$\mathbb{F}_p$-espaces vectoriels de formes différentielles logarithmiques sur la droite projective

Guillaume Pagot

Résumé

Let k be an algebraically closed field of characteristic $p > 0$. Let $m \in \mathbb{N}$, $(m, p) = 1$. We study $\mathbb{F}_p$-vector spaces of logarithmic differential forms on the projective line such that each non zero form has a unique zero at ∞ of given order $m-1$. We discuss the existence of such vectors spaces according to the value of m. We give applications to the lifting to characteristic 0 of $(\mathbb{Z}/p\mathbb{Z})^n$ actions as k-automorphisms of $k[[t]]$.

Introduction

Soit p un nombre premier et k un corps algébriquement clos de caractéristique p. Soit m un entier premier à p, l'objet de cet article est d'étudier les $\mathbb{F}_p$-espaces vectoriels de dimension $n \geq 1$ de formes différentielles logarithmiques sur $\mathbb{P}^1_k$ (i.e. de la forme $\frac{\mathrm{d}f}{f}$ pour $f \in k(\mathbb{P}^1)$), dont les éléments non nuls ont un seul zéro d'ordre $(m-1)$ en ∞. Un tel espace vectoriel sera noté $L_{m+1,n}$. Dans cette étude, nous nous intéressons principalement au cas où n est égal à 2. Nous donnons également des résultats en ce qui concerne les espaces vectoriels de dimension supérieure.

Nous commençons par expliciter les conditions imposées aux formes différentielles, et nous donnons quelques exemples afin d'illustrer la richesse et la complexité de tels objets.

Si $L_{m+1,2}$ est un espace vectoriel comme au-dessus, un lemme élémentaire montre que $m+1 \in p\mathbb{Z}$ et donne une première idée sur la répartition des pôles des formes différentielles non nulles de $L_{m+1,2}$. Nous indiquons une généralisation pour $n \geq 2$. Comme il est classique d'exprimer à partir de l'opération de Cartier le fait qu'une forme

Math. Subj. Class. (2000) : Primary 14D15, 14E22, 14F10 ; Secondary 14L30

Mots clés : Formes différentielles logarithmiques en caractéristique $p{>}0$, action de $(\mathbb{Z}/p\mathbb{Z})^n$ sur le disque ouvert p-adique.

différentielle soit logarithmique, nous aboutissons à des conditions algébriques nécessaires et suffisantes pour l'existence d'espaces $L_{m+1,n}$, qu'il est cependant difficile d'exploiter.

Nous montrons le théorème suivant qui traite du cas particulier où $p=2$ et donne une paramétrisation de tous les espaces $L_{m+1,2}$.

Théorème 0.1 *Supposons $p=2$ et posons $m+1=2n$.*

Soit $x_1,\cdots,x_n \in k$ deux à deux distincts, et $u \neq v \in k^*$. Alors il existe $f_1(z)=\prod_{i=1}^n (z-x_i)(z-y_i)$ et $f_2(z)=\prod_{i=1}^n (z-x_i)(z-z_i)$ avec $x_1,\cdots,x_n,y_1,\cdots,y_n,z_1,\cdots,z_n$ deux à deux distincts, tels que les formes différentielles $\omega_1 := \frac{\mathrm{d}f_1}{f_1}$ et $\omega_2 := \frac{\mathrm{d}f_2}{f_2}$ soient de la forme :

$$\omega_1 = \frac{u\mathrm{d}z}{\prod_{i=1}^{n}(z-x_i)(z-y_i)} \quad \text{et} \quad \omega_2 = \frac{v\mathrm{d}z}{\prod_{i=1}^{n}(z-x_i)(z-z_i)}$$

Ainsi $\mathbb{F}_2\omega_1 + \mathbb{F}_2\omega_2$ est un $L_{m+1,2}$.

Réciproquement, tout espace $L_{m+1,2}$ est de cette forme.

Lorsque $p \neq 2$ nous décrivons les $L_{m+1,2}$ seulement pour m petit.

Théorème 0.2 *On considère le cas $p \geq 3$.*

1. *Supposons que $m+1=p$. Alors il n'existe pas d'espaces vectoriels $L_{m+1,2}$.*
2. *Supposons que $m+1=2p$. Alors il existe un espace vectoriel $L_{m+1,2}$ si et seulement si $p=3$.*
3. *Supposons que $m+1=3p$. Alors il n'existe pas d'espaces vectoriels $L_{m+1,2}$.*

La démonstration de ce théorème ne fait pas appel à l'opération de Cartier mais à une analyse algébrique des équations sur les résidus aux pôles, ce qui la rend technique. La conclusion dépend d'un lemme (lemme 2.3) d'algèbre élémentaire dont nous n'avons pas vu trace dans la littérature.

Nous donnons également des exemples de tels espaces vectoriels de dimension quelconque en suivant une construction dûe à Matignon (cf [Ma]).

Le théorème 0.2 a des applications dans le relèvement à la caractéristique 0 d'action de groupes. En effet, considérons un automorphisme σ d'ordre p du disque ouvert p-adique. On lui associe naturellement le modèle minimal semi-stable qui déploie les points fixes de σ. La fibre spéciale de ce modèle est un arbre de droites projectives et des formes différentielles logarithmiques apparaissent sur les composantes terminales de cet arbre. Lorsque l'on étudie des actions de $(\mathbb{Z}/p\mathbb{Z})^2$ sur le disque ouvert p-adique, ce sont alors des espaces vectoriels de telles formes différentielles qui peuvent apparaitre. L'application principale est le théorème suivant, qui donne de nouvelles obstructions au relèvement d'actions de groupe et justifie ainsi l'introduction des espaces $L_{m+1,n}$.

Théorème 0.3 *Soit* $\mathrm{G} = (\mathbb{Z}/p\mathbb{Z})^2$, $p \geq 3$ *et* R *un anneau de valuation discrète dominant l'anneau des vecteurs de Witt de* k. *Supposons que* G *est un groupe de* k*-automorphismes de* $k[[z]]$ *et que chacune des sous-extensions d'ordre* p *de* $k[[z]]^{\mathrm{G}}$ *a un conducteur égal à* p *(i.e* $\forall \sigma \in G - \{\mathrm{Id}\}$, $v_z(\sigma(z) - z) = p$*). Alors, on ne peut pas relever* G *en un groupe de* R*-automorphisme de* $R[[Z]]$.

Le second interêt des espaces $L_{m+1,n}$ réside dans le théorème suivant :

Théorème 0.4 *On considère un* $L_{m+1,n}$ *et une base* $\omega_1, \cdots, \omega_n$ *de cet espace, chaque* ω_i *s'écrivant* $\frac{\mathrm{d}f_i}{f_i}$. *Soit* ζ *une racine primitive* p*-ième de l'unité et* $R=W(k)[\pi]$ *où* $\pi^m := \lambda := \zeta - 1$, *on note* K*=Frac(R). Alors on peut trouver* $F_i \in R[X]$ *relevant* f_i *tels que le produit fibré des revêtements de* $\mathbb{P}^1_{\mathrm{K}}$ *donnés par les équations* $Y_i^p = F_i(X)$ *induisent après normalisation un revêtement de* $\mathbb{P}^1_{\mathrm{K}}$ *galoisien de groupe* $(\mathbb{Z}/p\mathbb{Z})^n$ *ayant bonne réduction relativement à la valuation de Gauss* $T := \pi^{-p}X$. *La fibre spéciale du modèle lisse correspondant est un revêtement étale, galoisien de groupe* $(\mathbb{Z}/p\mathbb{Z})^n$, *de la droite affine* $\mathbb{A}^1_k$.

Je souhaite remercier chaleureusement Michel Matignon pour ses précieuses indications et pour sa disponibilité tout au long de l'avancement de ce travail.

1 Présentation et approche du problème

Soit p un nombre premier, m un entier strictement positif, et k un corps algébriquement clos de caractéristique p. On fixe une fois pour toutes un point ∞ de la droite projective $\mathbb{P}^1_k$.

Définition : On note $L_{m+1,n}$ un $\mathbb{F}_p$-espace vectoriel de dimension $n \geq 1$ de formes différentielles logarithmiques sur $\mathbb{P}^1_k$, dont les éléments non nuls ont un seul zéro d'ordre $(m-1)$ en ∞.

1.1 Espaces $L_{m+1,1}$

Nous allons exhiber quelques exemples d'espaces $E_{m+1,1}$ (il est en effet légitime de s'interroger sur l'existence de tels objets avant de considérer des espaces de dimension supérieure).

Soit $\mathbb{F}_p\omega$ un espace $L_{m+1,1}$ et z un paramètre de $\mathbb{P}^1_k - \{\infty\}$ tel que $z = 0$ n'est pas pôle de ω. Ainsi

$$\omega = \frac{\mathrm{d}f}{f}$$

avec

$$f = \prod_{i=1}^{m+1} (z - x_i)^{h_i}$$

et $x_i \in k^*$, $x_i \neq x_j$, $h_i \in \mathbb{Z} - p\mathbb{Z}$, $\sum_{i=1}^{m+1} h_i = 0 \bmod p$. Le $(m+1)$-uplet $(h_i)_i$ est appelé une **donne d'Hurwitz**. Remarquons que f est définie à une multiplication près par une puissance p-ième et que $h_i \equiv \mathrm{res}_{x_i}\omega \bmod p$.

De plus, ω a un seul zéro d'ordre $m-1$ en ∞, donc $\exists u \in k^*$ tel que :

$$\omega = \sum_{i=1}^{m+1} \frac{h_i}{z - x_i}\mathrm{d}z = \frac{u}{\prod_{i=1}^{m+1}(z - x_i)}\mathrm{d}z$$

Remarquons que les conditions imposées sur ω entraînent que $m \notin p\mathbb{Z}$. En effet, supposons que $m \in p\mathbb{Z}$. Vu que $\deg(f) \in p\mathbb{Z}$, on aurait alors que $\deg(f') \equiv -1 \bmod p$, ce qui est impossible.

Si on exprime la forme ω en fonction du nouveau paramètre $x := \frac{1}{z}$ propice au développement formel, on obtient :

$$\omega = \sum_{i=1}^{m+1} \frac{-h_i x_i}{1 - x_i x}\mathrm{d}x = \frac{-u x^{m-1}}{\prod_{i=1}^{m+1}(1 - x_i x)}\mathrm{d}x.$$

Ainsi l'existence d'un $L_{m+1,1}$ est équivalente à l'existence d'une solution du système :

$$\left\{\begin{array}{ll} \sum_{i=1}^{m+1} h_i x_i^\ell = 0 & \text{pour} \quad 1 \leq \ell \leq m-1 \\ \prod_{i<j}(x_i - x_j) \neq 0 & \\ x_i \in k, \ h_i \in \mathbb{Z} - p\mathbb{Z} & \end{array}\right. \qquad (*)$$

<u>*Remarque*</u> : Si on fixe les $h_i \in \mathbb{Z} - p\mathbb{Z}$, et si on voit ce système comme un système en les inconnues x_i, alors ce système est invariant par homothétie et translation. Cette remarque est essentielle ; dans la preuve du théorème 0.2, on sera amené à plusieurs reprises à effectuer une translation "adéquate" sur les x_i.

Par la suite, nous serons amenés à regarder le cas où $m + 1 \in p\mathbb{Z}$. Examinons donc le premier cas $m + 1 = p$ $(p > 2)$. Si on fixe x_0

et x_1, alors les équations traduisent le fait que le point $(x_2, \cdots, x_m)$ appartient à une sous-variété fermée de $\mathbb{A}^{m-1}_{\mathbb{F}_p} - V(\Delta)$ de dimension 0 (avec $\Delta = \prod_{2 \leq i < j}(x_i - x_j)$, cf.[Gr-Ma 2]). Dans le cas où une telle variété est non vide on dit que les h_i sont une donnée d'Hurwitz. Dans [He] Prop 3.18, Henrio donne un critère suffisant sur les h_i pour être une donnée d'Hurwitz. Malheureusement, dans le cas $m + 1 = p$ (et plus généralement dans le cas $m+1 \in p\mathbb{Z}$), ce critère ne fournit que des $(m+1)$-uplets $(h_i)_i$ où tous les h_i sont égaux ($h_i = 1, \forall i$). Néanmoins on peut exhiber d'autres exemples de données d'Hurwitz grâce à la remarque suivante :

On écrit $p - 1 = d_1 d_2$ comme produit de deux entiers supérieurs ou égaux à deux (il convient de choisir $p > 3$ pour que cela soit possible). Supposons que l'on connaisse une donnée d'Hurwitz $(h_i)_{0 \leq i \leq d_1}$ (donnée par exemple par le critère d'Henrio). On a alors un polynôme f de la forme :

$$f = \prod_{i=0}^{d_1} (z - x_i)^{h_i}$$

et tel que $\omega := \frac{\mathrm{d}f}{f} = \frac{u\mathrm{d}z}{\prod_{i=0}^{d_1}(z-x_i)}$.

Après translation éventuelle, on peut supposer que $x_0 = 0$ et donc :

$$\omega = \frac{u\mathrm{d}z}{zP(z)} \quad \text{avec} \quad P(z) := \prod_{i=1}^{d_1}(z - x_i)$$

L'idée est alors de faire un changement de variables $z := Q(t)$ tel que $Q'(t)$ divise $f(Q(t))$. Nous allons donner deux exemples de tels changement de variables et préciser dans chaque cas les données d'Hurwitz obtenues.

Exemple 1 : Prenons le changement de variables $z := t^{d_2}$. On obtient alors la forme différentielle logarithmique :

$$\frac{d_2 u\mathrm{d}t}{tP(t^{d_2})}$$

La détermination des données d'Hurwitz correspondantes est fournie par le calcul des résidus de cette forme différentielle. On trouve alors le p-uplet :

$$d_2 h_0, \underbrace{h_1 \cdots h_1}_{d_2 \text{ fois}}, \cdots, \underbrace{h_{d_1} \cdots h_{d_1}}_{d_2 \text{ fois}}$$

Exemple 2 : Posons cette fois-ci $z = Q(t) = t^{d_2 - 1}(t - \alpha)$, où α est choisi tel que $(t - \frac{d_2-1}{d_2}\alpha)$ divise $z - x_1$ (i.e $Q'(t)$ divise $f(Q(t))$). Soit $P_1(z)$

et $P_\alpha(t)$ tels que $P(z) = (z - x_1)P_1(z)$ et $z - x_1 = P_\alpha(t)(t - \frac{d_2-1}{d_2}\alpha)^2$. On obtient alors la forme suivante :

$$\omega = \frac{d_2 u \mathrm{d}t}{t(t-\alpha)P_\alpha(t)(t-\frac{d_2-1}{d_2}\alpha)P_1(t^{d_2-1}(t-\alpha))}$$

Cette fois-ci, la donnée d'Hurwitz prend la forme :

$$h_0, (d_2-1)h_0, \underbrace{h_1 \cdots h_1}_{d_2-2 \text{ fois}}, 2h_1, \underbrace{h_2 \cdots h_2}_{d_2 \text{ fois}}, \cdots, \underbrace{h_{d_1} \cdots h_{d_1}}_{d_2 \text{ fois}}$$

Ces quelques exemples montrent qu'il existe des formes différentielles ayant les propriétés susdécrites. En fait, des calculs menés sur ordinateur (pour de petites valeurs de p) montrent que beaucoup de p-uplets sont des données d'Hurwitz. La question de déterminer quels sont les p-uplets (h_i) convenables est déjà en soi un problème intéressant et difficile.

Remarque : Dans ce qui précède, on a utilisé soit le paramètre z, soit le paramètre $x = \frac{1}{z}$. En fait, chacune de ces deux écritures a son interêt propre. La première est agréable à manipuler quand il s'agit de faire un développement formel et d'exprimer les équations en les x_i. La seconde est plus appropriée pour des changements de variables, voire des calculs de résidus. Par la suite, il nous arrivera de privilégier l'une des deux écritures selon les besoins.

1.2 Conditions combinatoires pour les $L_{m+1,n}$ $(n \geq 2)$

En ce qui concerne les espaces $L_{m+1,2}$, on a un lemme combinatoire qui précise l'arrangement des pôles des formes différentielles non nulles :

Lemme 1.1 *Soit un espace vectoriel $L_{m+1,2}$; alors $m+1 \in p\mathbb{Z}$. De plus si on note (ω_1, ω_2) une base de cet espace, alors ces deux formes différentielles ont exactement $\frac{p-1}{p}(m+1)$ pôles en commun.*

Démonstration : Soit (ω_1, ω_2) une base de l'espace vectoriel en question. On note $(m+1-\lambda)$ le nombre de pôles communs à ω_1 et ω_2 (on a donc $0 \leq \lambda \leq m+1$). On note $x_0, \cdots, x_m$ les pôles de ω_1, et $h_0, \cdots, h_m$ les résidus en ces pôles. De même pour ω_2, on les note $x_\lambda, \cdots, x_{\lambda+m}$ et $h'_\lambda, \cdots, h'_{\lambda+m}$ les résidus correspondants (on convient de poser $h_i = 0$ pour $i > m$ et $h'_i = 0$ pour $i < \lambda$).

Soit $c \in \mathbb{P}^1(\mathbb{F}_p)$, $c = [a, b]$ (en coordonnées homogènes) ; alors $\omega := a\omega_1 + b\omega_2$ a exactement $m+1$ pôles. Donc, il existe exactement λ valeurs de i pour lesquelles $ah_i+bh'_i=0$. On a alors partitionné les $(m+1+\lambda)$ points x_i en $p+1$ ensembles de λ points. Ainsi $(m+1+\lambda)=(p+1)\lambda$ et $m+1=\lambda p$. On vérifie aisément que le nombre de pôles communs à ω_1 et ω_2 est celui annoncé.

$\square$

On peut montrer une généralisation dans le cas des espaces vectoriels $L_{m+1,n}$:

Lemme 1.2 *On conserve les notations précédentes. Considèrons un espace vectoriel $L_{m+1,n}$ ($n\geq 2$), alors $m+1\in p^{n-1}\mathbb{Z}$. De plus, si $(\omega_1,\cdots,\omega_n)$ est une base, alors ces n formes différentielles ont exactement $\frac{(p-1)^{n-1}}{p^{n-1}}(m+1)$ pôles en commun.*

<u>*Démonstration*</u> : La démonstration se fait par récurrence sur n. On prend donc un $\mathbb{F}_p$-espace vectoriel $L_{m+1,n}$ engendré par n formes différentielles linéairement indépendantes $(\omega_1,\cdots,\omega_n)$. L'hypothèse de récurrence aux rangs inférieurs dit que pour j formes differentielles ($j<n$) parmi les ω_i, ces j formes ont exactement $\frac{(p-1)^{j-1}}{p^{j-1}}(m+1)$ pôles en commun. Notons T le nombre total des pôles apparaissant dans les formes différentielles $\omega_1,\cdots,\omega_n$ et λ le nombre de pôles communs à toutes ces différentielles. On note également $N_{i_1i_2\cdots i_k}$ le nombre de pôles communs aux formes différentielles $\omega_{i_1},\cdots,\omega_{i_k}$.Alors, on a la relation :

$$\begin{aligned}
T &= \sum_{k=1}^{n}(-1)^{k+1}\sum_{i_1<i_2<\cdots<i_k}N_{i_1i_2\cdots i_k}\\
&= (m+1)\sum_{k=1}^{n-1}(-1)^{k+1}C_n^k\left(\frac{p-1}{p}\right)^{k-1}+(-1)^{n+1}\lambda\\
&= (m+1)\left(\frac{p}{p-1}\right)\sum_{k=1}^{n-1}(-1)^{k+1}C_n^k\left(\frac{p-1}{p}\right)^{k}+(-1)^{n+1}\lambda
\end{aligned}$$

$$\begin{aligned}
&= -(m+1)\left(\frac{p}{p-1}\right)\left(\left(1-\frac{p-1}{p}\right)^n-1-(-1)^n\left(\frac{p-1}{p}\right)^n\right)\\
&\quad +(-1)^{n+1}\lambda\\
&= (m+1)\left(\frac{p}{p-1}\right)\left(1+(-1)^n\left(\frac{p-1}{p}\right)^n-\left(\frac{1}{p}\right)^n\right)+(-1)^{n+1}\lambda
\end{aligned}$$

On note $x_1,\cdots,x_T$ les pôles et $h_{j,i}$ le résidu (éventuellement nul) de la forme différentielle ω_j au point x_i. Soit $[a_1,\cdots,a_n]\in\mathbb{P}^{n-1}(\mathbb{F}_p)$, alors on a :

$$a_1h_{1,i}+\cdots+a_nh_{n,i}=0$$

pour exactement $(T-(m+1))$ valeurs de i. D'autre part, si on considère un point x_i, il est pôle de toutes les formes différentielles sauf celles de la forme $a_1\omega_1 + \cdots + a_n\omega_n$, avec $a_1 h_{1,i} + \cdots + a_n h_{n,i} = 0$ (ce qui fait pour chaque i un total de $(p^{n-2} + p^{n-3} + \cdots + 1)$ formes différentielles modulo la multiplication par un élément de $\mathbb{F}_p^*$). En résumé, l'ensemble des pôles $x_1, \cdots, x_T$ est la réunion de $(p^{n-1} + p^{n-2} + \cdots + 1)$ ensembles de $(T-(m+1))$ éléments, chaque élément étant inclus dans exactement $(p^{n-2} + p^{n-3} + \cdots + 1)$ de ces ensembles. On a donc la relation :

$$T(p^{n-2} + p^{n-3} + \cdots + 1) = (T - (m+1))(p^{n-1} + p^{n-2} + \cdots + 1)$$

et donc :

$$T = \frac{(m+1)(p^n - 1)}{(p-1)p^{n-1}}$$

En comparant avec l'expression de T déjà calculée précédemment, il vient :

$$\begin{aligned} \frac{(m+1)p}{p-1}\left[\frac{p^n-1}{p^n} - \left(1 + (-1)^n\left(\frac{p-1}{p}\right)^n - \left(\frac{1}{p}\right)^n\right)\right] - (-1)^{n+1}\lambda &= 0 \\ \frac{(m+1)p}{p-1}\left[(-1)^{n+1}\left(\frac{p-1}{p}\right)^n\right] - (-1)^{n+1}\lambda &= 0 \\ \frac{(m+1)(p-1)^{n-1}}{p^{n-1}} - \lambda &= 0 \end{aligned}$$

Finalement $m+1 \in p^{n-1}\mathbb{Z}$ et $\lambda = \frac{(p-1)^{n-1}}{p^{n-1}}(m+1)$.

□

1.3 Conditions algébriques sur $L_{m+1,n}$

Soit z un paramètre de $\mathbb{P}^1_k - \{\infty\}$. Nous allons montrer la proposition suivante :

Proposition 1.3 *Soit ω_1, ω_2 deux formes différentielles sur $\mathbb{P}^1_k$. Alors $\mathbb{F}_p\omega_1 + \mathbb{F}_p\omega_2$ est un $L_{m+1,2}$ si et seulement si il existe deux polynômes A et B avec*

$$\deg(iA + jB) = \frac{m+1}{p}, \qquad \forall [i,j] \in \mathbb{P}^1(\mathbb{F}_p),$$

tels que :

$$\omega_1 = \frac{A\mathrm{d}z}{A^pB - AB^p} \quad \text{et} \quad \omega_2 = \frac{B\mathrm{d}z}{A^pB - AB^p}$$

et $((A^p - AB^{p-1})^{p-1})^{(p-1)} = -1$.

Démonstration : Supposons que $\mathbb{F}_p\omega_1 + \mathbb{F}_p\omega_2$ est un $L_{m+1,2}$. On sait d'après le lemme 1.1 que $m+1 = \lambda p$ et que l'ensemble des pôles est partitionné en $p+1$ ensembles de λ pôles. Plus précisément, on écrit que :

- ω_1 a ses pôles en les points $x_0, \cdots, x_{\lambda p-1}$
- ω_2 a ses pôles en les points $x_\lambda, \cdots, x_{\lambda(p+1)-1}$
- quitte à renuméroter, on peut supposer que $\omega_1 + i\omega_2$ (pour i variant de 1 à $p-1$) a des pôles en tous les x_j sauf pour $\lambda i \leq j \leq \lambda(i+1)-1$.

On note $P_j(z) = \prod_{k=\lambda j}^{\lambda(j+1)-1}(z - x_k)$. Alors ω_1 et ω_2 s'écrivent :

$$\omega_1 = \frac{uP_0(z)\mathrm{d}z}{\prod_{j=0}^{p} P_j(z)}\ ,\ \ \omega_2 = \frac{vP_p(z)\mathrm{d}z}{\prod_{j=0}^{p} P_j(z)}$$

où u et v sont des constantes non nulles.
On a alors deux écritures pour $\omega_1 + i\omega_2$:

$$\omega_1 + i\omega_2 = \frac{(uP_0(z) + ivP_p(z))\mathrm{d}z}{\prod_{j=0}^{p} P_j(x)} = \frac{(w_iP_i(z))\mathrm{d}z}{\prod_{j=0}^{p} P_j(z)}$$

où w_i est une constante non nulle.
On a donc $uP_0(z) + ivP_p(z) = w_iP_i(z)$. En identifiant les termes dominants de chaque expression, on trouve $w_i = u + iv$ et donc $uP_0(z) + ivP_p(z) = (u + iv)P_i(z)$.

Le rapport $\frac{u}{v}$ n'est pas dans $\mathbb{F}_p$. En effet, si $\frac{u}{v} = -i \in \mathbb{F}_p$, alors $(u + iv)P_i = 0 = u(P_0 - P_p)$ et donc $P_0 = P_p$, ce qui implique que les x_j ne sont pas distincts.

Posons $a = \frac{u}{v}$. Alors :

$$\omega_2 = v\prod_{j=0}^{p-1}\frac{(a+j)}{(aP_0 + jP_p)}\mathrm{d}z = \frac{v(a^p - a)}{(aP_0)^p - aP_0P_p^{p-1}}\mathrm{d}z$$

et

$$\omega_1 = a\omega_2\frac{P_0}{P_p} = \frac{v(a^p - a)}{(aP_0)^{p-1}P_p - P_p^p}\mathrm{d}z.$$

Soit $\alpha \in k$ tel que $\alpha^p v(a^p - a) = 1$ et posons $A := \alpha a P_0$, $B := \alpha P_p$. Vu que $a \notin \mathbb{F}_p$, on a :

$$\deg(iA + jB) = \frac{m+1}{p}, \qquad \forall [i,j] \in \mathbb{P}^1(\mathbb{F}_p),$$

Il reste maintenant à exprimer le fait que les formes différentielles :

$$\frac{A\mathrm{d}z}{A^pB - AB^p} \quad \text{et} \quad \frac{B\mathrm{d}z}{A^pB - AB^p}$$

sont logarithmiques. Pour exprimer cette condition, on peut exprimer la relation $\mathcal{C}\omega_i = \omega_i$, où la lettre $\mathcal{C}$ désigne l'opération de Cartier. Rappelons de quoi il s'agit ; si on considère une forme différentielle ω, alors on peut l'écrire :

$$\omega = (f_0^p(z) + zf_1^p(z) + \cdots + z^{p-1}f_{p-1}^p(z))\mathrm{d}z$$

On définit $\mathcal{C}\omega = f_{p-1}\mathrm{d}z$. Une condition nécessaire et suffisante pour que ω soit logarithmique est que $\mathcal{C}\omega = \omega$ (dans le cas de formes différentielles sur $\mathbb{P}^1$, la preuve est élémentaire). Remarquons que cette condition de Cartier peut également s'exprimer de la façon suivante : si on a $\omega = f\mathrm{d}z$ alors ω est logarithmique si et seulement si :

$$f^{(p-1)} = -f^p$$

A l'aide de cette opération, on va montrer que les hypothèses "ω_1 est logarithmique" et "ω_2 est logarithmique" sont équivalentes.

Supposons en effet que $\frac{B\mathrm{d}z}{A^pB-AB^p}$ est logarithmique. En écrivant que :

$$\frac{B\mathrm{d}z}{A^pB - AB^p} = \frac{B(A^pB - AB^p)^{p-1}\mathrm{d}z}{(A^pB - AB^p)^p}$$

on voit que la condition donnée par l'opération de Cartier s'exprime par l'égalité :

$$(B(A^pB - AB^p)^{p-1})^{(p-1)} = -B^p$$

A partir de cette expression, on en tire :

$$\begin{array}{rcl}
(A^pB(A^pB - AB^p)^{p-1})^{(p-1)} & = & -A^pB^p \\
(((A^pB - AB^p) + AB^p)(A^pB - AB^p)^{p-1})^{(p-1)} & = & -A^pB^p \\
(AB^p(A^pB - AB^p)^{p-1} + (A^pB - AB^p)^p))^{(p-1)} & = & -A^pB^p \\
(AB^p(A^pB - AB^p)^{p-1})^{(p-1)} & = & -A^pB^p \\
(A(A^pB - AB^p)^{p-1})^{(p-1)} & = & -A^p
\end{array}$$

et la dernière égalité entraîne que $\frac{A\mathrm{d}z}{A^pB-AB^p}$ est logarithmique.

On peut donc résumer ces conditions en disant que :

$$((A^p - AB^{p-1})^{p-1})^{(p-1)} = -1 \qquad (**)$$

Inversement si on a :

$$\omega_1 = \frac{A\mathrm{d}z}{A^pB - AB^p} \quad \text{et} \quad \omega_2 = \frac{B\mathrm{d}z}{A^pB - AB^p}$$

avec A,B vérifiant les conditions de la proposition, on montre facilement que les formes $i\omega_1 + j\omega_2$ (pour $(i, j) \neq 0$) sont logarithmiques et n'ont qu'un seul zéro d'ordre $(m - 1)$ en ∞.

$\square$

Remarque 1 : L'équation différentielle (**) est difficile à manipuler. En effet, si on la développe, il apparait des dérivées k-ièmes de puissances de A, A étant lui-même de degré λ (la résolution n'apparait simple que dans le cas où $\lambda = 1$ ou $p = 2$).

On peut donner une autre formulation de la condition (**) en termes de congruence : puisque $f := A^p - AB^{p-1} \in k[z]$, ω_1 est logarithmique si et seulement si $(f')^{p-1} = 1$ modulo f.

Remarque 2 : On a une formulation similaire du problème pour les $L_{m+1,n}$ $(n \geq 3)$. Pour cela, on reprend les notations du lemme 1.2. On note P un polynôme qui n'a que des racines simples qui sont les pôles des formes différentielles ω_i. Alors chaque forme ω_i peut s'écrire $\omega_i = \frac{Q_i}{P}\mathrm{d}z$ où Q_i est un polynôme avec pour seules racines simples les points x_i où ω_i n'a pas de pôles. Pour chaque valeur $[a_1, \cdots, a_n] \in \mathbb{P}^{n-1}(\mathbb{F}_p)$, le polynôme $a_1Q_1 + \cdots + a_nQ_n$ a exactement $(T - (m+1))$ racines simples (toujours parmi les pôles des formes différentielles), et chaque point x_i est racines d'exactement $(p^{n-2} + p^{n-3} + \cdots + 1)$ de ces polynômes. On a donc la relation :

$$P^{(p^{n-2}+p^{n-3}+\cdots+1)} = \gamma \prod_{i=1}^{n} \prod_{j_{i-1}=0}^{p-1} \cdots \prod_{j_1=0}^{p-1} (Q_i + j_{i-1}Q_{i-1} + \cdots + j_1Q_1)$$

où γ est une constante.
Quitte à multiplier P par une constante, on peut supposer $\gamma = 1$. La condition sur les ω_i pour être logarithmique s'exprime en disant que les formes :

$$\frac{P^{p(p^{n-3}+p^{n-4}+\cdots+1)}Q_i}{\prod_{i=1}^{n} \prod_{j_{i-1}=0}^{p-1} \cdots \prod_{j_1=0}^{p-1}(Q_i + j_{i-1}Q_{i-1} + \cdots + j_1Q_1)}$$

sont logarithmiques. On reconnait au dénominateur le déterminant de Moore des polynômes $Q_1 \cdots Q_n$ (cf. [Go]), ce qui généralise la forme que l'on avait pour $n = 2$; en effet, $A^pB - AB^p$ est le déterminant de Moore de A et B.

Remarque 3 : On a vu précédemment que lorsqu'on disposait d'un $L_{m+1,2}$ engendré par deux formes ω_1 et ω_2, les coefficients u et v "associés" étaient linéairement indépendants sur $\mathbb{F}_p$. On peut généraliser ce résultat aux espaces $L_{m+1,n}$: soit un espace $L_{m+1,n}$ engendré par les formes différentielles $\omega_1, \cdots, \omega_n$. Comme on l'a vu juste au-dessus on peut écrire $\omega_i = \frac{Q_i}{P}\mathrm{d}z$; on choisit de prendre P unitaire et on note u_i le

terme de plus haut degré de Q_i. Montrons que les u_i sont linéairement indépendants sur $\mathbb{F}_p$.
Soit $a := (a_1, \cdots, a_n) \in \mathbb{F}_p^n - \{0\}$; définissons $\omega_a := a_1\omega_1 + \cdots + a_n\omega_n$.
Alors :

$$\omega_a = \frac{a_1Q_1 + \cdots + a_nQ_n}{P}\mathrm{d}z := \frac{Q_a}{P}\mathrm{d}z$$

La forme ω_a doit avoir le même nombre de pôles que les ω_i, donc le polynôme Q_a a le même degré que les Q_i. En particulier le coefficient de plus haut degré de Q_a est non nul. Donc $a_1u_1 + \cdots + a_nu_n \neq 0$.

Remarque 4 : Soit $\Phi : \mathbb{P}_k^1 \longrightarrow \mathbb{P}_k^1$ donnée par $\Phi(t) = \alpha t + P(t^p)$ avec $\alpha \in k^*$ et $P \in k[t]$ (i.e Φ est un revêtement étale de $\mathbb{P}_k^1 - \{\infty\}$). Si F est un $L_{m+1,n}$ engendré par les formes différentielles $\omega_1, \cdots, \omega_n$ (avec $\omega_i = \frac{\mathrm{d}f_i}{f_i}$) alors Φ^*F est un $L_{(m+1)\deg\Phi,n}$ (où Φ^*F désigne le $\mathbb{F}_p$-espace vectoriel engendré par les formes $\frac{\mathrm{d}(f_i\circ\Phi)}{f_i\circ\Phi}$).

2 Résultats et applications

A défaut de pouvoir exploiter la condition (**) décrite ci-dessus, nous allons explorer les relations algébriques entre pôles et résidus.

2.1 Un cas particulier : $p = 2$

Le cas $p = 2$ apparaît comme un cas particulier dans la mesure où toutes les données d'Hurwitz sont égales à 1.

Théorème 2.1 *Supposons $p = 2$ et posons $m + 1 = 2n$.*

Soit $x_1, \cdots, x_n \in k$ deux à deux distincts, et $u \neq v \in k^*$. Alors il existe $f_1(z) = \prod_{i=1}^n(z - x_i)(z - y_i)$ et $f_2(z) = \prod_{i=1}^n(z - x_i)(z - z_i)$ avec $x_1, \cdots, x_n, y_1, \cdots, y_n, z_1, \cdots, z_n$ deux à deux distincts, tels que les formes différentielles $\omega_1 := \frac{\mathrm{d}f_1}{f_1}$ et $\omega_2 := \frac{\mathrm{d}f_2}{f_2}$ soient de la forme :

$$\omega_1 = \frac{u\mathrm{d}z}{\prod_{i=1}^{n}(z - x_i)(z - y_i)} \quad \text{et} \quad \omega_2 = \frac{v\mathrm{d}z}{\prod_{i=1}^{n}(z - x_i)(z - z_i)}$$

Ainsi $\mathbb{F}_2\omega_1 + \mathbb{F}_2\omega_2$ est un $L_{m+1,2}$.

Réciproquement, tout espace $L_{m+1,n}$ est de cette forme.

Démonstration : Vue la forme demandée pour ω_1, il faut que $f_1' = u$ et donc que f_1 soit de la forme :

$$f_1 = (q(z))^2 + uz$$

où $q = z^n + q_1 z^{n-1} + \cdots + q_n$ est un polynôme de degré n à coefficients dans k. De même, on a $f_2 = (r(z))^2 + vz$ où $r = z^n + r_1 z^{n-1} + \cdots + r_n$ est un polynôme du même type. Déterminons donc les polynômes q et r.

Remarquons que $f_1(x_i) = (q(x_i))^2 + ux_i = 0$ ce qui donne le système :

$$\left\{ \begin{array}{rcl} x_1^n + q_1 x_1^{n-1} + \cdots + q_n & = & \sqrt{ux_1} \\ \vdots & & \\ \vdots & & \\ x_n^n + q_1 x_n^{n-1} + \cdots + q_n & = & \sqrt{ux_n} \end{array} \right.$$

Vu que les x_i sont distincts, ceci est un système de type Vandermonde, ce qui donne une solution pour les $q_1, \cdots, q_n$ (et donc pour les $y_1, \cdots, y_n$). De plus, puisque $f_1'(z) = u$, f_1 n'a que des racines simples (donc les $x_1, \cdots, x_n, y_1, \cdots, y_n$ sont deux à deux distincts).

On obtient de façon identique que les coefficients du polynôme r sont obtenus par résolution d'un système de Vandermonde. Ceci fournit les points z_i (et de même on a que les $x_1, \cdots, x_n, z_1, \cdots, z_n$ sont deux à deux distincts). Il reste à vérifier que les $y_1, \cdots, y_n, z_1, \cdots, z_n$ sont distincts deux à deux.

Soit α une racine commune à f_1 et f_2. Alors :

$$(q(\alpha))^2 + u\alpha^{2n-1} = (r(\alpha))^2 + v\alpha^{2n-1} = 0$$

Donc $(vq^2 + ur^2)(\alpha) = 0 = (\sqrt{v}q + \sqrt{u}r)^2(\alpha)$. Or le polynôme $(\sqrt{v}q + \sqrt{u}r)$ est de degré n et a donc au plus n racines (qui sont en fait les x_i). Finalement les points $x_1, \cdots, x_n, y_1, \cdots, y_n, z_1, \cdots, z_n$ sont distincts deux à deux.

$\square$

2.2 Démonstration du résultat principal

Théorème 2.2 *On considère le cas $p \geq 3$.*

1. *Supposons que $m+1 = p$. Alors il n'existe pas d'espaces vectoriels $L_{m+1,2}$.*
2. *Supposons que $m+1 = 2p$. Alors il existe un espace vectoriel $L_{m+1,2}$ si et seulement si $p = 3$.*
3. *Supposons que $m+1 = 3p$. Alors il n'existe pas d'espaces vectoriels $L_{m+1,2}$.*

Démonstration : Dans les trois cas, la démonstration se fait par l'absurde et on considèrera donc à chaque fois un espace vectoriel répondant au problème. Soit z un paramètre de $\mathbb{P}_k^1 - \{\infty\}$ tel que $z = 0$

n'est pas pôle de ω_1 et ω_2. On utilise alors dans la démonstration le paramètre $x := \frac{1}{z}$.

Le cas $m+1=p$.

On note toujours (ω_1, ω_2) une base d'un espace vectoriel $L_{m+1,2}$. Ces deux formes s'écrivent :

$$\omega_1 = \frac{\mathrm{d}f_1}{f_1} = \sum_{i=0}^{p} \frac{h'_i x_i}{1-x_i x}\mathrm{d}x, \quad h'_0 = 0,\ h'_i \neq 0 \text{ si } i \neq 0,\ \sum_i h'_i \equiv 0 \bmod p$$

$$\omega_2 = \frac{\mathrm{d}f_2}{f_2} = \sum_{i=0}^{p} \frac{h_i x_i}{1-x_i x}\mathrm{d}x, \quad h_p = 0,\ h_i \neq 0 \text{ si } i \neq p,\ \sum_i h_i \equiv 0 \bmod p$$

et tous les x_i sont distincts.

La forme ω_1 s'écrit aussi :

$$\omega_1 = \frac{u x^{p-2}}{\prod_{i=1}^{p}(1-x_i x)}\mathrm{d}x \quad \text{avec } u \neq 0$$

En identifiant les termes en x^k des développements formels des deux expressions de ω_1, on trouve que :

$$\sum_{i=1}^{p} h'_i x_i^k = 0 \quad \text{si } k \leq p-2 \quad \text{et} \sum_{i=1}^{p} h'_i x_i^p = u \sum_{i=1}^{p} x_i$$

Or $\sum_{i=1}^{p} h'_i x_i^p = \sum_{i=1}^{p} (h'_i x_i)^p$ et vu que $u \neq 0$, il suit que $\sum_{i=1}^{p} x_i = 0$. En appliquant le même raisonnement à ω_2, il vient que $\sum_{i=0}^{p-1} x_i = 0$. Ainsi $x_0 = x_p$, ce qui fournit la contradiction attendue.

Supposons maintenant que $m+1=2p$.

D'après le lemme 1.1 on a $2p+2$ pôles que l'on peut partitionner en $p+1$ couples. On les note $x_0, y_0, \cdots, x_p, y_p$. Alors, après renumérotation éventuelle, on a que :

- $\omega_1 + i\omega_2$ a des pôles en tous les points sauf en x_i et y_i (i varie de 0 à $p-1$).
- ω_p a des pôles en tous les points sauf en x_p et y_p.

On peut écrire :

$$\omega_1 = \sum_{i=0}^{p} \left(\frac{h'_i x_i}{1-x_i x} + \frac{k'_i y_i}{1-y_i x} \right) \mathrm{d}x \quad \text{avec } h'_0 = k'_0 = 0$$

$$\omega_2 = \sum_{i=0}^{p} \left(\frac{h_i x_i}{1-x_i x} + \frac{k_i y_i}{1-y_i x} \right) \mathrm{d}x \quad \text{avec } h_p = k_p = 0$$

Etape 1 : Montrons que $x_i + y_i$ est une constante indépendante de i.

On pose $s_i = x_i + y_i$ et $p_i = x_i y_i$. Alors $P_i(z) = z^2 - s_i z + p_i$; on a donc, d'après le paragraphe 1.3, les relations suivantes :

$$s_i = \frac{as_0 + is_p}{a+i} \quad \text{et} \quad p_i = \frac{ap_0 + ip_p}{a+i}$$

et $a \notin \mathbb{F}_p$.
Le même argument que dans le cas $m+1=p$ montre que :

$$\sum_{i=1}^{p}(x_i + y_i) = 0 \text{ et } \sum_{i=0}^{p-1}(x_i + y_i) = 0$$

On en déduit donc que $s_0 = s_p$, puis finalement que $s_i = \text{cste}$, au vu de la relation $(a+i)s_i = as_0 + is_p$. ⌟

On posera $s_i = s$ dans la suite et $A_i(k) = h_i x_i^k + k_i y_i^k$ pour $k \geq 0$.

Etape 2 :Montrons par récurrence sur l que :

$$\sum_{i=0}^{p-1} p_i^l A_i(k) = 0 \quad 0 \leq k \leq 2p-2-2l$$

- $l = 0$: La relation annoncée est vraie, car la condition imposant à ω_2 d'avoir un zéro d'ordre $(2p-2)$ en zéro est :

$$\sum_{i=0}^{p-1} A_i(k) = 0, \quad 0 \leq k \leq 2p-2$$

- Supposons le résultat vrai au rang l. On part de l'égalité :

$$\sum_{i=0}^{p-1} p_i^l (A_i(k+2) - sA_i(k+1) + p_i A_i(k)) = 0 \quad \forall k \geq 0.$$

  Alors pour $2 \leq k+2 \leq 2p-2-2l$ (i.e $0 \leq k \leq 2p-2-2(l+1)$), on a

$$\sum_{i=0}^{p-1} p_i^l A_i(k+2) = 0$$

  et

$$\sum_{i=0}^{p-1} sp_i^l A_i(k+1) = 0$$

  Donc :

$$\sum_{i=0}^{p-1} p_i^{l+1} A_i(k) = 0 \quad \forall k \leq 2p-2-2(l+1)$$

$\lrcorner$

On aboutit donc à :

$$\sum_{i=0}^{p-1} p_i^l A_i(0) = 0 \quad \text{pour} \quad 1 \leq l \leq p-1 \tag{1}$$

$$\sum_{i=0}^{p-1} p_i^l A_i(1) = 0 \quad \text{pour} \quad 1 \leq l \leq p-2 \tag{2}$$

Etape 3 : Montrons que $A_i(0) = 0$ et qu'il existe β dans k^* tel que $A_i(1) = \beta(a+i)^{p-2}$ pour $0 \leq i \leq p-1$.

On sait que $p_i = p_p + \frac{a(p_0 - p_p)}{a+i} = b + \frac{c}{a+i}$ en posant $b = p_p$ et $c = a(p_0 - p_p) \neq 0$. Le système (1) implique en particulier que :

$$\sum_{i=0}^{p-1} \frac{A_i(0)}{(a+i)^l} = 0 \ \text{ pour } \ 1 \leq l \leq p-1$$

Posons $F(X) = \sum_{i=0}^{p-1} \frac{A_i(0)}{X+i}$. Alors a est une racine de F d'ordre au moins égal à $(p-1)$. Puisque $\sum_{i=0}^{p-1} A_i(0) = 0$, le numérateur de F est de degré au plus $(p-2)$, on en déduit que F est nul et donc que $A_i(0) = 0$ pour $0 \leq i \leq p-1$.

De même le système (2) implique que :

$$\sum_{i=0}^{p-1} \frac{A_i(1)}{(a+i)^l} = 0 \ \text{ pour } \ 1 \leq l \leq p-2$$

Posons $G(X) = \sum_{i=0}^{p-1} \frac{A_i(1)}{(X+i)}$. Alors a est une racine de G d'ordre au moins égale à $(p-2)$. Le numérateur de G étant de degré au plus $(p-2)$, on a que G est de la forme :

$$G(X) = \sum_{i=0}^{p-1} \frac{A_i(1)}{(X+i)} = \frac{\beta(X-a)^{p-2}}{X^p - X}$$

où β est une constante non nulle (en effet, $\beta = 0$ impliquerait que $A_i(1) = 0$ et, puisque $A_i(0) = 0$, on aurait $h_i = k_i = 0$). Après identification des coefficients dans cette décomposition en éléments simples, on aboutit à :

$$A_i(1) = \beta(a+i)^{p-2}$$

$\lrcorner$

En résumé, on a :

- $A_i(0) = 0$ donc $k_i = -h_i$.
- $A_i(1) = 2h_i x_i = \beta(i+a)^{p-2}$
- $s_i = 0$, après translation éventuelle sur les x_i, y_i (on voit en effet que les deux relations précédentes restent inchangées après translation). En particulier $x_i \neq 0$.

On a donc un système :

$$\left\{ \begin{array}{rcl} h_i x_i & = & \frac{\beta}{2}(i+a)^{p-2} \\ -x_i^2 & = & b + \frac{c}{a+i} \end{array} \right. \quad x_i \in k,\ 0 \leq i \leq p-1$$

Remarquons que ce système traduit à lui seul les conditions imposées par le problème considéré. On calcule :

$$\frac{h_i^2 x_i^2}{x_i^2} = -\frac{(\frac{\beta}{2})^2 (i+a)^{2(p-2)}}{b + \frac{c}{a+i}} = -\frac{(\frac{\beta}{2})^2 (i+a)^{2p-3}}{b(a+i)+c} = h_i^2$$

donc,

$$1 = (-1)^{\frac{p-1}{2}} \frac{(\frac{\beta}{2})^{p-1} (i+a)^{(2p-3)\frac{p-1}{2}}}{(b(a+i)+c)^{\frac{p-1}{2}}} \quad 0 \leq i \leq p-1$$

Ainsi si $H(X) := (\frac{\beta}{2})^{p-1}(X+a)^{(2p-3)(\frac{p-1}{2})} - (-1)^{\frac{p-1}{2}}(b(X+a)+c)^{\frac{p-1}{2}}$, $H(X) = 0 \bmod X^p - X$. En particulier le coefficient de X^{p-1} dans $H(X)$ modulo $X^p - X$ est nul. Or on a le :

Lemme 2.3 *Soit n un entier supérieur ou égal à 2 et p un nombre premier congru à 1 modulo n. Alors le coefficient de X^{p-1} dans $(X+a)^{(np-(n+1))(\frac{p-1}{n})}$ mod $X^p - X$ est :*

$$C_q^2 (a - a^p)^{q-2}$$

avec $q := \frac{(n-1)p+(n+1)}{n}$.

<u>*Démonstration*</u> : Remarquons tout d'abord que :

$$(np - (n+1))(\frac{p-1}{n}) = p(p-3) + \frac{(n-1)p+n+1}{n} = p(p-3) + q$$

On a donc :

$$\begin{array}{rcl} (X+a)^{(np-(n+1))(\frac{p-1}{n})} & = & (X^p + a^p)^{p-3}(X+a)^q \\ & = & (X + a^p)^{p-3}(X+a)^q \mod (X^p - X). \end{array}$$

Supposons que $p-1>n$, dans ce cas $q<p$. Notons T le coefficient de X^{p-1} dans l' expression $(X+a^p)^{p-3}(X+a)^q$, alors :

$$\begin{aligned}
T &= \sum_{j=2}^{q} C_q^j C_{p-3}^{p-1-j} a^{(q-j)} (a^p)^{(p-3-(p-1-j))} \\
&= \sum_{j=2}^{q} C_q^j C_{p-3}^{p-1-j} a^{(q-j)} (a^p)^{(j-2)} \\
&= \sum_{j=0}^{(q-2)} C_q^{j+2} C_{p-3}^{j} a^{(q-2)-j)} (a^p)^{j}
\end{aligned}$$

Regardons le terme C_{p-3}^j modulo p. On a :

$$C_{p-3}^j \equiv \frac{(-3)(-4)\cdots(-(j+2))}{j!} \equiv (-1)^j \frac{(j+1)(j+2)}{2} \equiv (-1)^j C_{j+2}^2$$

Donc :

$$\begin{aligned}
C_q^{j+2} C_{p-3}^j &\equiv \frac{q(q-1)(q-2)\cdots((q-2)-j+1)}{j!(j+1)(j+2)} \\
&\quad (-1)^j \frac{(j+1)(j+2)}{2} \\
&\equiv (-1)^j \; \frac{q(q-1)}{2} \\
&\quad \frac{(q-2)\cdots((q-2)-j+1)}{j!} \\
&\equiv (-1)^j C_q^2 C_{(q-2)}^j
\end{aligned}$$

Finalement :

$$\begin{aligned}
T &= C_q^2 \sum_{j=0}^{(q-2)} (-1)^j C_{(q-2)}^j a^{((q-2)-j)} (a^p)^j \\
&= C_q^2 (a-a^p)^{(q-2)}
\end{aligned}$$

Il reste à examiner le cas où $p-1=n$. Dans ce cas $q=p$ et

$$(X+a^p)^{p-3}(X+a)^q = (X+a^p)^{p-2} \mod (X^p - X).$$

Le coefficient de X^{p-1} dans l' expression $(X+a^p)^{p-3}(X+a)^q$ vaut donc 0, il coïncide avec $C_q^2 = C_p^2 \mod p$.

□

Si on regarde ce lemme pour $n = 2$, on voit que le coefficient de X^{p-1} dans $H(X)$ modulo $X^p - X$ est $\left(\frac{\beta}{2}\right)^{p-1} C^2_{\frac{p+3}{2}} (a^p - a)^{\frac{p-1}{2}}$. Pour $p > 3$, on a $C^2_{\frac{p+3}{2}} \neq 0$ et donc $a^p = a$, ce qui entraine $a \in \mathbb{F}_p$ (ce qui est impossible).

Remarque : Précisons ce qui se passe dans le cas $p = 3$.
Posons $a_1 = h_0 x_0 = \frac{\beta}{2} a$ et $a_2 = h_1 x_1 - h_0 x_0 = \frac{\beta}{2}$. Alors $h_2 x_2 = \frac{\beta}{2}(a - 1) = a_1 - a_2$. On sait enfin que $h'_1 x_1 + h'_2 x_2 + h'_3 x_3 = 0$, donc $h'_3 x_3 = -a_2$ (on utilise le fait que $h'_1 + h_1 = 0$ et $h'_2 + 2h_2 = 0$). L'ensemble des huit points $\{x_i,\, y_i\}$ est donc l'ensemble :

$$\{\epsilon_1 a_1 + \epsilon_2 a_2, (\epsilon_1, \epsilon_2) \in \mathbb{F}_3^2 \backslash \{(0,0)\}\}$$

Supposons enfin que $m + 1 = 3p$.

On généralise les notations du cas précédent en prenant maintenant x_i, y_i, z_i pour les pôles et h_i, k_i, l_i les résidus correspondants. On posera :

- $x_i + y_i + z_i = s =$ cste (même argument que dans le cas $m+1 = 2p$).
- $x_i y_i + y_i z_i + x_i z_i = m_i$.
- $x_i y_i z_i = p_i$
- $A_i(k) = h_i x_i^k + k_i y_i^k + l_i z_i^k$.

Etape 1 : Montrons que m_i est constant :

On raisonne par l'absurde et on suppose un instant que m_i est non constant. Cela permet après une translation sur les x_i, y_i, z_i, de se ramener à $p_0 = p_p$ puis à p_i constant (on notera p_0 cette constante).

On a encore cette fois-ci les relations :

$$\sum_{i=0}^{p-1} A_i(k) = 0 \quad \text{pour } 0 \leq k \leq 3p - 2,$$

$$m_i = \frac{am_0 + im_p}{a + i} \quad \text{et} \quad p_i = \frac{ap_0 + ip_p}{a + i} = p_0 \neq 0$$

Comme précédemment, on part de l'égalité :

$$A_i(k+3) - sA_i(k+2) + m_i A_i(k+1) - p_0 A_i(k) = 0 \quad \forall k \geq 0$$

qui en sommant sur tous les i donne :

$$\sum_{i=0}^{p-1}(A_i(k+3) - sA_i(k+2) + m_iA_i(k+1) - p_0A_i(k)) = 0 \quad \forall k \geq 0$$

et donc :

$$\sum_{i=0}^{p-1} m_iA_i(k) = 0 \quad \text{pour } 1 \leq k \leq 3p-4 \tag{3}$$

Il suit de même pour $k \geq 2$:

$$\sum_{i=0}^{p-1}(m_iA_i(k+2) - m_isA_i(k+1) + m_i^2A_i(k) - p_0m_iA_i(k-1)) = 0 \tag{4}$$

et donc que :

$$\sum_{i=0}^{p-1} m_i^2A_i(k) = 0 \quad \text{pour } 2 \leq k \leq 3p-6$$

Une récurrence comme dans l'étape 2 du cas $m+1 = 2p$ montre que l'on a de plus généralement :

$$\sum_{i=0}^{p-1} m_i^lA_i(k) = 0 \quad \text{pour } l \leq k \leq 3p-2-2l. \tag{5}$$

On a alors en particulier que :

$$\sum_{i=0}^{p-1} m_i^lA_i(p-1) = 0 \quad \text{si} \quad 1 \leq l \leq p-1$$

et

$$\sum_{i=0}^{p-1} m_i^lA_i(p) = 0 \quad \text{si} \quad 1 \leq l \leq p-1.$$

Sachant que $m_i = \frac{am_0+im_p}{a+i}$, et grâce à un argument analogue à celui du cas $m+1 = 2p$ (i.e on exhibe un polynôme de degré au plus $p-2$ ayant un zéro d'ordre au moins $p-1$), on a que :

$$A_i(p-1) = A_i(p) = 0$$

Or $A_i(p) = A_i(1)^p$, donc $A_i(1) = 0$. L'expression (4) évaluée en $k = 1$ donne alors $\sum_{i=0}^{p-1} m_iA_i(0) = 0$, i.e, la relation (3) pour $k = 0$. Ceci entraîne que la relation (5) est encore vraie pour $l-1 \leq k \leq 3p-2l-2$.

On a donc $\sum_{i=0}^{p-1} m_i^l A_i(p-2) = 0$ si $1 \leq l \leq p-1$ et donc par la même construction $A_i(p-2) = 0$.

Finalement, on a $A_i(p-2) = A_i(p-1) = A_i(p) = 0$, d'où $h_i = k_i = l_i = 0$ par résolution du système linéaire, ce qui est absurde. $\lrcorner$

On a donc $m_i = \text{cste} = m_0$. La même manipulation que dans le cas $m+1 = 2p$ (étape 2) donne les relations :

$$\sum_{i=0}^{p-1} A_i(0) p_i^l = 0 \quad \text{pour } 1 \leq l \leq p-1$$

$$\sum_{i=0}^{p-1} A_i(1) p_i^l = 0 \quad \text{pour } 1 \leq l \leq p-1$$

$$\sum_{i=0}^{p-1} A_i(2) p_i^l = 0 \quad \text{pour } 1 \leq l \leq p-2$$

et on en tire de la même façon que $A_i(0) = A_i(1) = 0$ et $A_i(2)$ est de la forme $\beta(i+a)^{p-2}$(l'argument est le même : on écrit qu'un polynôme de degré au plus $p-2$ a une racine d'ordre $p-1$ ou $p-2$ selon les cas). On distingue alors deux cas :

<u>1er cas</u> : $p = 3$

Puisque $A_i(0) = h_i + k_i + l_i = 0$ on a $h_i = k_i = l_i = \pm 1 = \epsilon_i$). On obtient $A_i(2) = \beta(i+a) = \epsilon_i(x_i^2 + y_i^2 + z_i^2)$, et $A_i(1) = 0 = x_i + y_i + z_i$. D'où :

$$\begin{aligned} (x_i + y_i + z_i)^2 &= x_i^2 + y_i^2 + z_i^2 + 2m_0 \\ 0 &= \epsilon_i \beta(i+a) + 2m_0 \end{aligned}$$

c'est-à-dire $\epsilon_i(i+a)$ est une constante. Il existe au moins deux valeurs de ϵ_i égales ce qui donne la contradiction attendue.

<u>2ème cas</u> : $p \neq 3$. On se ramène à $s = 0$ (par translation). On a :

$$\begin{pmatrix} 1 & 1 & 1 \\ x_i & y_i & z_i \\ x_i^2 & y_i^2 & z_i^2 \end{pmatrix} \begin{pmatrix} h_i \\ k_i \\ l_i \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \beta(i+a)^{p-2} \end{pmatrix}$$

et donc,

$$\begin{aligned} h_i &= \frac{\beta(i+a)^{p-2}}{\Delta}(z_i - y_i) \\ k_i &= \frac{\beta(i+a)^{p-2}}{\Delta}(x_i - z_i) \\ l_i &= \frac{\beta(i+a)^{p-2}}{\Delta}(y_i - x_i) \end{aligned}$$

où Δ désigne le déterminant de Vandermonde de la matrice écrite plus haut. Il suit que :

$$h_i k_i l_i = \frac{\beta^3 (i+a)^{3(p-2)}}{\Delta^2}$$

et

$$\begin{aligned} h_i k_i + h_i l_i + k_i l_i &= \frac{\beta^2 (i+a)^{2(p-2)}}{\Delta^2}((z_i - y_i)(x_i - z_i) + (z_i - y_i)(y_i - x_i) \\ &+ (x_i - z_i)(y_i - x_i)) \\ &= \frac{\beta^2 (i+a)^{2(p-2)}}{\Delta^2}(m_0 - (x_i^2 + y_i^2 + z_i^2)) \\ &= 3\frac{\beta^2 (i+a)^{2(p-2)}}{\Delta^2} m_0 \end{aligned}$$

<u>1er sous-cas</u> : $m_0 \neq 0$. Alors $\frac{h_i k_i l_i}{h_i k_i + h_i l_i + k_i l_i} = \frac{1}{3m_0}\beta(i+a)^{p-2} \in \mathbb{F}_p$. Donc $(\frac{i}{a}+1)^{p-2} \in \mathbb{F}_p$. Posons $A = \frac{1}{a}$, alors $(Ai+1)^{p(p-2)} - (Ai+1)^{p-2} = 0$ $\forall i \in \mathbb{F}_p$. Posons $F(X) = (AX+1)^{p(p-2)} - (AX+1)^{p-2}$, alors :

$$F(X) = (A^p X + 1)^{p-2} - (AX+1)^{p-2} = 0 \bmod (X^p - X)$$

D'où $A^p = A$ et donc $a \in \mathbb{F}_p$ ce qui est absurde.

<u>2ème sous-cas</u> : $m_0 = 0$. Dans ce cas $x_i^3 = p_i = b + \frac{c}{a+i}$, avec $b = p_p$ et $c = a(p_0 - p_p)$. On a la même relation pour y_i et z_i, donc $y_i = j x_i$, $z_i = j^2 x_i$, avec $j^3 = 1$, $j \neq 1$ (quitte à échanger y_i et z_i on peut supposer que j ne dépend pas de i).

- Si $j \notin \mathbb{F}_p$, alors :

$$\begin{aligned} h_i x_i + k_i y_i + l_i z_i &= 0 \\ x_i(h_i + k_i j - (1+j) l_i) &= 0 \\ (h_i - l_i) + j(k_i - l_i) &= 0 \end{aligned}$$

Donc $h_i = k_i = l_i$. Comme $A_i(0) = h_i + k_i + l_i = 0$ et que $p \neq 3$, on obtient une absurdité.

- Donc $j \in \mathbb{F}_p$ et $p \equiv 1 \bmod 3$. Des égalités $A_i(0) = A_i(1) = 0$, on tire le système linéaire en h_i, k_i, l_i :

$$\left\{ \begin{array}{rcl} h_i + k_i + l_i &=& 0 \\ h_i + j k_i - (1+j) l_i &=& 0 \end{array} \right.$$

ce qui permet par exemple d'exprimer k_i et l_i en fonction de h_i :

$$\left\{ \begin{array}{rcccl} k_i &=& \frac{-(2+j)}{2j+1} h_i &=& \mu h_i \\ l_i &=& \frac{1-j}{2j+1} h_i &=& \lambda h_i \end{array} \right.$$

μ, $\lambda \in \mathbb{F}_p$, (indépendants de i). Donc :

$$\begin{aligned} h_i x_i^2 + k_i y_i^2 + l_i z_i^2 &= \beta(i+a)^{p-2} = A_i(2) \\ h_i x_i^2(1+\mu j^2 + \lambda j^4) &= \beta(i+a)^{p-2} \\ h_i x_i^2 &= \beta'(i+a)^{p-2} \end{aligned}$$

en posant $\beta' = \beta(1+\mu j^2 + \lambda j^4)^{-1}$. Puisque $x_i^3 = b + \frac{c}{a+i}$, il suit que :

$$\frac{h_i^3 x_i^6}{x_i^6} = \frac{\beta'^3 (i+a)^{3(p-2)}}{(b+\frac{c}{a+i})^2} = \frac{\beta'^3(i+a)^{3p-4}}{(b(a+i)+c)^2} = h_i^3$$

donc,

$$1 = \frac{\beta'^{p-1}(i+a)^{(3p-4)\frac{p-1}{3}}}{(b(a+i)+c)^{2\frac{p-1}{3}}}$$

Posons $G(X) = \beta'^{p-1}(X+a)^{(3p-4)(\frac{p-1}{3})} - (b(X+a)+c)^{2\frac{p-1}{3}}$. Alors $G(X) = 0 \mod X^p - X$. En particulier le coefficient de X^{p-1} dans $G(X)$ modulo $X^p - X$ est nul.

On peut appliquer le lemme 2.3 pour $n = 3$, (notons que $p \equiv 1 \mod 3$) ; le coefficient en X^{p-1} de $G(X)$ modulo $X^p - X$ est $\beta'^{p-1} C^2_{\frac{2p+4}{3}} (a^p - a)^{\frac{2(p-1)}{3}}$. Or, $C^2_{\frac{2p+4}{3}} \neq 0$ donc $a^p = a$, et donc $a \in \mathbb{F}_p$, d'où la contradiction. ⌟

Dans tous les cas, il n'y a pas de $L_{3p,2}$ pour $p > 2$.

2.3 Exemples d'espaces vectoriels $L_{m+1,n}$

On peut expliquer la construction qui se trouve dans [Ma] d'actions de $(\mathbb{Z}/p\mathbb{Z})^n$ sur le disque ouvert p-adique par la présence cachée d'espaces $L_{m+1,n}$. Explicitons cela.

Dans cette construction, on utilise le fait que la forme $\omega := \frac{u\mathrm{d}z}{z^{p-1}-\alpha}$ ($\alpha \in k^*$ et $u = \frac{\alpha}{x_i}$, où x_i est une des racines du polynôme $z^{p-1} - \alpha$) est logarithmique, et la remarque 4 du paragraphe 1.3.

On se donne un entier n supérieur ou égal à 2. Considérons les formes différentielles suivantes :

$$\omega_j = \frac{u_j \mathrm{d}z}{\prod_{\substack{(\epsilon_1,\cdots,\epsilon_n)\in\{0,\cdots,p-1\}^n \\ \epsilon_j \neq 0}} (z - \sum_{i=1}^n \epsilon_i a_i)}$$

où u_j est une constante que l'on va montrer pouvoir choisir "convenablement" pour que la forme ω_j soit logarithmique. On a :

$$\begin{aligned}\omega_1 &= \frac{u_1 \mathrm{d}z}{\prod\limits_{\substack{(\epsilon_1,\cdots,\epsilon_n)\in\{0,\cdots,p-1\}^n\\ \epsilon_1\neq 0}} (z-\sum\limits_{i=1}^{n}\epsilon_i a_i)}\\ &= \frac{u_1 \mathrm{d}z}{\prod\limits_{j=1}^{p-1}\prod\limits_{(\epsilon_2,\cdots,\epsilon_n)\in\{0,\cdots,p-1\}^n} (z-ja_1+\sum\limits_{i=2}^{n}\epsilon_i a_i)}\end{aligned}$$

Notons

$$Ad_1(z) = \prod_{(\epsilon_2,\cdots,\epsilon_n)\in\{0,\cdots,p-1\}^n} (z-\sum_{i=2}^{n}\epsilon_i a_i)$$

Alors Ad_1 est un polynôme additif ; ω_1 s'écrit alors :

$$\begin{aligned}\omega_1 &= \frac{u_1 \mathrm{d}z}{\prod\limits_{j=1}^{p-1} Ad_1(z-ja_1)}\\ &= \frac{u_1 \mathrm{d}z}{\prod\limits_{j=1}^{p-1} (Ad_1(z)-jAd_1(a_1))}\\ &= \frac{u_1 \mathrm{d}z}{Ad_1(z)^{p-1}-Ad_1(a_1)^{p-1}}\end{aligned}$$

On peut écrire Ad_1 sous la forme $\alpha_1 z + P_1(z^p)$, car Ad_1 est additif (cf remarque 4 du paragraphe 1.3). En particulier, $Ad_1{}'(z) = \alpha_1$. Posons $Q(z) = Ad_1(z)^{p-1} - Ad_1(a_1)^{p-1}$ et calculons $Q'(\sum_{i=1}^{n}\epsilon_i a_i)$ pour $\epsilon_i \in \{0,\cdots,p-1\}$, $\epsilon_1 \neq 0$.

$$\begin{aligned}Q'(\sum_{i=1}^{n}\epsilon_i a_i) &= -\alpha_1 Ad_1(\sum_{i=1}^{n}\epsilon_i a_i)^{p-2}\\ &= -\alpha_1(\sum_{i=1}^{n}\epsilon_i Ad_1(a_i))^{p-2}\\ &= -\alpha_1(\epsilon_1 Ad_1(a_1))^{p-2}\end{aligned}$$

Posons alors $u_1 = -\alpha_1 Ad_1(a_1)^{p-2}$. Alors :

$$\begin{aligned}\omega_1 = \frac{u_1\mathrm{d}z}{Q(z)} &= \sum_{\substack{(\epsilon_1,\cdots,\epsilon_n)\in\{0,\cdots,p-1\}^n\\ \epsilon_1\neq 0}} \frac{\frac{u_1\mathrm{d}z}{Q'(\sum_{i=1}^{n}\epsilon_i a_i)}}{(z-\sum\limits_{i=1}^{n}\epsilon_i a_i)}\\ &= \sum_{\substack{(\epsilon_1,\cdots,\epsilon_n)\in\{0,\cdots,p-1\}^n\\ \epsilon_1\neq 0}} \frac{\epsilon_1\mathrm{d}z}{(z-\sum\limits_{i=1}^{n}\epsilon_i a_i)}\end{aligned}$$

ce qui prouve que ω_1 est bien logarithmique. De même, on peut trouver u_j pour que ω_j soit logarithmique ; ω_j s'écrit alors :

$$\omega_j = \sum_{\substack{(\epsilon_1,\cdots,\epsilon_n)\in\{0,\cdots,p-1\}^n \\ \epsilon_j\neq 0}} \frac{\epsilon_j \mathrm{d}z}{(z - \sum_{i=1}^{n} \epsilon_i a_i)}$$

Des considérations de degré montrent que le déterminant de Moore $\Delta(u_1, \cdots, u_n)$ est un polynôme en les $(a_i)_{1\leq i\leq n}$ non nul. Ainsi si $(a_1, \cdots, a_n)$
$\in k^n - V(\Delta(u_1, \cdots, u_n))$, alors $(u_1 \cdots, u_n)$ sont $\mathbb{F}_p$-linéairement indépendants (c'est la condition (*) de [Ma]).

Sous cette dernière condition, montrons que $< \omega_1, \cdots, \omega_n >$ est un $L_{m+1,n}$. Puisque $\Delta(a_1, \cdots, a_n) = \Delta(a_1, \cdots, a_{n-1})Ad_n(a_n)$ et que $u_n = -\Delta(a_1, \cdots, a_{n-1})^{p-1}Ad_n(a_n)^{p-2} \neq 0$, il suit que $a_1, \cdots, a_n$ sont $\mathbb{F}_p$-linéairement indépendants.

Soit $(b_1, \cdots, b_n) \in \mathbb{F}_p^n - \{0\}$; alors $b_1\omega_1 + \cdots + b_n\omega_n$ a un zéro d'ordre $m-1$ à l'infini et $m+1 = p^n - p^{n-1}$ pôles qui sont les :

$$\{\sum_{i=1}^{n} \epsilon_i a_i, \text{ avec } b_1\epsilon_1 + \cdots + b_n\epsilon_n \neq 0\}.$$

En résumé, si $(a_1, \cdots, a_n)$ vérifie la condition (*) de [Ma], on définit :

$$\omega_j := \frac{u_j \mathrm{d}z}{\prod_{\substack{(\epsilon_1,\cdots,\epsilon_n)\in\{0,\cdots,p-1\}^n \\ \epsilon_j\neq 0}} (z - \sum_{i=1}^{n} \epsilon_i a_i)}$$

Alors $< \omega_1, \cdots, \omega_n >$ est un $L_{m+1,n}$.

Remarque 1 : Si on reprend les arguments de la remarque 4 du paragraphe 1.3, on peut construire par changement de variables d'autres exemples d'espaces $L_{m+1,n}$.

Remarque 2 : Pour chaque exemple d'espaces $L_{m+1,n}$ ainsi construits, on constate que $m+1$ est un multiple de $p^{n-1}(p-1)$. Il est tentant de penser (cf. théorème 2.2) que cette condition est nécessaire.

2.4 Applications

Le problème de l'existence de ces espaces $L_{m+1,n}$ est intimement lié aux actions de $(\mathbb{Z}/p\mathbb{Z})^n$ sur le disque ouvert p-adique.

2.4.1 Action de $(\mathbb{Z}/p\mathbb{Z})^n$ sur le disque ouvert p-adique

(Pour plus de précisions sur les rappels qui vont suivre, on renvoie à [Gr-Ma 1] et [Gr-Ma 2].)

Soit R un anneau de valuation discrète dominant l'anneau des vecteurs de Witt de k. Soit $\mathrm{D}_0 = \mathrm{Spec}(\mathrm{R}[[Z]])$ et σ un automorphisme d'ordre p agissant sur D_0 et ayant $m+1$ points fixes. On note $\mathcal{D}_0$ le modèle semi-stable minimal qui déploie les $m+1$ points fixes en des points lisses et distincts dans la fibre spéciale $\mathcal{D}_{0,s}$. La fibre spéciale est alors un arbre de droites projectives, on montre que les spécialisations des points fixes se trouvent dans les composantes terminales de l'arbre. Notons $\mathcal{D}'_0 := \mathcal{D}_0/ < \sigma >$. Les fibres spéciales $\mathcal{D}_{0,s}$ et $\mathcal{D}'_{0,s}$ sont alors homéomorphes via le morphisme de passage au quotient par σ.

Considérons une composante terminale E' de $\mathcal{D}'_{0,s}$, alors des espaces $L_{m+1,1}$ apparaissent quand on analyse la dégénerescence du μ_p-torseur induit par σ sur le disque fermé correspondant à la composante E'. Précisément, si on note $x_0, \cdots, x_m$ les points fixes de σ qui se spécialisent dans la composante E', on montre qu'il existe $f \in k(E')$ telle que $\mathrm{ord}_\infty f = 0$ et $\mathrm{d}f$ a son diviseur à support dans $\{x_i\}_i \cup \{\infty\}$, $\mathrm{ord}_{x_i}\mathrm{d}f = h_i - 1 \pmod p$, $\mathrm{ord}_\infty \mathrm{d}f = m-1$ (et $\sum h_i = 0$),(cf [Gr-Ma 2] théorème III.3.1). Après un changement de paramètre, on voit que f est de la forme :

$$\prod_{i=0}^{m}(1 - x_i x)^{h_i}$$

$$\text{et } \frac{\mathrm{d}f}{f} = -\sum_{i=0}^{m} \frac{h_i x_i}{1 - x_i x}\mathrm{d}x = \frac{-u x^{m-1}}{\prod_{i=0}^{m}(1 - x_i x)},\ u \in k^*.$$

La géométrie la plus simple qui peut intervenir est la géométrie équidistante, i.e la fibre spéciale $\mathcal{D}_{0,s}$ est réduite à une droite projective. Dans la cas où $\sigma \neq Id \bmod \mathfrak{m}$ (où $\mathfrak{m}$ est l'idéal maximal de R), la distance mutuelle entre les points fixes est $|\zeta - 1|^{\frac{1}{m}}$; elle est donc déterminée par le conducteur de l'extension.

Plus généralement, on peut définir des données combinatoires et différentielles sur les autres composantes (cf. [Gr-Ma 2]). Henrio a établi dans [He] la réciproque, c'est-à-dire, reconstruire un automorphisme d'ordre p à partir de ces données.

Nous nous proposons dans ce qui suit d'aborder sous le même angle l'action du groupe $G := (\mathbb{Z}/p\mathbb{Z})^n$. Dans le cas d'une action de G sur le disque ouvert p-adique, la description des données combinatoires et différentielles est plus délicate. Nous allons examiner ici le cas de la combinatoire la plus simple, i.e. le cas où le lieu de branchement du G-torseur correspondant est équidistant.

On se donne donc un G-torseur au dessus de $\mathrm{SpecR}[[T]] := \mathrm{SpecR}[[Z]]^G$. On a ainsi n revêtements p-cycliques $\mathrm{SpecR}[[Z_i]] \to \mathrm{SpecR}[[T]]$ donnés par les équations $Z_i^p = f_i(T)$ (où $f_i \in \mathrm{R}[T]$). Considérons une extension de $\mathrm{SpecR}[[T]]$ p-cyclique intermédiaire ; elle est donnée par une équation du type $Y^p = f_1^{\epsilon_1} \cdots f_n^{\epsilon_n}$ avec $(\epsilon_1, \cdots, \epsilon_n) \in \mathbb{F}_p^n - \{0\}$. L'hypothèse faite sur le lieu de branchement (géométrie équidistante) impose alors que ce revêtement a pour conducteur $m+1$. En particulier la forme différentielle logarithmique associée à ce revêtement a $m+1$ pôles distincts et un zéro d'ordre $m-1$ à l'infini. On obtient donc ainsi un espace $L_{m+1,n}$.

Nous remarquons aussi qu'une action de $(\mathbb{Z}/p\mathbb{Z})^n$ sur $\mathrm{R}[[Z]]$ induit en réduction (i.e modulo $\mathfrak{m}$) une action de $(\mathbb{Z}/p\mathbb{Z})^n$ sur $k[[z]]$ (qui peut être triviale).

2.4.2 Construction de $(\mathbb{Z}/p\mathbb{Z})^n$-torseurs à partir d'espaces $L_{m+1,n}$

Dans un premier temps , nous allons montrer qu'un espace $L_{m+1,n}$ donne naissance à une action de $(\mathbb{Z}/p\mathbb{Z})^n$ sur le disque ouvert p-adique (nous précisons également le $(\mathbb{Z}/p\mathbb{Z})^n$-torseur obtenu en réduction modulo $\mathfrak{m}$).

Plus précisément, on a le théorème suivant :

Théorème 2.4 *On considère un $L_{m+1,n}$ et une base $\omega_1, \cdots, \omega_n$ de cet espace, chaque ω_i s'écrivant $\frac{\mathrm{d}f_i}{f_i}$. Soit ζ une racine primitive p-ième de l'unité et $R=W(k)[\pi]$ où $\pi^m := \lambda := \zeta - 1$, on note $K=Frac(R)$. Alors on peut trouver $F_i \in R[X]$ relevant f_i tels que le produit fibré des revêtements de $\mathbb{P}^1_{\mathrm{K}}$ donnés par les équations $Y_i^p = F_i(X)$ induisent après normalisation un revêtement de $\mathbb{P}^1_{\mathrm{K}}$ galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^n$ ayant bonne réduction relativement à la valuation de Gauss $T := \pi^{-p}X$. La fibre spéciale du modèle lisse correspondant est un revêtement étale, galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^n$ de la droite affine $\mathbb{A}^1_k$.*

La démonstration suit les méthodes utilisées dans [Ma]. Nous allons l'adapter au cas qui nous préoccupe.

Nous montrons d'abord le lemme suivant :

Lemme 2.5 *Soit $\omega_1, \cdots, \omega_n$ une base d'un espace $L_{m+1,n}$; soit $(x_i)_{1\leq i\leq T}$ la réunion des pôles de ω_j pour $1 \leq j \leq n$ et $(x_i)_{i\in I_j}$ les pôles de ω_j. Chaque ω_j s'écrit $\frac{\mathrm{d}f_j}{f_j}$ avec $f_j = \prod_{i=1}^T (1 - x_i x)^{h_{ij}}$ et $h_{ij} = 0$ pour $i \notin I_j$. Soit $X_i \in W(k)$ des relèvements de x_i pour $1 \leq i \leq T$. On pose $F_j(X) := \prod_{i=1}^T (1 - X_i X)^{h_{ij}}$. Alors il existe $\hat{Q}_j(X), \hat{R}_j(X), \hat{S}_j(X) \in W(k)[X]$ et $U_j \in W(k)$ inversible tels que :*

$$F_j(X) = (1 + X\hat{Q}_j(X))^p + U_j X^m (1 + X\hat{R}_j(X)) + p\hat{S}_j(X) \qquad (*)$$

Démonstration : On a :

$$f_j' = \frac{u_j x^{m-1}}{\prod_{i=1}^{T}(1-x_i x)} \prod_{i=1}^{T}(1-x_i x)^{h_{ij}} = u_j x^{m-1}(1+xr(x))$$

où $r(x)$ est un polynôme dans lequel on a regroupé tous les termes de degré supérieur. Le polynôme f_j est donc de la forme :

$$f_j = (1+xq(x))^p + \frac{u_j x^m}{m}(1+x\tilde{r}(x)).$$

Donc F_j qui est un relèvement de g s'écrit :

$$F_j = (1+X\hat{Q}_j(X))^p + U_j X^m(1+X\hat{R}_j(X)) + p\hat{S}_j(X)$$

□

Démonstration du théorème : L'approximation (*) du lemme 2.5 n'est a priori pas suffisante pour garantir que les F_j satisfassent le théorème. On va améliorer cette approximation en utilisant l'automorphisme de Frobenius. L'action du Frobenius inverse sur $k[t]$ est définie de la façon suivante : si $f := \sum a_i x^i \in k[t]$ alors on pose $f^{F^{-1}} := \sum a_i^{\frac{1}{p}} x^i$. Cette opération commute avec la dérivation (i.e $(f^{F^{-1}})' = (f')^{F^{-1}}$). On peut donc étendre cette action aux formes différentielles que l'on considère. En particulier, si on a un espace $L_{m+1,n}$ engendré par les n formes différentielles $\omega_1, \cdots, \omega_n$ alors on en déduit que le $\mathbb{F}_p$-espace vectoriel engendré par les formes $\omega_1^{F^{-1}}, \cdots, \omega_n^{F^{-1}}$ est encore un espace $L_{m+1,n}$.

On choisit une des fonctions f_j (que l'on appelle f dans la suite pour ne pas surcharger les notations ; de la même façon on notera h_i à la place de h_{ij}). Nous allons montrer qu'il existe des X_i relevant x_i tels que la fonction F définie par $F := \prod_{i=1}^{T}(1-X_i X)^{h_i}$ soit de la forme :

$$F(X) = (1+XQ(X))^p + U^p X^m(1+XR(X)) + pX^{\frac{(m+1)}{p}}S(X) + p^2 T(X)$$

avec $Q(X), R(X), S(X), T(X) \in W(k)[X]$ et $U \in W(k)$ inversible.

Soit $y_i \in k$ tels que $y_i^p = x_i$; prenons $Y_i \in W(k)$ relevant y_i. Posons :

$$F(X) := \prod_{i=1}^{T}(1-Y_i^p X)^{h_i}$$

Il est clair que F relève f. Vérifions que F est de la forme annoncée.

On a :

$$\begin{aligned}
F(X^p) &= \prod_{i=1}^{T}(1-(Y_iX)^p)^{h_i} \\
&= \prod_{j=0}^{p-1}\prod_{i=1}^{T}(1-\zeta^k Y_i X)^{h_i}
\end{aligned}$$

Or, on a $(\prod_{i=1}^{T}(1-y_ix)^{h_i}) = f(x)^{F^{-1}}$, donc $\prod_{i=1}^{T}(1-y_ix)^{h_i}$ vérifie les hypothèses du lemme 2.5 et il existe $\hat{Q}(X), \hat{R}(X), \hat{S}(X) \in W(k)[X]$ et $U \in W(k)$ inversible tels que :

$$\prod_{i=1}^{T}(1-Y_i(\zeta^jX))^{h_i} = (1+\zeta^jX\hat{Q}(\zeta^jX))^p + U(\zeta^jX)^m(1+\zeta^jX\hat{R}(\zeta^jX)) + p\hat{S}(\zeta^jX)$$

ce que l'on peut écrire aussi :

$$\begin{aligned}
\prod_{i=1}^{T}(1-Y_i(\zeta^jX))^{h_i} &= (1+\zeta^jX\hat{Q}(\zeta^jX))^p(1+U(\zeta^jX)^m(1+\zeta^jX\tilde{R}(\zeta^jX)) \\
&+ p\tilde{S}(\zeta^jX))
\end{aligned}$$

avec $\tilde{R}(X), \tilde{S}(X) \in W(k)[[X]]$. Ce qui donne :

$$\begin{aligned}
F(X^p) &= \prod_{j=0}^{p-1}(1+\zeta^jX\hat{Q}(\zeta^jX))^p \\
&\quad \prod_{j=0}^{p-1}(1+U(\zeta^jX)^m(1+\zeta^jX\tilde{R}(\zeta^jX))p\tilde{S}(\zeta^jX))
\end{aligned}$$

que nous regardons modulo p^2. On a :

$$\prod_{j=0}^{p-1}(1+\zeta^jX\hat{Q}(\zeta^jX))^p \in 1+X^pW(k)[X^p]$$

et

$$\begin{aligned}
&\prod_{j=0}^{p-1}(1+U(\zeta^jX)^m(1+\zeta^jX\tilde{R}(\zeta^jX))p\tilde{S}(\zeta^jX)) \\
= &\prod_{j=0}^{p-1}(1+U(\zeta^jX)^m(1+\zeta^jX\tilde{R}(\zeta^jX))) + p\sum_{j=0}^{p}(\tilde{S}(\zeta^jX) \\
&\prod_{\substack{k\in\{0,\cdots,p-1\}\\ k\neq j}}(1+U(\zeta^kX)^m(1+\zeta^kX\tilde{R}(\zeta^kX))) \bmod p^2
\end{aligned}$$

Remarquons que la dernière somme appartient à $(\zeta-1)W(k)[[\zeta,X]]\cap W(k)[[X]]=pW(k)[[X]]$, donc :

$$p\sum_{j=0}^{p}(\tilde{S}(\zeta^j X)\prod_{\substack{k\in\{0,\cdots,p-1\}\\ k\neq j}}(1+U(\zeta^k X)^m(1+\zeta^k X\tilde{R}(\zeta^k X)))=0 \bmod p^2$$

Enfin, on a :

$$\prod_{j=0}^{p-1}(1+U(\zeta^j X)^m(1+\zeta^j X\tilde{R}(\zeta^j X)))\equiv(1+U^p X^{pm}(1+X^p\tilde{R}^p(X))) \bmod (\zeta-1)$$

ainsi que :

$$\prod_{j=0}^{p-1}(1+U(\zeta^j X)^m(1+\zeta^j X\tilde{R}(\zeta^j X)))$$

$$\in W(k)[[X^p]]\cap(1+X^m W(k)[[X]])=1+(X^p)^{([\frac{m}{p}]+1)}W(k)[[X^p]]$$

Donc $F(X)$ est de la forme annoncée.

Nous allons montrer que l'équation $Y^p=F(X)$ définit une courbe ayant bonne réduction sur R relativement à la valuation de Gauss en $T:=\lambda^{\frac{-p}{m}}X$.

En effet, si on pose $Y=\lambda Z+1+XQ(X)$ et $T:=\lambda^{\frac{-p}{m}}X$ alors l'équation $Y^p=F(X)$ donne en réduction :

$$z^p-z=u^p t^m$$

Encore une fois, on a l'égalité des genres des fibres géométriques et spéciales, ce qui assure la bonne réduction.

On obtient ainsi n revêtements $Y_i^p=F_i(X)$ $(1\leq i\leq n)$ de $\mathbb{P}^1_{\mathrm{K}}$ qui ont simultanément bonne réduction pour la même valuation de Gauss (l'équation en réduction est $z_i^p-z_i=u_i t^m$). On considère le produit fibré de ces revêtements, après normalisation il induit un revêtement $\mathcal{C}\to\mathbb{P}^1_R$ galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^n$. De plus, la fibre spéciale C_s est intègre car les u_i sont linéairement indépendants sur $\mathbb{F}_p$ (cf. remarque 3 du paragraphe 1.3). Il reste à voir que ce revêtement a bonne réduction sur R.

On écrit $m+1=qp^{n-1}$, $q\in\mathbb{N}^*$. Le degré de la différente spéciale du compositum des n extensions $z_i^p-z_i=u_i t^m$ est :

$$\begin{aligned} d_s &= (m+1)(p-1)(1+p+\cdots p^{n-1}) \\ &= qp^{n-1}(p-1)(1+p+\cdots p^{n-1}) \end{aligned}$$

Notons d_η le degré de la différente du revêtement $C_\eta \to \mathbb{P}^1_K$. Ce revêtement n'est ramifié qu'en les points qui sont des relèvements des pôles des formes différentielles, i.e au plus $T = q(1+\cdots+p^{n-1})$ points (voir la démonstration du lemme 1.2). Les groupes d'inertie étant cycliques d'ordre p, on obtient :

$$d_\eta \leq p^{n-1}(q(1+p+\cdots+p^{n-1}))(p-1) = d_s$$

On obtient la bonne réduction en appliquant le critère local de bonne réduction donné dans [Gr-Ma 1].

$\square$

Remarque : Si on regarde cette dernière action en réduction modulo l'idéal maximal de R, on trouve un $(\mathbb{Z}/p\mathbb{Z})^n$-torseur au dessus de $k[[t]]$ donné par les équations :

$$\left\{ \begin{array}{rcl} z_1^p - z_1 & = & u_1 t^m \\ & \vdots & \\ z_n^p - z_n & = & u_n t^m \end{array} \right.$$

où les u_i sont $\mathbb{F}_p$-indépendants, car attachés à un espace $L_{m+1,n}$ (cf. remarque 3 du paragraphe 1.3).

2.4.3 Déformation des $(\mathbb{Z}/p\mathbb{Z})^2$-torseurs

On s'intéresse ici à la déformation de $(\mathbb{Z}/p\mathbb{Z})^2$-torseurs au dessus de Spec$k[[t]]$ avec une géométrie équidistante ; ceci impose de ne considérer que des extensions de $k[[t]]$ pour lesquelles les sous-extensions intermédiaires ont des conducteurs égaux.

Dans le cas $m+1 = p$, on sait d'après [Gr-Ma 2] Théorème III.3.1 que la géométrie qui apparait est équidistante. Ainsi on a le théorème suivant corollaire du théorème 2.2 :

Théorème 2.6 *Soit* $\mathrm{G} = (\mathbb{Z}/p\mathbb{Z})^2$, $p \geq 3$ *et* R *un anneau de valuation discrète dominant l'anneau des vecteurs de Witt de k. Supposons que G est un groupe d'automorphismes de* $k[[z]]$ *et que chacune des sous-extensions de* $k[[z]]^{\mathrm{G}}$*, d'ordre p a un conducteur égal à p. Alors, on ne peut pas relever G en un groupe d'automorphismes de* $R[[Z]]$.

Démonstration : On rappelle le critère de relèvement donné par [Gr-Ma 1] Théorème I.5.1. Pour qu'il y ait relèvement, il faut et il suffit que :

"Etant donné deux extensions intermédiaires de la forme $k[[z]]^{\mathrm{G}_1}$, $k[[z]]^{\mathrm{G}_2}$, on puisse relever chacune de ces extensions en $\mathrm{R}[[Z]]^{\mathrm{G}_i}/\mathrm{R}[[Z]]^{\mathrm{G}}$ telles que ces deux derniers revêtements aient exactement $(p-1)$ points de branchement en commun."

Supposons que le relèvement soit possible et traduisons ce qui doit se passer au niveau de la fibre spéciale $\mathcal{D}_{0,s}$. Les équations des deux revêtements intermédiaires sont de la forme $Y_1^p = F_1(X)$ et $Y_2^p = F_2(X)$. On a $m < p$, donc pour chacune de ces extensions, $\mathcal{D}_{0,s}$ est une droite projective sur laquelle on a $m+1$ points équidistants qui correspondent aux spécialisations des points fixes par l'automorphisme d'ordre p correspondant (cf. [Gr-Ma 2] théorème III.3.1). On a donc des fonctions f_1, f_2 (qui sont les réductions de F_1 et F_2) de la forme :

$$f_1 = \prod_{i=0}^{p}(1 - x_i x)^{h_i} \quad h_0 = 0,\ h_i \neq 0,\ \sum h_i = 0$$

$$f_2 = \prod_{i=0}^{p}(1 - x_i x)^{h'_i} \quad h'_p = 0,\ h'_i \neq 0,\ \sum h'_i = 0$$

telles que $\mathrm{d}f_1$ et $\mathrm{d}f_2$ aient les conditions sur leurs diviseurs énoncées précédemment. Cette écriture traduit déjà le fait que l'on a $(p-1)$ points de branchement en commun (leurs spécialisations sont $x_1, \cdots, x_{p-1}$).

Posons $\omega_1 = \frac{\mathrm{d}f_1}{f_1}$ et $\omega_2 = \frac{\mathrm{d}f_2}{f_2}$. Toute autre extension intermédiaire est donnée par une équation de la forme $\mathrm{Y}^p = f_1^{\epsilon_1} f_2^{\epsilon_2}$, $((\epsilon_1, \epsilon_2) \in \mathbb{F}_p^2 - \{(0,0)\})$, donc donne naissance à une différentielle $\omega_j = \epsilon_1 \frac{\mathrm{d}f_1}{f_1} + \epsilon_2 \frac{\mathrm{d}f_2}{f_2}$ qui a aussi p pôles distincts et un zéro d'ordre $m-1$ en 0.

On voit donc que dans le cas $m+1 = p$, la possibilité de relever l'action du groupe G implique l'existence d'espaces $L_{p,2}$, ce qui est démenti par le théorème **??**.

□

Remarque 1 : Dans [Be], Bertin donne des obstructions au relèvement d'actions de groupe. Le théorème 2.6 donne de nouvelles obstructions qui sont de nature différentielle.

Remarque 2 : Le théorème 2.6 utilise juste le premier résultat du théorème 2.2. Pour les cas $m+1 = 2p$ ou $3p$, on ne peut pas énoncer un théorème analogue car on n'a pas forcément une géométriquement équidistante. On peut juste dire dans ces cas-là que si le relèvement est possible, il doit faire apparaitre une géométrie plus complexe.

Enfin nous considérons le cas où $p = 2$ avec cette fois-ci un conducteur quelconque. On a alors le théorème suivant :

Théorème 2.7 *On considère une action de G= $(\mathbb{Z}/2\mathbb{Z})^2$ comme groupe d'automorphismes de $k[[t]]$ dans laquelle chacune des sous-extensions de $k[[t]]^{\mathrm{G}}$ d'ordre 2 a même conducteur (on note $m+1 = 2n$ ce conducteur). Alors on peut déformer cette action en une action de G sur $R[[T]]$, où $R= W(k)[\lambda^{\frac{1}{2n-1}}]$.*

La démonstration est dûe à Ito et suit des indications de M.Matignon. Nous la redonnons avec quelques modifications.

On a tout d'abord besoin du lemme suivant :

Lemme 2.8 *Soit $X_1, \cdots, X_n \in W(k)$ deux à deux distincts et $U \in W(k)^*$. Alors il existe $X_{n+1}, \cdots, X_{2n}$ (avec $X_i \neq X_j$ dès que $1 \leq i < j \leq 2n$) et $Q(X), R(X) \in W(k)[X]$ tels que le polynôme :*

$$F(X) := \prod_{i=1}^{2n}(1 - X_i X) = (Q(X))^2 + UX^{2n-1} + 2R(X)$$

et tels que le revêtement de Spec$(W(k)[X])$ donné par $Y^2 = F(X)$ ait bonne réduction.

<u>Démonstration :</u> Notons x_i la réduction de X_i modulo l'idéal maximal de $W(k)$. D'après le théorème 2.1, on peut trouver $x_{n+1}, \cdots, x_{2n}$ tels que :

$$f(x) := \prod_{i=1}^{2n}(1 - x_i x) = (q(x))^2 + ux^{2n-1}$$

(où u est la réduction de U). Choisissons des relèvements X_i de x_i et posons :

$$\tilde{F}(X) = \prod_{i=1}^{2n}(1 - X_i X)$$

$\tilde{F}$ est aussi de la forme :

$$\tilde{F}(X) = Q^2(X) + 2R(X) + UX^{2n-1}$$

avec $Q = 1 + a_1 X + \cdots + a_n X^n \in W(k)[X]$, $R = b_1 X + \cdots + b_{2n-1}X^{2n-1} \in W(k)[X]$. Ecrivons $\tilde{F}$ en fonction du paramètre $T := (-2)^{-\frac{2}{2n-1}} X$:

$$\begin{aligned}\tilde{F}(T) \quad &= \quad Q^2((-2)^{\frac{2}{2n-1}}T) + 2(b_1(-2)^{\frac{2}{2n-1}}T + \cdots + b_{2n-1}(-2)^2 T^{2n-1}) + \\ &\quad\quad (-2)^2 UT^{2n-1}\end{aligned}$$

Posons $Y = -2Z + Q$; si le coefficient $(b_1(-2)^{\frac{2}{2n-1}}T + \cdots + b_m(-2)^2 T^m)$ est nul modulo 2, alors on a en réduction :

$$\begin{aligned}\frac{((-2)Z + Q)^2 - Q^2}{(-2)^p} &= UT^m \\ Z^2 - Z &= UT^m\end{aligned}$$

Ceci est suffisant pour avoir la bonne réduction. En effet, le revêtement d'équation $Y^2 = \tilde{F}(X)$ est ramifié en $2n$ points (nombre de racines de $\tilde{F}$), donc le genre de la fibre générique est $\frac{(2n-2)(2-1)}{2}$ (formule d'Hurwitz), c'est-à-dire le même que celui de la fibre spéciale.

On va donc chercher à modifier $\tilde{F}$. On écrit $\tilde{F}(X) = \prod_{i=1}^{2n}(1-X_iX)$. Posons

$$F(X) = \prod_{i=1}^{2n}(1 - X_iX - 2\epsilon_iX)$$

où $\epsilon_i = 0$ si $i \leq n$ et $(\epsilon_i, i > n)$ sont des constantes à déterminer pour avoir bonne réduction.

$$\begin{aligned}
F(X) &= \prod_{i=1}^{2n}(1 - X_iX)\left(1 + 2\sum_{i=1}^{2n-1}\frac{\epsilon_iX}{1 - X_iX}\right) \text{ mod } [4] \\
&= (Q^2 + 2R)\left(1 + 2\sum_{i=1}^{2n}\frac{\epsilon_iX}{1 - X_iX}\right) + UX^{2n-1} \text{ mod } [4, X^{2n}, 2X^{2n-1}] \\
&= Q^2 + 2\left(Q^2\sum_{i=1}^{2n}\frac{\epsilon_iX}{1 - X_iX} + R\right) + UX^{2n-1} \text{ mod } [4, X^{2n}, 2X^{2n-1}] \\
&= Q^2 + 2(Q^2X\sum_{i=1}^{2n}\epsilon_i(1 + X_iX + \cdots + (X_iX)^{2n-2}) + R) \\
&+ UX^{2n-1} \text{ mod } [4, X^{2n}, 2X^{2n-1}]
\end{aligned}$$

On va donc s'arranger pour que le terme

$$Q^2X\sum_{i=1}^{2n}\epsilon_i(1 + X_iX + \cdots + (X_iX)^{2n-2}) + R)$$

soit nul modulo 2. Remarquons tout d'abord que si $k \geq n$, alors les termes en X^k (écrits en fonction du paramètre T) sont nuls modulo 2. Il suffit donc de voir que l'on peut choisir les ϵ_i de telle façon que les termes en X^k $(1 \leq k \leq n-1)$ de l'expression :

$$Q^2X\sum_{i=1}^{2n-1}\epsilon_i(1 + X_iX + \cdots + (X_iX)^{2n-2}) + R)$$

soient nuls. Soit α_k le k-ième terme de la série de Taylor de $(-RQ^{-2})$ (i.e $(-RQ^{-2}) = \sum_{k\geq 1}\alpha_kX^k$). Alors la condition que l'on vient d'énoncer se ramène au système :

$$\sum_{i=n+1}^{2n}\epsilon_iX_i^k = -\alpha_k \quad \text{pour} \quad 0 \leq k \leq n-2$$

qui a des solutions puisque c'est un système de Vandermonde avec des équations en moins.

$\square$

Revenons à la démonstration du théorème. Considérons une $(\mathbb{Z}/2\mathbb{Z})^2$-extension $k[[z]]/k[[t]]$ telle que les sous-extensions intermédiaires C_i aient le même conducteur $m+1 = 2n$. Après un changement de paramètre t, on peut supposer que C_1 et C_2 sont données par les équations :

$$\begin{cases} C_1 : y_1^2 + y_1 &= \frac{u}{t^{2n-1}} \\ C_2 : y_2^2 + y_2 &= \frac{p(t)}{t^{2n-1}} \end{cases}$$

avec $u \in k^*$ et $p(t) = 1 + p_1 t + \cdots + p_{2n-2} t^{2n-2}$. D'après [Gr-Ma 1] Th I.5.1, il faut pouvoir relever C_1 et C_2 de façon à ce que ces deux revêtements aient exactement n points de branchements en commun.

Posons $t' = t(p(t))^{\frac{-1}{2n-1}}$. Alors les deux extensions intermédiaires sont données par :

$$\begin{cases} C_1 : y_1^2 + y_1 &= \frac{u}{t^{2n-1}} \\ C_2 : y_2^2 + y_2 &= \frac{1}{t'^{2n-1}} \end{cases}$$

Soit T un paramètre du disque ouvert relevant t et $T' := T(p(T))^{\frac{-1}{2n-1}}$ un paramètre relevant t' (et $P(T)$ est un relèvement de $p(t)$). Si on écrit $T' = \tau(T)$, alors τ définit un automorphisme du disque ouvert $\mathrm{Spec} W(k)[[T]]$. Notons $X = 2^{\frac{2}{2n-1}} T^{-1}$. Alors τ induit un automorphisme sur le disque fermé $\mathrm{Spec} W(k)\{\{X^{-1}\}\}$ (rappelons que que les éléments de $W(k)\{\{X^{-1}\}\}$ sont les séries formelles de la forme $\sum_{\nu \geq 0} a_\nu X^{-\nu}$ avec $\lim_{\nu \to \infty} a_\nu = 0$). Ce qui donne $\tau(X^{-1}) = X^{-1} P(2^{\frac{2}{2n-1}} X^{-1})^{\frac{-1}{2n-1}}$ et τ est l'identité en réduction. Soit $\tilde{C}_2 : Y_2^2 = 1 + \frac{4}{T'^{2n-1}}$ un relèvement de C_2 que l'on peut reécrire en choisissant de nouveaux paramètres :

$$(Y_2')^2 = 1 - (X')^{2n-1} = \prod_{i=1}^{2n} (1 - X_i' X')$$

Les idéaux $(1 - X_i' X')$ définissent des points distincts dans $\mathrm{Spec} W(k)\{\{X^{-1}\}\}$. Posons $(1 - X_i X) := \tau^{-1}(1 - X_i' X')$. On applique alors le lemme précédent aux points $X_1 \cdots X_n$, ce qui permet d'obtenir un revêtement d'équation :

$$\tilde{C_1} : (Y_1')^2 = A(X)^2 + 2B(X) + UX^{2n-1}$$

qui a bonne réduction et qui a n points de branchement en commun avec $\tilde{C}_2$. Le relèvement souhaité est alors donné par la normalisation de $\tilde{C}_1 \times_{W(k)[[X]]} \tilde{C}_2$.

Remarque : Dans le cas $p > 2$ une généralisation du théorème 2.7 est un problème ouvert. On s'aperçoit déjà au vu du théorème 2.2 que la condition $p/m+1$ n'est pas suffisante : il faut en plus l'existence d'espaces $L_{m+1,2}$.

Références

[Be] J.Bertin : *Obstructions locales au relèvement de revêtements galoisiens de courbes lisses* C.R Acad. Sci. Paris, t.326, Série I, p.55-58, (1998)

[Go] D.Goss : *Basic Structures of Function Field Arithmetic.* Ergebnisse der Mathematik **35**, Springer-Verlag (1996).

[Gr-Ma 1] B.Green, M.Matignon : *Liftings of Galois covers of smooth curves.* Compositio Math, Vol **113**, 239-274 (1998).

[Gr-Ma 2] B.Green, M.Matignon : *Order p automorphisms of the open disc of a p-adic field.* J.Amer.Math.Soc. **12**, 269-303 (1999).

[He] Y.Henrio : *Arbres de Hurwitz et automorphismes d'ordre p des disques et des couronnes p-adiques formels.* à paraître dans Compositio Mathematica.

[It] T.Ito : *On the liftability of* $(2,2)$*-covering of curves in characteristic* 2. Communication personnelle (2000).

[Ma] M.Matignon : *p-Groupes abéliens et disques ouverts p-adiques.* Manuscripta Math, Vol **99**, 93-109 (1999).

Guillaume Pagot
Laboratoire de théorie des nombres
et algorithmique arithmétique,
Université de Bordeaux I,
351, cours de la libération,
33405 Talence Cedex
email : pagot@math.u-bordeaux.fr