ayant pour domaines de définition respectifs l'ensemble des sous espaces vectoriels  $V \subset C^n$  rationnels sur  $R$  et l'ensemble des sous  $A$  modules  $H$ , définies par

$$\text{Exp}: V \rightarrow \exp(V)$$

$$T: H \rightarrow T_H$$

sont des bijections réciproques. On a de plus

$$\dim H = \dim T_H.$$

Pour faire la démonstration de ce théorème, nous procéderons par étapes.

*Etape 1: cas des sous-modules de codimension 1*

Soit  $H$  un sous  $A$  module de  $C^n$  de dimension  $n - 1$ . Pour les groupes algébriques, les composantes connexes correspondent aux composantes irréductibles. Donc  $H$  est irréductible et

$$I(H) = \{P \in C[X_1, \dots, X_n] \mid P(H) = 0\}$$

est un idéal premier de  $C[X_1, \dots, X_n]$ . De plus cet idéal est principal car  $\dim H = n - 1$  (voir [H]). Soit  $P$  un générateur; on a alors

$$H = Z(P) = \{(x_1, \dots, x_n) \mid P(x_1, \dots, x_n) = 0\}.$$

Comme  $H$  est un  $\mathbb{F}_q$ -espace vectoriel et que  $P$  est un polynôme de degré minimal s'annulant sur  $H$ ,  $P$  est  $\mathbb{F}_q$ -linéaire. On pose

$$P(x_1, \dots, x_n) = P_1(x_1) + \dots + P_n(x_n),$$

avec  $P_i \in C\{\tau\}$ . Or  $H$  est stable par  $A$ , d'où pour tout  $a \in A$

$$P_1 \circ \phi_a(x_1) + \dots + P_n \circ \phi_a(x_n) \in I(H);$$

c'est-à-dire  $\ker P \subset \ker(P_1 \circ \phi_a(x_1) + \cdots + P_n \circ \phi_a(x_n))$ . L'application  $P$  étant surjective, il existe une unique application  $\mathbb{F}_q$ -linéaire  $\psi_a : C \rightarrow C$  telle que

$$P_1 \circ \phi_a(x_1) + \cdots + P_n \circ \phi_a(x_n) = \psi_a(P_1(x_1) + \cdots + P_n(x_n)).$$

Donc, pour tout  $i$ , on a  $P_i \circ \phi_a = \psi_a \circ P_i$ . Comme  $P$  est irréductible, il existe  $j$  tel que  $P_j \neq 0$  car sinon  $P$  serait une puissance  $q$ -ième d'un polynôme. L'anneau  $C\{\tau\}$  étant euclidien à droite, il existe donc  $Q_a, R_a \in C\{\tau\}$  tel que

$$P_j \circ \phi_a = Q_a \circ P_j + R_a$$

$$\deg_{\tau} R_a < \deg_{\tau} P_j.$$

D'où  $R_a = (\psi_a - Q_a) \circ P_j$ . Donc le polynôme  $R_a$  s'annule dès que  $P_j$  s'annule. Or les racines de  $P_j$  sont distinctes et  $\deg_{\tau} R_a < \deg_{\tau} P_j$ , ceci entraîne que  $R_a$  est nul et donc

$$\psi_a = Q_a \in C\{\tau\}.$$

De plus  $\psi'_a P'_j = P'_j \phi'_a$ . Donc

$$\psi'_a = \phi'_a = a.$$

Il est facile de vérifier que  $a \rightarrow \psi_a$  est un morphisme d'anneaux.

On a donc montré que  $\psi : A \rightarrow C\{\tau\}$  est un module de Drinfeld. Les  $P_i$  sont donc des morphismes de  $\phi$  vers  $\psi$ . Notons  $\Lambda'$  le réseau associé à  $\psi$ , qui est donc de même rang sur  $\mathbb{F}_q[x]$  que  $\Lambda$ , et  $\gamma_i \in C$  le morphisme de réseau associé à  $P_i$ , c'est-à-dire

$$\gamma_i \Lambda \subset \Lambda'$$

$$e_{\Lambda'}(\gamma_i z) = P_i \circ e_{\Lambda}(z).$$

Notons  $L : C^n \rightarrow C$  la forme linéaire définie par

$$L(x_1, \dots, x_n) = \sum_{i=1}^n \gamma_i x_i.$$

LEMME. *Avec les notations précédentes,  $\ker L$  est rationnel sur  $R$ , et on a*

$$T_H = \ker L$$

$$H/\text{Exp}(T_H) \simeq \Lambda'/L(\Lambda^n).$$

DEMONSTRATION. La première égalité provient des équivalences suivantes.

$$\begin{aligned}
 (x_1, \dots, x_n) \in T_H &\Leftrightarrow \forall z \in C \exp(zx_1, \dots, zx_n) \in H \\
 &\Leftrightarrow \forall z \in C \sum_{i=1}^n P_i(e_{\Lambda}(zx_i)) = 0 \\
 &\Leftrightarrow \forall z \in C \sum_{i=1}^n e_{\Lambda'}(\gamma_i zx_i) = 0 \\
 &\Leftrightarrow \forall z \in C e_{\Lambda'} \left( \left( \sum_{i=1}^n \gamma_i x_i \right) z \right) = 0 \\
 &\Leftrightarrow \sum_{i=1}^n \gamma_i x_i = 0 \\
 &\Leftrightarrow (x_1, \dots, x_n) \in \ker L.
 \end{aligned}$$

Comme  $\Lambda$  est homomorphe à  $\Lambda'$  et qu'ils sont de même rang, il existe  $b \in C^*$  tel que

$$b\Lambda' \subset \Lambda.$$

D'où, pour tout  $i$ ,  $b\gamma_i \Lambda \subset b\Lambda' \subset \Lambda$ . Donc

$$b\gamma_i \in R.$$

On a donc montré que  $T_H$  est rationnel sur  $R$ .

Il est trivial que  $\text{Exp}(T_H) \subset H$ . Soit  $(x_1, \dots, x_n) \in C^n$  tel que

$$\exp(x_1, \dots, x_n) \in H.$$

D'où

$$P(\exp(x_1, \dots, x_n)) = 0.$$

Par un calcul fait plus haut, cela entraîne  $e_{\Lambda'}(\sum_{i=1}^n \gamma_i x_i) = 0$ . Donc  $\sum_{i=1}^n \gamma_i x_i \in \Lambda'$ .

Soit  $f$  l'application définie par

$$f: \begin{cases} H \rightarrow \Lambda'/L(\Lambda^n) \\ \exp(x_1, \dots, x_n) \rightarrow \sum_{i=1}^n \gamma_i x_i \text{ mod } L(\Lambda^n). \end{cases}$$

L'application  $f$  est bien définie car  $\exp(x_1, \dots, x_n) = \exp(y_1, \dots, y_n)$  si et seulement si pour tout  $1 \leq i \leq n$ ,  $x_i - y_i \in \Lambda$ .

Soit  $j$  tel que  $\gamma_j \neq 0$ . Pour tout  $\lambda' \in \Lambda'$ ,

$$(0, \dots, e_\Lambda(\lambda'/\gamma_j), \dots, 0) \in H,$$

car  $P(0, \dots, e_\Lambda(\lambda'/\gamma_j), \dots, 0) = P_j(e_\Lambda(\lambda'/\gamma_j)) = e_\Lambda(\gamma_j(\lambda'/\gamma_j)) = 0$ . De plus

$$f\left(\left(0, \dots, e_\Lambda\left(\frac{\lambda'}{\gamma_j}\right), \dots, 0\right)\right) = \lambda' \bmod L(\Lambda^n).$$

Donc  $f$  est surjective.

L'application  $f$  étant additive, le lemme sera montré si on prouve  $\ker f = \text{Exp}(T_H)$ .

Comme  $T_H = \ker L$ , on a trivialement

$$\text{Exp}(T_H) \subset \ker f.$$

Réciproquement, soit  $\exp(x_1, \dots, x_n) \in \ker f$ , c'est-à-dire  $\sum_{i=1}^n \gamma_i x_i \in L(\Lambda^n)$ . Donc il existe  $\lambda_1, \dots, \lambda_n \in \Lambda$  tel que

$$\sum_{i=1}^n (x_i - \lambda_i) \gamma_i = 0.$$

D'où  $\exp(x_1, \dots, x_n) = \exp(x_1 - \lambda_1, \dots, x_n - \lambda_n) \in \text{Exp}(\ker L)$ . □

On peut maintenant montrer une première partie du théorème.

**THEOREME.** *Soit  $H$  un sous  $A$  module de  $C^n$  de dimension  $n - 1$ ; alors*

$$H = \text{Exp}(T_H).$$

**DEMONSTRATION.** Grâce au lemme et avec les notations précédentes, il suffit de voir que

$$\Lambda' = L(\Lambda^n).$$

On pose  $\Lambda'' = L(\Lambda^n)$ . Il s'agit bien d'un réseau de  $C$  car  $\Lambda'' \subset \Lambda'$ . Comme  $\gamma_j \Lambda \subset \Lambda''$  avec  $\gamma_j \neq 0$ , on en déduit que le rang de  $\Lambda''$  est égal à celui de  $\Lambda$  et  $\Lambda'$ .

Pour tout  $1 \leq i \leq n$ ,  $\gamma_i \Lambda \subset \Lambda''$ . Donc il existe  $Q_i \in C\{\tau\}$  tel que

$$e_{\Lambda''}(\gamma_i z) = Q_i \circ e_\Lambda(z).$$

De même comme  $\Lambda'' \subset \Lambda'$ , il existe  $S \in C\{\tau\}$  tel que

$$e_{\Lambda'}(z) = S \circ e_{\Lambda''}(z).$$

De plus

$$P_i(e_{\Lambda}(z)) = e_{\Lambda'}(\gamma_i z) = S(e_{\Lambda''}(\gamma_i z)) = S(Q_i(e_{\Lambda}(z))).$$

D'où pour tout  $i$

$$S \circ Q_i = P_i.$$

D'où  $P = S \circ (\sum_{i=1}^n Q_i(x_i))$ . Donc  $\sum_{i=1}^n Q_i(x_i)$  divise  $P$  car  $S(0) = 0$ . Or  $P$  est irréductible. Donc il existe  $c \in C$  tel que

$$\sum_{i=1}^n Q_i(x_i) = c \quad \text{ou} \quad \sum_{i=1}^n Q_i(x_i) = cP.$$

Si

$$\sum_{i=1}^n Q_i(x_i) = c \quad \text{alors} \quad \sum_{i=1}^n Q_i(x_i) = \sum_{i=1}^n Q_i(0) = 0,$$

et donc  $P = S \left( \sum_{i=1}^n Q_i(x_i) \right) = 0$ .

Ce qui est absurde. D'où

$$P = c \sum_{i=1}^n Q_i(x_i),$$

et  $S = cId$ , mais  $S' = 1$  donc  $S = Id$ . On a alors  $e_{\Lambda'} = e_{\Lambda''}$  et donc  $\Lambda' = \Lambda''$ .  $\square$

*Etape 2: récurrence sur la dimension de  $H$*

On fait l'hypothèse de récurrence suivante: Pour tout  $H \subset C^n$  sous  $A$  module alors

$$H = \text{Exp}(T_H)$$

$$T_H \text{ est rationnel sur } R$$

$$\dim H = \dim T_H.$$

Il est trivial que cette hypothèse est vraie pour  $n = 1$ .

Soit  $n \geq 2$  tel que l'hypothèse de récurrence soit vraie au rang  $n - 1$ . Soit  $H \subset C^n$  un sous  $A$  module.

Si  $H = C^n$  alors  $T_H = C^n$  et on a bien le résultat souhaité car  $e_\Lambda$  est surjective.

Supposons  $H \neq C^n$ . Pour appliquer l'hypothèse au rang  $n - 1$ , on utilisera le lemme suivant.

LEMME. *Il existe  $G \subset C^n$  sous  $A$  module de dimension  $\dim H + 1$  tel que*

$$H \subset G.$$

DEMONSTRATION (suggérée par le rapporteur). Comme  $H$  est un sous-groupe propre de  $C^n$ , il existe une droite de coordonnées  $D = (0, \dots, C, \dots, 0)$  qui n'est pas incluse dans  $H$ . L'action de  $A$  étant diagonale,  $D$  est un sous  $A$  module. Il est alors clair que la composante neutre de  $H + D$  vérifie les conditions du lemme.  $\square$

Revenons à la récurrence. En appliquant le lemme précédent, il existe  $G$  sous  $A$  module de  $C^n$  contenant  $H$  et de codimension 1. D'après l'étape 1,

$$G = \text{Exp}(T_G)$$

et  $T_G$  est un hyperplan de  $C^n$  rationnel sur  $R$ . Soit

$$L(x_1, \dots, x_n) = \sum_{i=1}^n \gamma_i x_i,$$

avec  $\gamma_i \in R$  une équation de  $T_G$ . Comme  $L \neq 0$ , il existe  $j$  tel que  $\gamma_j \neq 0$ . Quitte à permuter les indices, ce qui ne change pas le problème, on peut supposer que  $\gamma_n \neq 0$ .

Soit  $\Pi$  le morphisme de  $A$  modules défini par

$$\Pi: \begin{cases} G \rightarrow C^{n-1} \\ (x_1, \dots, x_n) \rightarrow (x_1, \dots, x_{n-1}). \end{cases}$$

Le noyau de  $\Pi$  est donc stable par  $A$ .

Soit  $(0, \dots, 0, x) \in \ker \Pi$ . Comme  $G = \text{Exp}(T_G)$ , il existe  $(z_1, \dots, z_n) \in T_G$  tel que

$$(0, \dots, 0, x) = \exp(z_1, \dots, z_n).$$

D'où pour tout  $1 \leq i \leq n - 1$ ,  $z_i \in \Lambda$ .

Calculons  $\gamma_n * (0, \dots, 0, x) = (0, \dots, 0, e_\Lambda(\gamma_n z_n))$ . Comme  $\gamma_i \in R$ ,  $\gamma_i \Lambda \subset \Lambda$  et

donc, pour tout  $1 \leq i \leq n - 1$ ,  $\gamma_i z_i \in \Lambda$ . Or  $(z_1, \dots, z_n) \in T_G$ , d'où

$$\gamma_n z_n = - \sum_{i=1}^{n-1} \gamma_i z_i \in \Lambda.$$

Donc  $\ker \Pi \subset \{0\} \times \dots \times \{0\} \times \ker \phi_{\gamma_n}$ . Il est fini et donc de torsion sur  $A$ . Il existe alors  $a_0 \in A - \{0\}$  tel que

$$a_0 * \ker \Pi = \{0\}.$$

Comme  $\Pi$  est un morphisme algébrique,  $\Pi(H)$  est un sous groupe algébrique de  $C^n$  (voir [B]). Il est de plus connexe et stable par  $A$ . Donc  $\Pi(H)$  est un sous  $A$  module de  $C^{n-1}$ . On peut lui appliquer l'hypothèse de récurrence,

$$\Pi(H) = \text{Exp}(T_{\Pi(H)})$$

$T_{\Pi(H)}$  est rationnel sur  $R$

$$\dim \Pi(H) = \dim T_{\Pi(H)}.$$

Comme  $\Pi$  a un noyau fini, on a  $\dim \Pi(H) = \dim H$ .

LEMME. On a un isomorphisme entre  $T_H$  et  $T_{\Pi(H)}$  donné par

$$f : \begin{cases} T_H \rightarrow T_{\Pi(H)} \\ (z_1, \dots, z_n) \rightarrow (z_1, \dots, z_{n-1}). \end{cases}$$

L'isomorphisme réciproque étant donné par

$$g : \begin{cases} T_{\Pi(H)} \rightarrow T_H \\ (z_1, \dots, z_{n-1}) \rightarrow \left( z_1, \dots, z_{n-1}, \frac{- \sum_{i=1}^{n-1} \gamma_i z_i}{\gamma_n} \right). \end{cases}$$

On en déduit donc que  $\dim H = \dim T_H$  et que  $T_H$  est rationnel sur  $R$ .

DEMONSTRATION. Si  $(z_1, \dots, z_n) \in T_H$  alors pour tout  $x \in C$

$$\exp(xz_1, \dots, xz_n) \in H.$$

Donc  $\exp(xz_1, \dots, xz_{n-1}) \in \Pi(H)$ , ce qui entraîne par définition que

$$(z_1, \dots, z_{n-1}) \in T_{\Pi(H)}.$$



L'application  $f$  est donc bien définie.

Si  $(z_1, \dots, z_{n-1}) \in T_{\Pi(H)}$  alors pour tout  $x \in C$

$$\exp(xz_1, \dots, xz_{n-1}) \in \Pi(H).$$

Posons

$$z_n = \frac{-\sum_{i=1}^{n-1} \gamma_i z_i}{\gamma_n} \quad \text{alors} \quad (z_1, \dots, z_n) \in T_G.$$

Donc il existe  $h_x \in H$  tel que

$$\exp(xz_1, \dots, xz_n) - h_x \in \ker \Pi.$$

D'où  $\exp(a_0 x z_1, \dots, a_0 x z_n) = a_0 * h_x \in H$ . Comme  $a_0 \neq 0$  on a par définition de  $T_H$

$$(z_1, \dots, z_n) \in T_H.$$

On a donc montré que  $T_H \cap T_G \simeq T_{\Pi(H)}$ . Comme  $H \subset G$ ,  $T_H \subset T_G$ . □

Appliquons  $\Pi^{-1}$  à l'équation

$$\Pi(H) = \text{Exp}(T_{\Pi(H)}).$$

Pour le membre de gauche, on a donc  $\Pi^{-1}(\Pi(H)) = H + \ker \Pi$ .

Le lemme précédent implique

$$\Pi(\text{Exp}(T_H)) = \text{Exp}(T_{\Pi(H)}).$$

D'où  $\Pi^{-1}(\text{Exp}(T_{\Pi(H)})) = \text{Exp}(T_H) + \ker \Pi$ . On en déduit donc

$$H + \ker \Pi = \text{Exp}(T_H) + \ker \Pi.$$

En multipliant par  $a_0$ , on a

$$a_0 * H = a_0 * \text{Exp}(T_H).$$

Or  $a_0 * \text{Exp}(T_H) = \text{Exp}(a_0 T_H) = \text{Exp}(T_H)$ . Comme  $H$  est stable par  $A$ ,  $a_0 H \subset H$ . De plus  $a_0 H$  est connexe comme image continue d'un connexe et de même

dimension que  $H$  car l'action de  $a_0$  a un noyau fini. D'où  $a_0H = H$  et

$$H = \text{Exp}(T_H).$$

On a donc montré l'hypothèse de récurrence au rang  $n$ . □

*Etape 3: étude de la réciproque*

Il faut maintenant étudier la réciproque. Soit  $V \subset C^n$  un sous espace vectoriel rationnel sur  $R$ . Il existe donc un système d'équations à coefficients dans  $R$

$$S: \sum_{i=1}^n \gamma_{i,j} z_i = 0, \quad 1 \leq j \leq m,$$

tel que  $V = \ker S$  et  $n - m = \dim V$ .

Soit  $H$  le sous groupe algébrique de  $C^n$  défini par les équations

$$\sum_{i=1}^n \phi_{\gamma_{i,j}}(x_i) = 0, \quad 1 \leq j \leq m.$$

Comme  $H$  est défini par  $m$  équations, on a  $\dim H \geq n - m$ . De plus  $H$  est stable par  $A$ . Donc  $H_0$ , la composante connexe de  $0$  dans  $H$ , est un sous  $A$  module de même dimension.

Soit  $(z_1, \dots, z_n) \in T_{H_0}$  alors pour tout  $x \in C$

$$\exp(xz_1, \dots, xz_n) \in H_0 \subset H.$$

Donc, pour tout  $1 \leq j \leq m$ ,

$$\sum_{i=1}^n \phi_{\gamma_{i,j}}(e_\lambda(xz_i)) = 0.$$

D'où  $e_\lambda((\sum_{i=1}^n \gamma_{i,j} z_i)x) = 0$  ce qui entraîne

$$\sum_{i=1}^n \gamma_{i,j} z_i = 0.$$

Donc  $T_{H_0} \subset V$ . Or  $\dim T_{H_0} = \dim H_0 = \dim H \geq n - m$ . On en déduit

$$V = T_{H_0}.$$

D'où  $\text{Exp}(V) = \text{Exp}(T_{H_0}) = H_0$  et donc

$$V = T_{\text{Exp}(V)}. \quad \square$$

**References**

- [A] Bosch-Gunzter-Remmert: *Non Archimedean Analysis*, Springer, 1984.
- [B] A. Borel: *Linear Algebraic Groups*, W.-A. Benjamin, 1969.
- [C] W. D. Brownawell: Some remarks on semi-resultant, Academic Press, London, 1977, pp. 205–210.
- [D] L. Denis: Théorème de Baker et modules de Drinfeld (thèse).
- [H] R. Hartshorne: *Algebraic Geometry*, Springer, 1977.
- [L] S. Lang: *Algebra*, Addison-Wesley, 1967.
- [P<sub>1</sub>] P. Philippon, Critère d'indépendance algébrique en caractéristique finie, à paraître.
- [P<sub>2</sub>] P. Philippon: Lemmes de zéros dans les groupes algébriques commutatifs, *Bull. Soc. Math. France* 114 (1986) 355–383.
- [Y<sub>1</sub>] J. Yu: Transcendence in finite characteristic, the arithmetic of function fields. Proceedings of the workshop at the Ohio State University, June 1991, W. de Gruyter.
- [Y<sub>2</sub>] J. Yu: Transcendence and Drinfeld modules, *Invent. Math.* 83 (1986) p. 507–517.