Relèvement en caractéristique zéro d'actions de groupes abéliens de type (p,...,p).

Guillaume Pagot

Relèvement en caractéristique zéro d'actions de groupes abéliens de type (p,...,p).

Guillaume Pagot

N°d'ordre : 2603

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Guillaume PAGOT

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

RELÈVEMENT EN CARACTÉRISTIQUE ZÉRO D'ACTIONS DE GROUPES ABÉLIENS DE TYPE $(p, \cdots, p)$

Soutenue le : 9 décembre 2002

Après avis de :

I. BOUW, Chercheur	Universität Gesamthochschule Essen	Rapporteur
M. GARUTI, Chercheur	Université de Padoue	Rapporteur

Devant la commission d'examen formée de :

I. BOUW, Chercheur	Universität Gesamthochschule Essen	
P. DEBES, Professeur	Université de Lille	Président
M. GARUTI, Chercheur	Université de Padoue	Rapporteur
M. MATIGNON, Professeur	Université Bordeaux 1	Directeur

- 2002 -

Relèvement en caractéristique zéro d'actions de groupes abéliens de type $(p, \cdots, p)$

Guillaume Pagot

20 septembre 2002

Table des matières

Introduction

Soit p un nombre premier et k un corps algébriquement clos de caractéristique p. Soit R un anneau de valuation discrète dominant l'anneau des vecteurs de Witt de k, $W(k)$.

Soit C une courbe propre et lisse sur k et G un groupe de k-automorphismes de C. On étudie ici le problème de la déformation à la caractéristique 0 du couple (C, G) : il s'agit de trouver $\mathcal{C}$ une courbe propre et lisse sur R, de fibre spéciale C, et une injection $G \longrightarrow \mathrm{Aut}_R\mathcal{C}$ qui induise en réduction $G \longrightarrow \mathrm{Aut}_k C$. Ce problème est de nature locale et se ramène à la question suivante : étant donné G un groupe de k-automorphismes de $k[[z]]$, peut on relever G en un groupe de R-automorphismes de $R[[Z]]$ (où Z est un relèvement de z) ?

Dans cette thèse on étudie particulièrement le cas où $G = (\mathbb{Z}/p\mathbb{Z})^2$. Lorsque $p \geq 3$, on établit l'existence de nouvelles obstructions (de nature combinatoire et différentielle) au relèvement. Le cas $p = 2$ est traité à part et on montre qu'il n'y a pas d'obstructions au relèvement lorsque $G = (\mathbb{Z}/2\mathbb{Z})^2$.

Des obstructions au relèvement d'action de $(\mathbb{Z}/p\mathbb{Z})^2$ sont déjà connues. En effet, considérons une extension galoisienne de groupe $(\mathbb{Z}/p\mathbb{Z})^2$ de l'anneau $k[[t]]$. Celle-ci est donnée par les deux équations :

$$\begin{cases} x_1^p - x_1 &= f_1\left(\frac{1}{t}\right) \\ x_2^p - x_2 &= f_2\left(\frac{1}{t}\right) \end{cases}$$

où f_1, f_2 sont deux polynômes de degrés respectifs m_1 et m_2 (avec $m_1 \leq m_2$, et m_1, m_2 premiers à p). Une première condition nécessaire au relèvement est $m_1 + 1 \in p\mathbb{Z}$ (on renvoie pour cela à [Gr-Ma 1] ou à [Be]). Dans [Gr-Ma 1] on trouve en outre une condition nécessaire et suffisante pour déterminer quand ce relèvement est possible (ceci sera rappelé dans le Théorème 1.4.2).

Considérons un automorphisme σ du disque ouvert p-adique $D_0 :=\mathrm{Spec}R[[Z]]$. On lui associe naturellement le modèle minimal semi-stable qui déploie les points fixes en des points lisses et distincts à la fibre spéciale. Cette fibre spéciale est alors un arbre de droites projectives, et des formes différentielles logarithmiques apparaissent sur les composantes terminales de cet arbre.

Considérons maintenant une action de $G := (\mathbb{Z}/p\mathbb{Z})^2$ sur le disque ouvert p-adique ($p \geq 3$). On note $G_0, \cdots, G_p$ les sous-groupes d'ordre p de G et Rev_i $(0 \leq i \leq p)$ les revêtements intermédiaires $\mathrm{Spec}R[[Z]]^{G_i} \longrightarrow \mathrm{Spec}R[[Z]]^G$. Soit F la réunion des points de branchement de Rev_i et $\mathcal{D}_0$ le modèle minimal semi-stable qui déploie les points de F en des points lisses

et distincts à la fibre spéciale. On montre alors l'existence de $\mathbb{F}_p$-espaces vectoriels de formes différentielles logarithmiques sur les composantes terminales de la fibre spéciale $\mathcal{D}_{0,s}$. Plus précisément, on montre que les espaces qui apparaissent sur les composantes terminales de $\mathcal{D}_{0,s}$ ont trois formes possibles, à savoir : $L_{m+1,1}$, $L_{qp,2}$, $L^j_{qp,2}$ (ces espaces sont introduits dans la Définition 2.1.3).

Le chapitre 1 est consacré à quelques rappels concernant le relèvement en caractéristique zéro d'actions de groupes sur les courbes lisses. On rappelle un principe local-global qui permet de ramener la question au relèvement d'actions de $k[[z]]$ à $R[[Z]]$, ainsi que quelques résultats relatifs aux autorphismes d'ordre p du disque ouvert p-adique. On donne enfin un critère de relèvement dans le cas particulier où $G = (\mathbb{Z}/p\mathbb{Z})^2$.

L'étude des espaces $L_{m+1,1}$, $L_{qp,2}$ et $L^j_{qp,2}$ est l'objet du chapitre 2. Un lemme élémentaire (Lemme 2.2.2) donne une première idée sur la répartition des pôles des formes différentielles non nulles d'un espace $L_{m+1,n}$. Comme il est classique d'exprimer à partir de l'opération de Cartier le fait qu'une forme 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. On s'intéresse de façon plus particulière aux espaces $L_{m+1,2}$ et on montre le théorème suivant :

Théorème 0.0.1 *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 fait appel à une analyse algébrique des équations sur les résidus aux pôles, ce qui la rend technique. La conclusion dépend d'un lemme (Lemme 2.2.6) dont nous n'avons pas vu trace dans la littérature.

Le chapitre 3 donne des applications directes de l'étude de ces espaces. Nous commençons par montrer que la donnée d'un espace $L_{m+1,n}$ donne naissance à une action de $(\mathbb{Z}/p\mathbb{Z})^n$ sur le disque ouvert p-adique. Ensuite, comme principale application, nous montrons l'existence de nouvelles obstructions au relèvement. Ceci est l'objet du théorème suivant :

Théorème 0.0.2 *Soit $p \geq 3$ un nombre premier et $G := (\mathbb{Z}/p\mathbb{Z})^2$. On suppose que G est un groupe de k-automorphismes de $k[[z]]$ et que chacune des sous-extensions de $k[[z]]^G$ de degré p a un conducteur égal à $m+1$.*

1. *Si $m+1 = p$, alors on ne peut pas relever G en un groupe de R-automorphismes de $R[[Z]]$.*
2. *Supposons que $m+1 = 2p$. Alors G se relève en un groupe de R-automorphismes de $R[[Z]]$ si et seulement si la géométrie du lieu de branchement du revêtement*

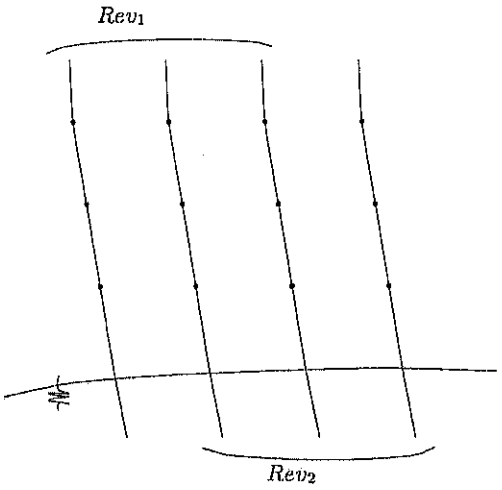
$$\mathrm{Spec}R[[Z]] \to \mathrm{Spec}R[[Z]]^G$$

est équidistante. Il suit que p doit être égal à 3.

3. *Supposons que* $m+1=3p$. *Alors* G *se relève en un groupe de* R*-automorphismes de* $R[[Z]]$ *si et seulement si* $p=3$ *et la géométrie du lieu de branchement du revêtement*

$$\mathrm{Spec}R[[Z]] \to \mathrm{Spec}R[[Z]]^G$$

a la forme suivante :



La démonstration du Théorème 0.0.2 repose sur un examen combinatoire de toutes les géométries possibles. Outre les résultats du Théorème 0.0.1, cette démonstration met en œuvre une analyse des $\mathbb{F}_p$-espaces vectoriels de formes différentielles exactes qui apparaissent sur les composantes internes de $\mathcal{D}_{0,s}$, ainsi que l'étude de la variation de la différente pour chacun des revêtements Rev_i.

Les obstructions exhibées dans le Théorème 0.0.2 ne sont pas les seules. En effet, lorsque l'on examine le cas où les conducteurs des extensions intermédiaires ne sont plus égaux, on obtient de nouvelles conditions pour le relèvement. On montre notamment le théorème suivant :

Théorème 0.0.3 *Soit* $p \geq 5$, *un nombre premier et* $G := (\mathbb{Z}/p\mathbb{Z})^2$. *On suppose que* G *est un groupe de* k*-automorphismes de* $k[[z]]$ *et que l'une des sous-extensions de* $k[[z]]^G$ *de degré* p *a un conducteur* m_1+1 *égal à* p *tandis que les* p *autres sous-extensions ont un conducteur* m_2+1 *tel que* $p+1 < m_2+1 < 2p-1$. *Alors on ne peut pas relever* G *en un groupe de* R*-automorphismes de* $R[[Z]]$.

Dans le chapitre 4, nous donnons des exemples de réalisations de $(\mathbb{Z}/p\mathbb{Z})^n$ comme groupe d'automorphismes du disque ouvert p-adique. A la différence de la construction dans ([Ma]), la géométrie du lieu de branchement est non équidistante et la combinatoire des points de branchement est un peu plus complexe. Les conducteurs utilisés sont eux aussi différents.

Enfin dans le chapitre 5, nous traitons le cas particulier où $p = 2$ et $G = (\mathbb{Z}/2\mathbb{Z})^2$. On a alors ce théorème :

Théorème 0.0.4 *Soit $G = (\mathbb{Z}/2\mathbb{Z})^2$ un groupe de k-automorphismes de $k[[z]]$. Alors on peut trouver R un anneau de valuation discrète dominant $W(k)$ tel que G se relève en un groupe de R-automorphismes de $R[[Z]]$.*

Le principe de la démonstration consiste à donner des équations explicites du relèvement.

Une partie de ces résultats se trouve dans un article en cours de publication (cf. [Pa]). Cet article se concentrait sur les cas où la géométrie du lieu de branchement est équidistante, ce qui nécéssitait en particulier l'étude des espaces $L_{m+1,n}$. Il nous a semblé préférable, dans la rédaction de la thèse, de ne pas séparer ce cas des autres, et donc de fondre l'article dans le reste de la thèse.

Chapitre 1

Déformation de courbes avec groupe d'automorphismes

Dans ce premier chapitre, nous rappelons quelques résultats qui seront utilisés au cours des démonstrations à venir. Le résultat le plus utile pour nous sera le Théorème 1.4.2 qui donne un critère exploitable pour déterminer si une action de $(\mathbb{Z}/p\mathbb{Z})^2$ sur $k[[z]]$ se relève en caractéristique zéro.

1.1 Un théorème local-global

Soient k un corps algébriquement clos de caractéristique $p > 0$ et R un anneau de valuation discrète dominant l'anneau des vecteurs de Witt $W(k)$ du corps k. On note K le corps des fractions de R et π une uniformisante de R. On suppose de plus que R contient une racine p-ième de l'unité ζ (que l'on fixe une fois pour toute), et on note $\lambda := \zeta - 1$.

On note (C, G) le couple formé d'une courbe C propre et lisse sur k, et de G un sous-groupe fini de $\mathrm{Aut}_k(C)$. On se propose d'étudier la déformation en caractéristique 0 de ce couple.

Définition 1.1.1 (Relèvement global) *On appelle relèvement sur R du couple (C, G) la donnée d'un couple $(\mathcal{C}, i : G \to \mathrm{Aut}_R(\mathcal{C}))$ où $\mathcal{C}$ est une courbe propre et lisse sur R telle que $\mathcal{C} \times_R k$ est isomorphe à C, et tel que $i : G \to \mathrm{Aut}_R(\mathcal{C})$ induise en réduction l'inclusion $G \to \mathrm{Aut}_k(C)$.*

Des obstructions au relèvement global existent : par exemple, si (C, G) ne vérifie pas l'inégalité de Hurwitz $|G| \leq 84(g(C) - 1)$, il n'y a pas de relèvement possible.

On se propose maintenant d'étudier les obstructions locales au relèvement. On se donne $(\mathcal{C}, G)$ un relèvement sur R de (C, G) et un point fermé $x \in \mathcal{C}$; la courbe $\mathcal{C}$ étant lisse, le complété de l'anneau local $\mathcal{O}_{\mathcal{C},x}$ est isomorphe à $R[[Z]]$ et donne en réduction $k[[z]]$, i.e le complété de l'anneau $\mathcal{O}_{C,x}$ (z désigne ici un paramètre uniformisant en x). Soit $I_x = \{\sigma \in G \subset \mathrm{Aut}_k(C), \sigma(x) = x\}$, le groupe d'inertie de G en x qui est alors un groupe de

k-automorphismes de $k[[z]]$. L'existence du relèvement $(\mathcal{C}, G)$ permet d'écrire $I_x = \{\sigma \subset G \in \mathrm{Aut}_k(\mathcal{C}), \sigma(x) = x\}$ qui est aussi un groupe de R-automorphismes de $R[[Z]]$. On est ainsi amené à considérer la condition de relèvement local.

Définition 1.1.2 (Relèvement local) *Soit G un groupe fini et $f : G \to \mathrm{Aut}_k k[[z]]$ un morphisme de groupes injectif. Nous dirons que f a la propriété de relèvement local si on a un diagramme commutatif :*

$$\begin{array}{ccc} \mathrm{Aut}_k(k[[z]]) & \longleftarrow & \mathrm{Aut}_k(R[[Z]]) \\ & \nearrow & \uparrow f \\ & & G \end{array}$$

On peut maintenant énoncer le principe local-global.

Théorème 1.1.3 (Principe Local-Global) *Soit $\overline{f} : Y \longrightarrow X$ un morphisme séparable fini entre courbes algébriques sur k, connexes, affines, réduites. Soit x un point fermé de X et X' l'ouvert complémentaire du point x. On suppose X' lisse sur k, $\overline{f}$ étale au-dessus de X' et l'image réciproque de x réduite à un point fermé y. On se place dans le cas particulier où x (resp. y) est un point lisse de X (resp. Y).*

Soit $\mathcal{X}$ un schéma formel affine normal, plat et topologiquement de type fini sur R, de fibre spéciale X. On note $\mathcal{X}'$ l'ouvert de $\mathcal{X}$ correspondant à X'. La restriction de $\overline{f}$ au-dessus de X' s'étend de façon unique (à isomorphisme près) en un revêtement étale $f' : \mathcal{Y}' \longrightarrow \mathcal{X}'$.

On se donne une $\hat{\mathcal{O}}_{\mathcal{X},x}$-algèbre A finie, normale, R-plate et un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \pi A & \longrightarrow & A & \longrightarrow & \hat{\mathcal{O}}_{Y,y} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \pi\hat{\mathcal{O}}_{\mathcal{X},x} & \longrightarrow & \hat{\mathcal{O}}_{\mathcal{X},x} & \longrightarrow & \hat{\mathcal{O}}_{X,x} & \longrightarrow & 0. \end{array}$$

i) Il existe alors un revêtement fini $f : \mathcal{Y} \longrightarrow \mathcal{X}$ relevant $\overline{f}$ tel que $\mathcal{Y}$ est normal, $f_{|\mathcal{X}'} = f'$ et f induit l'extension $\hat{\mathcal{O}}_{\mathcal{X},x} \longrightarrow A$.

ii) Si de plus $\overline{f}$ est galoisien de groupe de Galois G, et si A est munie d'une action de G de sorte que $A^G = \hat{\mathcal{O}}_{\mathcal{X},x}$ et que l'homomorphisme de R-algèbres $A \longrightarrow \hat{\mathcal{O}}_{Y,y}$ soit G-équivariant, le revêtement $f : \mathcal{Y} \longrightarrow \mathcal{X}$ est galoisien , de groupe de Galois G, relevant l'action sur Y.

Pour la démonstration de ce résultat on renvoie à [He2] (Théorème 2.8). On peut également montrer ce principe local-global par des techniques de géométrie rigide (voir [Gr-Ma 1]) ou par des méthodes cohomologiques (voir [Be-Me]).

1.2 Un critère local de bonne réduction

Soit σ un automorphisme d'ordre fini n de $R[[Z]]$ qui n'induit pas l'identité résiduellement (i.e le groupe d'inertie en (π) est différent de $<\sigma>$). On prouve alors que $R[[Z]]^{\sigma} = R[[T]]$ avec $T := Z\sigma(Z)\cdots\sigma^{n-1}(Z)$ (cf. Claim 3.1 dans [Gr-Ma 1]). Notons d_η (resp. d_s) le degré de la différente générique (resp. spéciale) de l'extension $R[[Z]]/R[[T]]$. On a alors $d_\eta = d_s$ (cf. Claim 3.2 dans [Gr-Ma 1]). On peut également énoncer une réciproque :

Théorème 1.2.1 (Critère de bonne réduction) *Soit $A := R[[T]]$ et B un A-module fini qui est en même temps un anneau local intégralement clos. Posons $K :=Frac(R)$, $A_K := A \otimes_R K$, $B_K := B \otimes_R K$, $A_0 := A/\pi A$ et $B_0 := B/\pi B$. Supposons que B_0 est réduit et que l'extension B_0/A_0 est génériquement étale. Soit $\tilde{B}_0$ la clôture intégrale de B_0 et $\delta_k(B) :=dim_k \tilde{B}_0/B_0$. Soit d_η (resp. d_s) le degré de la différente de l'extension B_K/A_K (resp. B_0/A_0). Alors $d_\eta = d_s + 2\delta_k(B)$; de plus si $d_\eta = d_s$ on a $\delta_k(B) = 0$ et B est de la forme $R[[Z]]$.*

Pour une démonstration de ce résultat, on renvoie à [Gr-Ma 1] (paragraphe I.3.4).

1.3 Réduction des μ_p-torseurs et variation de la différente

La proposition qui suit est un outil essentiel pour les démonstrations à venir ; nous renvoyons à [He1] pour un exposé plus complet.

Soit n un entier strictement positif, on note $\mathcal{G}_n$ le schéma en groupes $\mathrm{Spec}R\left[X, 1/1+\pi^n X\right]$ dont la fibre générique est isomorphe au groupe multiplicatif et la fibre spéciale s'identifie au groupe additif. Pour $0 < n \leq v_K(\lambda)$, le polynôme $((\pi^n X+1)^p - 1)/\pi^{pn}$ est à coefficients dans R, ce qui permet de considérer l'homomorphisme :

$$\Psi_n : R\left[Y, \frac{1}{\pi^{pn}Y+1}\right] \longrightarrow R\left[X, \frac{1}{\pi^n X+1}\right],$$

défini par $\Psi_n(Y) = ((\pi^n X+1)^p - 1)/\pi^{pn}$. Soit $\mathcal{H}_n$ le noyau de Ψ_n. Le schéma $\mathcal{H}_n$ est fini, plat sur R, de degré p. Sa fibre générique est isomorphe au groupe $\mu_{p,K}$. Si $0 < n < v_K(\lambda)$, sa fibre spéciale est le groupe radiciel $\boldsymbol{\alpha}_p$ et si $n = v_K(\lambda)$, sa fibre spéciale est le groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 1.3.1 *Soit $\mathcal{X} :=SpecA$ un schéma affine plat sur R, dont les fibres sont intègres et de dimension 1 ; on suppose que A est une R-algèbre factorielle et complète pour la topologie π-adique. Soit $\mathcal{Y}_K \longrightarrow \mathcal{X}_K$ un μ_p-torseur étale non trivial, donné par une équation $y^p = f$, où f est inversible dans A_K, et $\mathcal{Y}$ le normalisé de $\mathcal{X}$ dans $\mathcal{Y}_K$; on suppose que la fibre spéciale de $\mathcal{Y}$ est intègre. Soit η (resp. η') le point générique de la fibre spéciale de $\mathcal{X}$ (resp. $\mathcal{Y}$). Les anneaux locaux $\mathcal{O}_{\mathcal{X},\eta}$ et $\mathcal{O}_{\mathcal{Y},\eta'}$ sont alors des anneaux de valuation discrète d'uniformisante π. Notons δ la valuation de la différente de $\mathcal{O}_{\mathcal{Y},\eta'}/\mathcal{O}_{\mathcal{X},\eta}$. On distingue alors deux cas suivant la valeur de δ.*

- *Si $\delta = v_K(p)$, $\mathcal{Y}$ est un $\mu_{p,R}$-torseur pour la topologie fppf, donc $\mathcal{Y} = \mathrm{Spec}B$, avec $B := A[Y]/(Y^p - u)$, où U est une unité de A, unique à la multiplication d'une puissance p-ième d'une unité de A près.*

  On dit dans ce cas que le torseur a réduction ***multiplicative.***

- *Si $0 \leq \delta < v_K(p)$, on a $\delta = v_K(p) - n(p-1)$, où n est un entier tel que $0 < n(p-1) \leq v_K(p)$, et $\mathcal{Y} \longrightarrow \mathcal{X}$ est un torseur sous $\mathcal{H}_n$ pour la topologie fppf, donc donné par*

$$B := \frac{A[W]}{\frac{(\pi^n W+1)^p-1}{\pi^{pn}} - u}$$

  où u est un élément de A. De plus, si B est isomorphe à

$$\frac{A[W]}{\frac{(\pi^n W+1)^p-1}{\pi^{pn}} - u'}$$

  il existe $v \in A$ tel que $u' = u(\pi^n v + 1)^p + ((\pi^n v + 1)^p - 1)/\pi^{pn}$.

  Si $0 < \delta < v_K(p))$ (resp. $\delta = 0$), on dit que le torseur $\mathcal{Y} \longrightarrow \mathcal{X}$ a réduction ***additive*** *(resp.* ***étale****).*

Soit D_0 :=Spec$R[[Z]]$ le disque ouvert p-adique et σ un automorphisme d'ordre p du disque. On suppose que les points fixes de σ sont rationnels sur K et en nombre supérieur ou égal à deux. Il existe alors un modèle semi-stable minimal $\mathcal{D}_0$ de D_K qui déploie les spécialisations des points fixes en des points lisses et distincts. La fibre spéciale de ce modèle est un arbre de droites projectives se croisant en des points doubles ordinaires, relié à la stransformée stricte E_∞ du point générique de la fibre spéciale de D_0. On oriente cet arbre à partir de E_∞ et on montre que les spécialisations des points fixes se situent 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 (par la suite, on parlera de l'arbre $\mathcal{D}'_{0,s}$ pour désigner la fibre spéciale de $\mathcal{D}'_0$).

Soit Z_0 un point fixe de σ. Pour $\rho \in R^{\mathrm{alg}}$, on note v_ρ la valuation de Gauss sur Frac$R[[Z]]$ relative au paramètre $(Z - Z_0)/\rho$ et $d(v(\rho))$ la valuation de la différente de l'extension (Frac$R[[Z]]$)/(Frac$R[[Z]]$)$^{<\sigma>}$ pour la valuation v_ρ. Le graphe de $d(v(\rho))$ est une courbe affine par morceaux. Considérons un intervalle de la forme $[v(\rho_1), v(\rho_2)]$ sur lequel $d(v(\rho))$ est affine ; la pente du graphe sur cet intervalle est égale à $(p-1)(\mu - 1)$ (où μ désigne le nombre de points fixes Z_i tels que $v(Z_i - Z_0) \geq v(\rho_2)$).

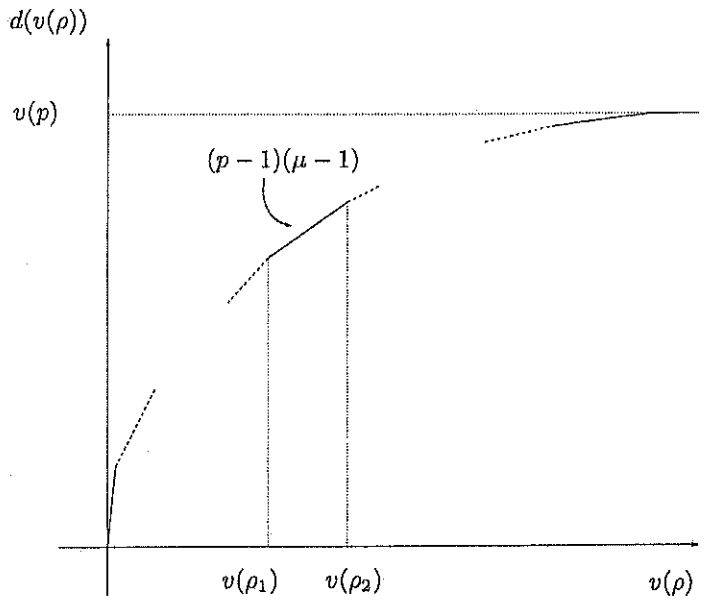


FIG. 1.1 – Graphe de la différente

Partons toujours d'un point fixe Z_0 de σ. L'action de σ sur l'espace tangent est donné par la multiplication par une racine p-ième de l'unité qui s'écrit $\zeta^{h_0^{-1}}$. L'entier $h_0 \in \mathbb{F}_p^*$ est appelé donnée d'Hurwitz en Z_0. On peut associer à chaque composante de la fibre spéciale $\mathcal{D}'_{0,s}$ des données différentielles. Ceci est l'objet du théorème suivant (cf. Théorème III.2.1 de [Gr-Ma 2]) :

Théorème 1.3.2 *a) Soit E_i une composante terminale de $\mathcal{D}'_{0,s}$ et m_i+1 le nombre de points fixes se spécialisant sur E_i. On note $t_{i,j}$ ces spécialisations et $h_{i,j}$ la donnée d'Hurwitz correspondante. Alors il existe une fraction rationnelle $\overline{u}_i \in k(E_i)$, unique à multiplication par une puissance p-ième près, telle que le diviseur de la forme différentielle $\omega_i := \mathrm{d}\overline{u}_i/\overline{u}_i$ soit égal à :*

$$(m_i-1)[\infty] - \sum_{j=1}^{m_i+1}[t_{i,j}]$$

et le résidu en $t_{i,j}$ de ω_i vaut $h_{i,j}$.

b) Soit P_α une composante interne de $\mathcal{D}'_{0,s}$. On note $t_{\alpha,n}$ $(1 \leq n \leq n_\alpha)$ ses points d'intersection. A chaque point $t_{\alpha,n}$ on associe l'ensemble des composantes terminales E_i, indexé par $i \in I_n$, qui sont reliées à $t_{\alpha,n}$ par un chemin positif. On pose $m_{\alpha,n}+1 = \sum_{i\in I_n}(m_i+1)$. Alors il existe une fraction rationnelle $\overline{u}_\alpha \in k(P_\alpha)$, unique à l'addition d'une puissance p-ième près, telle que le diviseur de la forme différentielle $\omega_\alpha := \mathrm{d}\overline{u}_\alpha$ soit égal à :

$$((\sum_{n=1}^{n_\alpha}(m_\alpha+1)) - 2)[\infty] - \sum_{n=1}^{n_\alpha}[t_{\alpha,n}].$$

La démonstration de ce théorème s'effectue en analysant la dégénérescence des μ_p-torseurs induits par σ sur le disque fermé correspondant à chaque composante (on utilise notamment la Proposition 1.3.1).

1.4 Un critère de relèvement pour les actions de $(\mathbb{Z}/p\mathbb{Z})^2$

Considérons une action de $G := (\mathbb{Z}/p\mathbb{Z})^2$ sur le disque $\mathrm{Spec}R[[Z]]$; elle induit un $(\mu_p \times \mu_p)$-torseur au-dessus du disque ouvert p-adique $\mathrm{Spec}R[[T]]$ qui est donné génériquement par deux équations :

$$\begin{cases} Y_1^p &= U_1(T)F_1(T) \\ Y_2^p &= U_2(T)F_2(T) \end{cases}$$

où U_1, U_2 sont des unités de $R[[T]]$ et $F_1, F_2 \in R[T]$ (ceci est une conséquence immédiate du théorème de préparation de Weierstrass). Nous allons voir que, dans le cas où cette action induit modulo π un torseur sous $(\mathbb{Z}/p\mathbb{Z})^2$, il est possible de "supprimer" les unités U_1, U_2 dans les équations (cela sera utilisé dans la démonstration de la Proposition 3.2.7). Une façon de procéder est de compactifier l'action de G sur $R[[Z]]$ en une action de G sur une courbe propre et lisse sur R, afin d'obtenir des équations globales. Plus précisément :

Proposition 1.4.1 *Soit $G := (\mathbb{Z}/p\mathbb{Z})^2$, et $k[[z]]/k[[z]]^G := k[[t]]$ une extension galoisienne de groupe G. Supposons que l'action de G se relève en une action sur $R[[Z]]$ (on note $R[[T]] := R[[Z]]^G$). Alors il existe un G-revêtement $\mathcal{Y} \longrightarrow \mathcal{X} = \mathbb{P}^1_R$, où $\mathcal{Y}$ est une courbe propre et lisse sur R, vérifiant les propriétés suivantes :*

- *$\mathcal{Y} \longrightarrow \mathcal{X}$ a bonne réduction modulo π. On note Y (resp. X) la fibre spéciale de $\mathcal{Y}$ (resp. $\mathcal{X}$).*
- *Le revêtement $Y \longrightarrow X$ est étale en dehors de l'infini, et totalement ramifié à l'infini.*
- *Le revêtement $\mathrm{Spec}\hat{\mathcal{O}}_{\mathcal{Y},\infty} \longrightarrow \mathrm{Spec}\hat{\mathcal{O}}_{\mathcal{X},\infty}$ est isomorphe à $\mathrm{Spec}R[[Z]] \longrightarrow \mathrm{Spec}R[[T]]$.*

Le revêtement $\mathcal{Y} \longrightarrow \mathcal{X}$ est alors donné génériquement par des équations :

$$\begin{cases} Y_1^p &= \tilde{F}_1(T) \\ Y_2^p &= \tilde{F}_2(T) \end{cases}$$

où $\tilde{F}_1, \tilde{F}_2$ sont deux polynômes.

Démonstration : Soit G_1 et G_2 deux sous-groupes distincts de G d'ordre p. Les extensions $R[[Z]]^{G_1}/R[[Z]]^G$ et $R[[Z]]^{G_2}/R[[Z]]^G$ donnent en réduction modulo π les extensions $k[[z]]^{G_1}/k[[t]]$ et $k[[z]]^{G_1}/k[[t]]$. Posons $s := 1/t$. L'extension $k[[z]]/k[[t]]$ est donnée par deux équations :

$$\begin{cases} x_1^p - x_1 &= q_1(s) \\ x_2^p - x_2 &= q_2(s) \end{cases}$$

où q_1, q_2 sont deux polynômes tels que $\deg(q_i, p) = 1$. Ces équations induisent un G-revêtement de $\mathbb{P}^1_k$ (que l'on écrit $\overline{f} : Y \longrightarrow X := \mathbb{P}^1_k$) qui est étale en dehors du point $s = \infty$ et totalement ramifié en ce point. La restriction $\overline{f}$ à $X' := X - \{\infty\} = \mathbb{A}^1_k$ s'étend donc de façon unique en un revêtement étale $f' : \mathcal{Y}' \longrightarrow \mathcal{X}'$. On peut alors appliquer le Théorème 1.1.3 (avec $A := R[[Z]]$) et en déduire l'existence d'un revêtement $f : \mathcal{Y} \longrightarrow \mathcal{X} := \mathbb{P}^1_R$ qui vérifie les conditions données dans la proposition.

□

Remarque : Cette proposition reste encore valable si on considère un p-groupe G quelconque. En effet, en appliquant le Théorème 2.1.4 dans [Ka], on peut toujours étendre l'action de G en un revêtement galoisien de $\mathbb{P}^1_k$, de groupe de Galois G, pour lequel G est le groupe d'inertie à l'infini. On conclut ensuite en appliquant le Théorème 1.1.3.

Nous rappelons maintenant le Théorème I.5.1 de [Gr-Ma 1] qui fournit une condition nécessaire et suffisante pour déterminer si une action de $(\mathbb{Z}/p\mathbb{Z})^2$ sur $k[[z]]$ se relève en une action sur $R[[Z]]$.

Théorème 1.4.2 *Soit $G := (\mathbb{Z}/p\mathbb{Z})^2$ et G_i, $1 \leq i \leq p+1$, les $p+1$ sous-groupes d'ordre p de G. Supposons que G soit un groupe de k-automorphismes de $k[[z]]$. Quitte à renuméroter les G_i, on peut supposer que les extensions $k[[z]]^{G_i}/k[[z]]^G$ ont pour conducteur m_i avec $m_1 \leq \cdots \leq m_{p+1}$. On note m_i' le conducteur de l'extension $k[[z]]/k[[z]]^{G_i}$. Alors si G se relève en un groupe de R-automorphismes de $R[[Z]]$, deux cas sont à envisager :*

a) Premier cas : On a $m_1 < m_2$. Alors $m_1 + 1 \equiv 0 \ mod\ p$, $m_1' = m_2 p - m_1(p-1)$, $m_i = m_2$, et $m_i' = m_1$ pour $2 \leq i \leq p+1$.

b) Deuxième cas : On a $m_1 = m_2$. Alors $m_i = m_1 \equiv -1 \ mod\ p$, et $m_i' = m_1$ pour $1 \leq i \leq p+1$.

Dans les deux cas les deux revêtements $R[[Z]]^{G_1}/R[[Z]]^G$ et $R[[Z]]^{G_2}/R[[Z]]^G$ ont exactement $(p-1)(m_1+1)/p$ points de branchement géométriques en commun.

Inversement, si $m_1 + 1 \equiv 0 \ mod\ p$, et si on peut relever $k[[z]]^{G_1}/k[[z]]^G$ et $k[[z]]^{G_2}/k[[z]]^G$ de telle sorte que les revêtements correspondants aient $(p-1)(m_1+1)/p$ points de branchement géométriques en commun, alors la normalisation du compositum des deux extensions $R[[Z]]^{G_1}/R[[Z]]^G$ et $R[[Z]]^{G_2}/R[[Z]]^G$ relève $k[[z]]/k[[z]]^G$.

La démonstration de ce théorème s'appuie sur le Théorème 1.2.1. On écrit l'égalité des degrés des différentes génériques et spéciales (d_η et d_s), et le calcul de d_η fait alors intervenir le nombre de points de branchements communs aux revêtements Rev_1 et Rev_2.

Ce théorème est crucial. Dans la suite, on se ramènera systématiquement à la condition du Théorème 1.4.2 pour relever des actions de $(\mathbb{Z}/p\mathbb{Z})^2$ ou pour exhiber des obstructions.

Chapitre 2

Espaces de formes différentielles logarithmiques $L_{m+1,n}$ et $L^{j}_{qp,2}$

Soit $p > 2$ un nombre premier et $G := (\mathbb{Z}/p\mathbb{Z})^2$. On suppose que G est un groupe de R-automorphismes du disque ouvert p-adique $D_0 := \mathrm{Spec}R[[Z]]$. Le revêtement $\mathrm{Spec}R[[Z]] \to \mathrm{Spec}R[[Z]]^G$ possède $p+1$ revêtements intermédiaires de degré p. L'objet de cette première partie est de classifier les $\mathbb{F}_p$-espaces vectoriels de formes différentielles logarithmiques qui apparaissent dans les bouts de l'arbre correspondant au modèle semi-stable minimal qui déploie les points de branchement de chacun de ces revêtements.

Le cas $p = 2$ sera traité à part (cf. chapitre 5) et par d'autres méthodes. En effet, dans ce cas, certains des résultats énoncés dans cette partie ne sont plus valides (notamment la Proposition 2.1.2). Néanmoins, nous indiquerons quelques résultats relatifs au cas $p = 2$ (cf. Théorème 2.2.4).

2.1 Etude des actions de $(\mathbb{Z}/p\mathbb{Z})^2$ sur le disque ouvert p-adique

Soit p un nombre premier et $G := (\mathbb{Z}/p\mathbb{Z})^2$. On suppose que G est un groupe de R-automorphismes du disque ouvert p-adique $D_0 := \mathrm{Spec}R[[Z]]$. D'après ([Gr-Ma 1]), un des revêtements a $m_1 + 1$ points de branchement ($m_1 + 1 \in p\mathbb{Z}$) et les p autres revêtements ont $m_2 + 1$ points de branchement ($m_2 \geq m_1$). Nous allons décrire la combinatoire du lieu de branchement et montrer que les points de branchement se répartissent en $p+1$ paquets de points. Plus précisément on a le lemme suivant :

Lemme 2.1.1 *Supposons que l'un des revêtements intermédiaires de degré p a m_1+1 points de branchement ($m_1+1 \in p\mathbb{Z}$) et que les p autres revêtements ont m_2+1 points de branchement ($m_2 \geq m_1$). On écrit $m_1+1 = pq$. Alors il y a $(p+1)q+m_2-m_1$ points de branchement se répartissant en p paquets de q points (notés $S_0, \cdots, S_{p-1}$) et un paquet de $m_2 - m_1 + q$*

points noté S_p de sorte que le lieu de branchement du i-ème revêtement intermédiaire de degré p (noté Br_i) est :

$$Br_i = \coprod_{\substack{j=0 \\ j\neq i}}^{p} S_j \quad \text{pour } 0 \leq i \leq p.$$

Démonstration : On prend deux revêtements intermédiaires Rev_0 et Rev_p, Rev_p ayant m_1+1 points de branchement. On note m_1+1-n le nombre de points de branchement communs à Rev_0 et Rev_p. Les équations de ces deux revêtements sont de la forme :

$$Y_p^p = u(X)\prod_{j=0}^{m_1}(X-X_j)^{\alpha_j} \quad Y_0^p = v(X)\prod_{j=n}^{m_2+n}(X-X_j)^{\beta_j}$$

avec u, v des unités de $R[[X]]$, $\alpha_j, \beta_j \neq 0 \bmod p$ et $\sum_{j=0}^{m_1}\alpha_j = \sum_{j=n}^{m_2+n}\beta_j = 0 \bmod p$. On pose $\alpha_j = 0$ si $j \geq m_1+1$ et $\beta_j = 0$ si $j \leq n-1$. Le i-ème revêtement intermédiaire Rev_i s'écrit :

$$Y_i^p = u(X)^i v(X)\prod_{j=0}^{m_2+n}(X-X_j)^{i\alpha_j+\beta_j}$$

pour $1 \leq i \leq p-1$, et donc $i\alpha_j + \beta_j = 0$ pour exactement n valeurs de j. Il vient donc $m_1+1-n = (p-1)n$, i.e $n = q$.

Notons S_i l'ensemble des points en lesquels Rev_i n'est pas ramifié. On obtient ainsi la répartition annoncée.

□

Soit F la réunion des points de branchement de Rev_i et $\mathcal{D}'_0$ le modèle minimal semi-stable qui déploie les points de F en des points lisses et distincts à la fibre spéciale (la construction de ce modèle est identique à celle qui déploie les points fixes d'un automorphisme d'ordre p).

Proposition 2.1.2 *Si $p > 2$ les spécialisations des points de F se trouvent dans les bouts de l'arbre $\mathcal{D}'_{0,s}$.*

Démonstration : On raisonne par l'absurde et on suppose que l'un des points de branchement (que l'on note X_1) se spécialise sur une composante interne P_α de l'arbre. Soient X_2 et X_3 deux points de branchement qui se spécialisent dans une même composante terminale située dans le sous-arbre d'origine P_α (voir la figure 2.1).

Comme $p \geq 3$, d'après le lemme précédent, le lieu de branchement se répartit en au moins quatre paquets de points S_j. Il existe donc un paquet qui ne contient aucun des X_i, i.e il existe un revêtement intermédiaire Rev_0 de degré p dont le lieu de branchement contient l'ensemble $\{X_1, X_2, X_3\}$. On note Br_0 le lieu de branchement de Rev_0. Alors l'arbre (noté A) qui déploie les spécialisations de Br_0 est obtenu à partir de $\mathcal{D}'_{0,s}$ en contractant

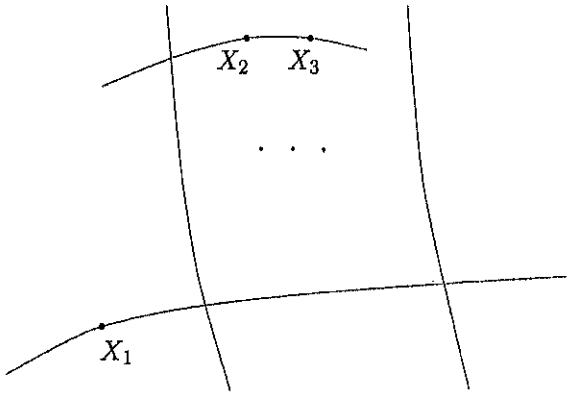


FIG. 2.1 –

éventuellement quelques composantes. De toute façon l'arbre A contient la composante P_α car dans A apparaît forcément la composante qui correspond au disque fermé de rayon minimal contenant X_1 et X_2. De plus P_α n'est pas une composante terminale car on ne peut pas contracter la composante qui porte X_2 et X_3. Le point X_1 est donc la spécialisation d'un point de branchement de Rev_0 qui ne se trouve pas sur une composante terminale, ce qui contredit la Proposition 1.2 dans [Gr-Ma 2].

□

Remarque : Pour $p = 2$ cette proposition n'est plus valable. On peut construire des exemples d'actions de $(\mathbb{Z}/2\mathbb{Z})^2$ dont le lieu de branchement n'a pas toutes ses spécialisations dans les bouts (voir le Théorème 5.2.1).

Nous allons maintenant décrire les espaces de formes différentielles logarithmiques existant sur les composantes terminales de $\mathcal{D}'_{0,s}$, ce qui nécessite quelques définitions préalables.

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 2.1.3 *On appelle espace $L_{m+1,n}$ 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 ∞.*

Définition 2.1.4 *Soit $j, q \in \mathbb{N}^*$ tels que $j \leq q$. On appelle $L^j_{qp,2}$ un $\mathbb{F}_p$-espace vectoriel de dimension deux engendré par ω_0 et ω_p, deux formes différentielles logarithmiques sur $\mathbb{P}^1_k$, telles que :*

- *ω_p a qp pôles distincts et un seul zéro d'ordre $qp-2$ en ∞.*
- *$\omega_0 + i\omega_p$ a $qp-j$ pôles distincts et un seul zéro d'ordre $qp-j-2$ en ∞ pour $0 \leq i \leq p-1$.*

Proposition 2.1.5 *On suppose $p > 2$. Soit E_i une composante terminale de $\mathcal{D}'_{0,s}$. Alors il existe un $\mathbb{F}_p$-espace vectoriel de formes différentielles logarithmiques sur la composante E_i qui est un $L_{qp,2}$, $L^j_{qp,2}$ ou un $L_{m+1,1}$.*

Démonstration : On distingue trois cas :

- Premier cas : Tous les revêtements intermédiaires d'ordre p ont le même nombre de points de branchement sur la composante E_i. Soient Rev_0 et Rev_p deux de ces revêtements. On note ω_0 (resp. ω_p) la forme différentielle logarithmique induite par Rev_0 (resp. Rev_p) sur E_i. Ces deux formes différentielles ont alors le même nombre de pôles et un unique zéro à l'infini. De plus pour chaque autre revêtement intermédiaire de degré p, la forme différentielle logarithmique induite sur E_i est $\omega_0 + j\omega_p$ (pour $1 \leq j \leq p-1$) et ces formes ont toujours le même nombre de pôles et un unique zéro à l'infini. On a donc un espace $L_{m+1,2}$ sur E_i. De plus, on verra par la suite que si un tel espace existe, alors $m+1 \in p\mathbb{Z}$ (voir Lemme 2.2.1). On a donc un espace $L_{qp,2}$ sur E_i (avec $q \in \mathbb{N}$).
- Deuxième cas : Tous les revêtements intermédiaires d'ordre p font apparaître la composante E_i dans la fibre spéciale de leur modèle minimal semi-stable, mais n'ont pas le même nombre de spécialisations sur cette composante. Soient Rev_0 et Rev_p deux revêtements intermédiaires d'ordre p avec respectivement n_1+1 et n_2+1 points de branchement sur E_i ($n_1 < n_2$). On note n_1+1-n le nombre de points de branchement communs à Rev_0 et Rev_p sur E_i et ω_0 (resp. ω_p) la forme différentielle logarithmique sur E_i induite par Rev_0 (resp. Rev_p). Ces formes différentielles s'écrivent :

$$\omega_0 = \frac{u\,\mathrm{d}x}{\prod_{j=0}^{n_1}(x-x_j)} \quad \text{et} \quad \omega_p = \frac{v\,\mathrm{d}x}{\prod_{j=n}^{n_2+n}(x-x_j)}$$

où $u, v \in k^*$. Les $(p-1)$ autres revêtements intermédiaires d'ordre p font apparaître les formes différentielles $\omega_0 + i\omega_p$ ($1 \leq i \leq p-1$). Comme $n_1 < n_2$, ces $(p-1)$ formes différentielles ont chacune n_1+1 pôles simples. Notons h_j (resp. h'_j) les résidus de ω_0 (resp. ω_p) au point x_j. Alors si $0 \leq i \leq p-1$ on a $h_j + ih'_j = 0$ pour exactement $n_2 - n_1 + n$ valeurs de j. On a donc :

$$\begin{aligned} n_2+1 &= p(n_2-n_1+n) \\ (n_2+1)(p-1) &= p(n_1+1-n) \\ n_2+1 &= p\left(\frac{n_1+1-n}{p-1}\right) \in p\mathbb{Z}. \end{aligned}$$

Posons $q := (n_1+1-n)/(p-1) \in \mathbb{Z}$ de sorte que $n_2+1 = qp$. On a alors $n_1+1-n = q(p-1)$, i.e $n_1+1 = q(p-1)+n$ avec $0 \leq n < q$ (puisque $n_1 < n_2$). En posant $j := q-n$ on voit apparaître un espace $L^j_{qp,2}$.

- Troisième cas : L'un des revêtements intermédiaire d'ordre p ne fait pas apparaître la composante P_i dans son modèle semi-stable minimal. A ce moment-là il apparaît des espaces $L_{m+1,1}$.

2.2 Etude des espaces $L_{m+1,n}$ et $L^j_{qp,2}$

L'objet de cette partie est de donner des résultats de type combinatoire sur ces espaces ainsi que des théorèmes d'existence dans les cas les plus simples (i.e pour $n = 2$ et pour les premières valeurs de $m+1$ et de q).

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

Nous commençons par exhiber quelques exemples d'espaces $L_{m+1,1}$ (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 $x_i \in k^*$, $x_i \neq x_j$, $h_i \in \mathbb{Z} - p\mathbb{Z}$, $\sum_{i=1}^{m+1} h_i = 0 \bmod p$. 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 $\deg(f') \equiv -1 \bmod p$, ce qui est impossible.

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

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

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

$$\begin{cases} \sum_{i=1}^{m+1} h_i x_i^{\ell} = 0 \qquad \text{pour} \quad 1 \leq \ell \leq m-1 \\ \prod_{i<j}(x_i - x_j) \neq 0 \\ x_i \in k,\ h_i \in \mathbb{Z} - p\mathbb{Z} \end{cases} \tag{2.1}$$

Remarque : 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 2.2.5, 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 [Hel] 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

$$\left(t - \frac{d_2-1}{d_2}\alpha\right)$$

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

$$z - x_1 = P_\alpha(t)\left(t - \frac{d_2-1}{d_2}\alpha\right)^2.$$

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 $x = 1/z$. En fait, chacune de ces deux écritures a son intérêt 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.

2.2.2 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 2.2.1 *Soit un espace vectoriel $L_{m+1,2}$; alors $m+1 \in p\mathbb{Z}$. De plus si on note (ω_0, ω_p) une base de cet espace, alors ces deux formes différentielles ont exactement $(m+1)(p-1)/p$ pôles en commun.*

Démonstration : Soit (ω_0, ω_p) une base de l'espace vectoriel en question. On note $(m+1-q)$ le nombre de pôles communs à ω_0 et ω_p (on a donc $0 \leq q \leq m+1$). On note $x_0, \cdots, x_m$ les pôles de ω_0, et $h_0, \cdots, h_m$ les résidus en ces pôles. De même pour ω_p, on les note $x_q, \cdots, x_{q+m}$ et $h'_q, \cdots, h'_{q+m}$ les résidus correspondants (on convient de poser $h_i = 0$ pour $i > m$ et $h'_i = 0$ pour $i < q$).

Soit $c \in \mathbb{P}^1(\mathbb{F}_p)$, $c = [a, b]$ (en coordonnées homogènes) ; alors $\omega := a\omega_0 + b\omega_p$ a exactement $m+1$ pôles. Donc, il existe exactement q valeurs de i pour lesquelles $ah_i + bh'_i = 0$. On a alors partitionné les $(m+1+q)$ points x_i en $p+1$ ensembles de q points. Ainsi $(m+1+q) = (p+1)q$ et $m+1 = qp$. On vérifie aisément que le nombre de pôles communs à ω_0 et ω_p est celui annoncé.

□

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

Lemme 2.2.2 *Considérons 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 $(m+1)(p-1)^{n-1}/p^{n-1}$ pôles en commun.*

Démonstration : 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 différentielles $(j < n)$ parmi les ω_i, ces j formes ont exactement $(m+1)(p-1)^{j-1}/p^{j-1}$ pôles en commun. Notons T le nombre total des pôles apparaissant dans les formes différentielles $\omega_1, \cdots, \omega_n$ et q le nombre de pôles communs à toutes ces différentielles. On note également $N_{i_1 i_2 \cdots i_r}$ le nombre de pôles communs aux formes différentielles $\omega_{i_1}, \cdots, \omega_{i_r}$. Alors, on a la relation :

$$T = \sum_{r=1}^{n} (-1)^{r+1} \sum_{i_1 < i_2 < \cdots < i_r} N_{i_1 i_2 \cdots i_r}$$

qui donne après simplifications :

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

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 :

$$a_1 h_{1,i} + \cdots + a_n h_{n,i} = 0$$

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 :

$$\frac{(m+1)(p-1)^{n-1}}{p^{n-1}} - q = 0.$$

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

□

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

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

Proposition 2.2.3 *Soit ω_0, ω_p deux formes différentielles sur $\mathbb{P}^1_k$. Alors $\mathbb{F}_p\omega_0 + \mathbb{F}_p\omega_p$ 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 :

$$\omega_0 = \frac{A\mathrm{d}z}{A^pB - AB^p} \quad \text{et} \quad \omega_p = \frac{B\mathrm{d}z}{A^pB - AB^p}$$

et $((A^p - AB^{p-1})^{p-1})^{(p-1)} = -1$.
(Dans cette dernière expression, l'exposant entre parenthèses désigne une dérivation et l'exposant sans parenthèses désigne une puissance).

Démonstration : Supposons que $\mathbb{F}_p\omega_0 + \mathbb{F}_p\omega_p$ est un $L_{m+1,2}$. On sait d'après le Lemme 2.2.1 que $m+1 = qp$ et que l'ensemble des pôles est partitionné en $p+1$ ensembles de q pôles. Plus précisément, on écrit que :

- ω_p a ses pôles en les points $x_0, \cdots, x_{qp-1}$
- ω_0 a ses pôles en les points $x_q, \cdots, x_{q(p+1)-1}$
- quitte à renuméroter, on peut supposer que $\omega_0 + i\omega_p$ (pour i variant de 1 à $p-1$) a des pôles en tous les x_j sauf pour $qi \leq j \leq q(i+1) - 1$.

On note $P_j(z) = \prod_{r=qj}^{q(j+1)-1}(z - x_r)$. Alors ω_0 et ω_p s'écrivent :

$$\omega_0 = \frac{uP_0(z)\mathrm{d}z}{\prod_{j=0}^{p} P_j(z)}, \quad \omega_p = \frac{vP_p(z)\mathrm{d}z}{\prod_{j=0}^{p} P_j(z)}$$

où u et v sont des constantes non nulles.

On a alors deux écritures pour $\omega_0 + i\omega_p$:

$$\omega_0 + i\omega_p = \frac{(uP_0(z) + ivP_p(z))\mathrm{d}z}{\prod_{j=0}^{p} P_j(x)} = \frac{(w_i P_i(z))\mathrm{d}z}{\prod_{j=0}^{p} P_j(z)}$$

où w_i est une constante non nulle.
On a donc $uP_0(z) + ivP_p(z) = w_i P_i(z)$. 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 u/v n'est pas dans $\mathbb{F}_p$. En effet, si $u/v = -i \in \mathbb{F}_p$, 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 $a = u/v$. Alors :

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

et

$$\omega_0 = a\omega_p \frac{P_0}{P_p} = \frac{v(a^p - a)}{(aP_0)^{p-1}P_p - P_p^p}\mathrm{d}z.$$

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 :

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

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

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

sont logarithmiques. Pour traduire cette condition, on peut utiliser 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 :

$$\omega = (f_0^p(z) + z f_1^p(z) + \cdots + z^{p-1} f_{p-1}^p(z))\mathrm{d}z.$$

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_0 est logarithmique" et "ω_p est logarithmique" sont équivalentes.

Supposons en effet que $B\mathrm{d}z/(A^pB - AB^p)$ 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 :

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

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

On peut donc résumer ces conditions en disant que :

$$((A^p - AB^{p-1})^{p-1})^{(p-1)} = -1. \tag{2.2}$$

Inversement si on a :

$$\omega_0 = \frac{A\mathrm{d}z}{A^pB - AB^p} \quad \text{et} \quad \omega_p = \frac{B\mathrm{d}z}{A^pB - AB^p}$$

avec A,B vérifiant les conditions de la proposition, on montre facilement que les formes $i\omega_0 + j\omega_p$ (pour $(i,j) \neq (0,0)$) sont logarithmiques et n'ont qu'un seul zéro d'ordre $(m-1)$ en ∞.

□

Remarque 1 : L'équation différentielle (2.2) est difficile à manipuler. En effet, si on la développe, il apparaît des dérivées r-ièmes de puissances de A, A étant lui-même de degré q (la résolution n'apparaît simple que dans le cas où $q = 1$ ou $p = 2$).

On peut donner une autre formulation de la condition (2.2) en termes de congruence : puisque $f := A^p - AB^{p-1} \in k[z]$, ω_0 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 2.2.2. On note P un polynôme qui n'a que des racines simples, ces racines étant les pôles des formes différentielles ω_i. Alors chaque forme

ω_i peut s'écrire $\omega_i = Q_i/P\mathrm{d}z$ 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 reconnaît 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 $\omega_i = Q_i/P\mathrm{d}z$; 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 $\Phi : \mathbb{P}^1_k \longrightarrow \mathbb{P}^1_k$ 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 $\mathbb{P}^1_k - \{\infty\}$). Si F est un $L_{m+1,n}$ engendré par les formes différentielles $\omega_1, \cdots, \omega_n$ (avec $\omega_i = \mathrm{d}f_i/f_i$) 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 $\mathrm{d}(f_i \circ \Phi)/(f_i \circ \Phi)$).

2.2.4 Les espaces $L_{m+1,2}$

A défaut de pouvoir exploiter la condition (2.2) décrite ci-dessus, nous allons explorer les relations algébriques entre pôles et résidus.

Nous allons d'abord régler le cas $p = 2$. Ce dernier apparaît comme un cas particulier dans la mesure où toutes les données d'Hurwitz sont égales à 1.

Théorème 2.2.4 *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 $f_0(z) = \prod_{i=1}^n (z - x_i)(z - y_i)$ 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 $\omega_0 := \mathrm{d}f_0/f_0$ et $\omega_2 := \mathrm{d}f_2/f_2$ soient de la forme :

$$\omega_0 = \frac{u\,\mathrm{d}z}{\prod_{i=1}^n (z - x_i)(z - y_i)} \quad \text{et} \quad \omega_2 = \frac{v\,\mathrm{d}z}{\prod_{i=1}^n (z - x_i)(z - z_i)}.$$

Ainsi $\mathbb{F}_2\omega_0 + \mathbb{F}_2\omega_2$ est un $L_{m+1,2}$.

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

<u>*Démonstration*</u> : Vu la forme demandée pour ω_0, il faut que $f_0' = u$ et donc que f_0 soit de la forme :

$$f_0 = (q(z))^2 + uz \tag{2.3}$$

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 $f_0(x_i) = (q(x_i))^2 + ux_i = 0$ ce qui donne le système :

$$\begin{cases} x_1^n + q_1 x_1^{n-1} + \cdots + q_n &= \sqrt{ux_1} \\ \qquad\qquad \vdots & \\ \qquad\qquad \vdots & \\ x_n^n + q_1 x_n^{n-1} + \cdots + q_n &= \sqrt{ux_n}. \end{cases}$$

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 $f_0'(z) = u$, f_0 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 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.

□

Dès que $p > 2$ la situation devient beaucoup plus compliquée. On peut malgré tout énoncer le théorème suivant :

Théorème 2.2.5 *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 considérera donc à chaque fois un espace vectoriel répondant au problème. Soit z un paramètre de $\mathbb{P}^1_k - \{\infty\}$ tel que $z = 0$ n'est pas pôle de ω_0 et ω_p. On utilise alors dans la démonstration le paramètre $x := 1/z$.

Le cas $m+1 = p$.

On note toujours (ω_0, ω_p) une base d'un espace vectoriel $L_{m+1,2}$. Ces deux formes s'écrivent :

$$\omega_0 = \frac{\mathrm{d}f_0}{f_0} = \sum_{i=0}^{p} \frac{h'_i x_i}{1 - x_i x}\mathrm{d}x, \quad h'_0 = 0,\ h'_i \neq 0 \text{ si } i \neq 0,\ \sum_i h'_i \equiv 0 \bmod p$$

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

et tous les x_i sont distincts.

La forme ω_0 s'écrit aussi :

$$\omega_0 = \frac{u x^{p-2}}{\prod_{i=1}^{p}(1 - x_i x)}\mathrm{d}x \quad \text{avec } u \neq 0.$$

En identifiant les termes en x^r des développements formels des deux expressions de ω_0, on trouve que :

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

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_p, 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 2.2.1 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 peut supposer que :

- $\omega_0 + i\omega_p$ 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 :

$$\omega_0 = \sum_{i=0}^{p} \left(\frac{h'_i x_i}{1 - x_i x} + \frac{k'_i y_i}{1 - y_i x} \right) \mathrm{d}x \quad \text{avec } h'_0 = k'_0 = 0$$

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

Étape 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 2.2.3, les relations suivantes :

$$s_i = \frac{a s_0 + i s_p}{a + i} \quad \text{et} \quad p_i = \frac{a p_0 + i p_p}{a + i}$$

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 $(a+i)s_i = a s_0 + i s_p$. ⌟

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

Étape 2 :Montrons par récurrence sur ℓ que :

$$\sum_{i=0}^{p-1} p_i^\ell A_i(r) = 0 \quad 0 \leq r \leq 2p - 2 - 2\ell.$$

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

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

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

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

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

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

et

$$\sum_{i=0}^{p-1} s p_i^\ell A_i(r+1) = 0.$$

Donc :

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

⌟

On aboutit donc à :

$$\sum_{i=0}^{p-1} p_i^\ell A_i(0) = 0 \quad \text{pour} \quad 1 \leq \ell \leq p-1 \tag{2.4}$$

$$\sum_{i=0}^{p-1} p_i^\ell A_i(1) = 0 \quad \text{pour} \quad 1 \leq \ell \leq p-2. \tag{2.5}$$

Étape 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 $p_i = p_p + a(p_0 - p_p)/(a+i) = b + c/(a+i)$ en posant $b = p_p$ et $c = a(p_0 - p_p) \neq 0$. Le système (2.4) implique en particulier que :

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

Posons $F(X) = \sum_{i=0}^{p-1} A_i(0)/(X+i)$. 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 (2.5) implique que :

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

Posons $G(X) = \sum_{i=0}^{p-1} A_i(1)/(X+i)$. 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 :

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

⌟

En résumé, on a :

- $A_i(0) = 0$ donc $k_i = -h_i$.
- $s_i = 0$, après translation éventuelle sur les x_i, y_i. En particulier $x_i \neq 0$.
- $A_i(1) = 2h_i x_i = \beta(i+a)^{p-2}$

On a donc un système :

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

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

$$H(X) := \left(\frac{\beta}{2}\right)^{p-1} (X+a)^{(2p-3)(\frac{p-1}{2})} - (-1)^{\frac{p-1}{2}} (b(X+a)+c)^{\frac{p-1}{2}}$$

$H(X) = 0 \bmod X^p - X$. En particulier le coefficient de X^{p-1} dans $H(X)$ modulo $X^p - X$ est nul. Or ce coefficient vaut :

$$\left(\frac{\beta}{2}\right)^{p-1} C^2_{\frac{p+3}{2}} (a^p - a)^{\frac{p-1}{2}}.$$

(ce résultat s'obtient en appliquant le Lemme 2.2.6 pour $n = 2$, lemme que nous démontrons juste après). Pour $p > 3$, on a $C^2_{p+3/2} \neq 0$ et donc $a^p = a$, ce qui entraîne $a \in \mathbb{F}_p$ (ce qui est impossible). On a donc ainsi montré l'inexistence des espaces $L_{2p,2}$ pour $p > 3$.

Remarque : Précisons ce qui se passe dans le cas $p = 3$.
Posons $a_1 = h_0x_0 = \beta/2a$ et $a_2 = h_1x_1 - h_0x_0 = \beta/2$. Alors $h_2x_2 = \beta/2(a-1) = a_1 - a_2$. On sait enfin que $h'_1x_1 + h'_2x_2 + h'_3x_3 = 0$, donc $h'_3x_3 = -a_2$ (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 :

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

Il ne reste plus qu'à démontrer le lemme suivant :

Lemme 2.2.6 *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 $(X+a)^{(np-(n+1))(p-1)/n}$ mod $X^p - X$ est :*

$$C^2_{q'}(a - a^p)^{q'-2}$$

avec $q' := ((n-1)p + (n+1))/n$.

Démonstration : 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 :

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

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 :

$$\begin{aligned}T &= \sum_{j=2}^{q'} C^j_{q'} C^{p-1-j}_{p-3} a^{(q'-j)} (a^p)^{(p-3-(p-1-j))} \\ &= \sum_{j=2}^{q'} C^j_{q'} C^{p-1-j}_{p-3} a^{(q'-j)} (a^p)^{(j-2)} \\ &= \sum_{j=0}^{(q'-2)} C^{j+2}_{q'} C^j_{p-3} a^{(q'-2)-j)} (a^p)^j.\end{aligned}$$

Regardons le terme C^j_{p-3} modulo p. On a :

$$C^j_{p-3} \equiv \frac{(-3)(-4)\cdots(-(j+2))}{j!} \equiv (-1)^j \frac{(j+1)(j+2)}{2} \equiv (-1)^j C^2_{j+2}.$$

Donc :

$$\begin{aligned} C^{j+2}_{q'}C^j_{p-3} &\equiv \frac{q'(q'-1)(q'-2)\cdots((q'-2)-j+1)}{j!(j+1)(j+2)} \\ &\quad (-1)^j\frac{(j+1)(j+2)}{2} \\ &\equiv (-1)^j\,\frac{q'(q'-1)}{2} \\ &\quad \frac{(q'-2)\cdots((q'-2)-j+1)}{j!} \\ &\equiv (-1)^j C^2_{q'}C^j_{(q'-2)}. \end{aligned}$$

Finalement :

$$\begin{aligned} T &= C^2_{q'}\sum_{j=0}^{(q'-2)}(-1)^j C^j_{(q'-2)}a^{((q'-2)-j)}(a^p)^j \\ &= C^2_{q'}(a-a^p)^{(q'-2)}. \end{aligned}$$

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 $C^2_{q'} = C^2_p \mod p$, ce qui achève la démonstration du lemme.

□

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 :

- $x_i+y_i+z_i = s = \text{cste}$ (même argument que dans le cas $m+1=2p$).
- $x_iy_i + y_iz_i + x_iz_i = m_i$.
- $x_iy_iz_i = p_i$
- $A_i(r) = h_ix_i^r + k_iy_i^r + l_iz_i^r$.

Étape 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 :

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

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

Comme précédemment, on part de l'égalité :

$$A_i(r+3) - sA_i(r+2) + m_iA_i(r+1) - p_0A_i(r) = 0 \quad \forall r \geq 0.$$

qui en sommant sur tous les i donne :

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

et donc :

$$\sum_{i=0}^{p-1} m_iA_i(r) = 0 \quad \text{pour } 1 \leq r \leq 3p-4. \tag{2.6}$$

Il suit de même pour $r \geq 2$:

$$\sum_{i=0}^{p-1}(m_iA_i(r+2) - m_isA_i(r+1) + m_i^2A_i(r) - p_0m_iA_i(r-1)) = 0 \tag{2.7}$$

et donc que :

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

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

$$\sum_{i=0}^{p-1} m_i^\ell A_i(r) = 0 \quad \text{pour } \ell \leq r \leq 3p-2-2l. \tag{2.8}$$

On a alors en particulier :

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

et

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

Sachant que $m_i = (am_0 + im_p)/(a+i)$, 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 :

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

Or $A_i(p) = A_i(1)^p$, donc $A_i(1) = 0$. L'expression (2.7) évaluée en $r = 1$ donne alors $\sum_{i=0}^{p-1} m_i A_i(0) = 0$, i.e, la relation (2.6) pour $r = 0$. Ceci entraîne que la relation (2.8) est encore vraie pour $\ell - 1 \leq r \leq 3p - 2\ell - 2$. On a donc $\sum_{i=0}^{p-1} m_i^\ell A_i(p-2) = 0$ si $1 \leq \ell \leq p-1$ 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. ⌟

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

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

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

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

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 :

1er cas : $p = 3$

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.

2ème cas : $p \neq 3$. 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

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

1er sous-cas : $m_0 \neq 0$. 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 $(i/a+1)^{p-2} \in \mathbb{F}_p$. Posons $A = 1/a$, 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.

2ème sous-cas : $m_0 = 0$. Dans ce cas $x_i^3 = p_i = b + c/(a+i)$, avec $b = p_p$ et $c = a(p_0 - p_p)$. On a la même relation pour y_i et z_i, donc $y_i = jx_i$, $z_i = j^2 x_i$, 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 :

$$\begin{cases} h_i + k_i + l_i & = & 0 \\ h_i + jk_i - (1+j)l_i & = & 0 \end{cases}$$

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

$$\begin{cases} k_i & = & \frac{-(2+j)}{2j+1}h_i & = & \mu h_i \\ l_i & = & \frac{1-j}{2j+1}h_i & = & \lambda h_i \end{cases}$$

$\mu, \lambda \in \mathbb{F}_p$, (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 $x_i^3 = b + c/(a+i)$, 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 $G(X) = 0 \bmod X^p - X$. En particulier le coefficient de X^{p-1} dans $G(X)$ modulo $X^p - X$ est nul.

On peut appliquer le Lemme 2.2.6 pour $n = 3$, (notons que $p \equiv 1 \bmod 3$) ; 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, $C^2_{(2p+4)/3} \neq 0$ 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 $p > 2$.

□

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

On peut expliquer la construction d'actions de $(\mathbb{Z}/p\mathbb{Z})^n$ sur le disque ouvert p-adique qui se trouve dans [Ma] par la présence cachée d'espaces $L_{m+1,n}$. Dans cette construction, on utilise le fait que la forme $\omega := (u\,\mathrm{d}z)/(z^{p-1}-\alpha)$ ($\alpha \in k^*$ et $u = \alpha/x_i$, où x_i est une des racines du polynôme $z^{p-1}-\alpha$) est logarithmique, et la remarque 4 du paragraphe 2.2.3.

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

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

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

On a :

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

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 2.2.3). 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 :

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

ce qui prouve que ω_1 est bien logarithmique. De même, on peut trouver u_j pour que ω_j soit logarithmique ; la forme différentielle 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 :

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

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 : Si on reprend les arguments de la remarque 4 du paragraphe 2.2.3, 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 2.2.5) que cette condition est nécessaire.

2.2.6 Les espaces $L^j_{qp,2}$

Nous allons maintenant énoncer quelques résultats relatifs aux espaces $L^j_{qp,2}$ qui auront des applications directes par la suite.

Espaces $L^1_{p,2}$

Nous allons décrire ici les espaces $L^1_{p,2}$. Un tel espace est engendré par deux formes différentielles ω_0 et ω_p qui s'écrivent :

$$\omega_0 := \frac{u\,\mathrm{d}x}{\prod_{j=1}^{p-1}(x-x_j)} \quad \text{et} \quad \omega_p := \frac{v\,\mathrm{d}x}{\prod_{j=0}^{p-1}(x-x_j)}$$

avec $u, v \in k^*$ et les x_j distincts deux à deux (après translation éventuelle, on peut se ramener à prendre $x_0 = 0$). Quitte à réindexer les x_j, on peut supposer que $\omega_0 + i\omega_p$ $(0 \leq i \leq p-1)$ a des pôles en tous les x_j pour $j \neq i$. On a alors deux écritures pour $\omega_0 + i\omega_p$:

$$\omega_0 + i\omega_p = \frac{(ux+iv)\mathrm{d}x}{\prod_{j=0}^{p-1}(x-x_j)} = \frac{u(x-x_i)\mathrm{d}x}{\prod_{j=0}^{p-1}(x-x_j)}.$$

En posant $a' := v/u$ et en identifiant les deux termes il vient $x_i = -a'i$, $\forall i \leq p-1$. On calcule les résidus de ω_0 et ω_p en les x_i, et on montre ainsi que $\omega_0 := \mathrm{d}f_0/f_0$ et $\omega_p := \mathrm{d}f_p/f_p$ avec :

$$f_0 := \prod_{i=1}^{p-1}(x-a'i)^i \quad \text{et} \quad f_p := \prod_{i=0}^{p-1}(x-a'i)$$

et $u := -(a')^{p-2}$, $v = -(a')^{p-1}$.

Espaces $L^2_{2p,2}$

On démontre ici que de tels espaces n'existent pas.

On raisonne par l'absurde et on considère un $L^2_{2p,2}$ engendré par deux formes différentielles ω_0 et ω_p qui s'écrivent :

$$\omega_0 := \frac{u\,\mathrm{d}x}{\prod_{j=1}^{p-1}(x-x_j)(x-y_j)} \quad \text{et} \quad \omega_p := \frac{v\,\mathrm{d}x}{\prod_{j=0}^{p-1}(x-x_j)(x-y_j)}$$

avec $u, v \in k^*$ et les x_j, y_j tous distincts. Quitte à réindexer les x_j, y_j, on peut supposer que $\omega_0 + i\omega_p$ $(0 \leq i \leq p-1)$ a des pôles en tous les x_j et tous les y_j pour $j \neq i$. On a alors deux écritures pour $\omega_0 + i\omega_p$:

$$\omega_0 + i\omega_p = \frac{u(x^2 - s_0x + p_0) + iv\,\mathrm{d}x}{\prod_{j=0}^{p-1}(x-x_j)(x-y_j)} = \frac{u(x^2 - s_ix + p_i)\mathrm{d}x}{\prod_{j=0}^{p-1}(x-x_j)(x-y_j)}$$

où $s_i := x_i + y_i$ et $p_i = x_iy_i$. Après translation éventuelle, on se ramène à $s_0 = 0$. En posant $a := v/u$ et en identifiant les deux termes il vient $s_i = 0$ et $p_i = p_0 + ai$.

On note h_i (resp. k_i) le résidu de ω_2 en x_i (resp. y_i). Posons $A_i(r) := h_ix_i^r + k_iy_i^r$ pour $r \geq 0$ et $0 \leq i \leq p-1$. Alors en reprenant le même raisonnement que lors de l'étude des espaces $L_{qp,2}$, on montre que :

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

et que

$$\begin{cases} \sum_{i=0}^{p-1} i^\ell A_i(0) &= 0 \quad 0 \leq \ell \leq p-1 \\ \sum_{i=0}^{p-1} i^\ell A_i(1) &= 0 \quad 0 \leq \ell \leq p-2. \end{cases}$$

La résolution de ce système donne $A_i(0) = 0$ et $A_i(1) =$cste. Vu que $y_i = -x_i$ et $k_i = -h_i$, on obtient $A_i(1) = 2h_ix_i =$cste, ce qui est absurde.

Chapitre 3

Applications au relèvement d'actions de $(\mathbb{Z}/p\mathbb{Z})^n$ sur $k[[z]]$

Dans ce chapitre nous donnons des applications directes aux résultats du chapitre précédents. Nous montrons d'abord que chaque espace $L_{m+1,n}$ permet de construire une action de $(\mathbb{Z}/p\mathbb{Z})^n$ sur le disque ouvert p-adique. Nous verrons ensuite que le Théorème 2.2.5 implique l'impossibilité de relever certaines actions de $(\mathbb{Z}/p\mathbb{Z})^2$ sur $k[[z]]$ et fournit ainsi des obstructions de nature nouvelle au relèvement.

3.1 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 π). Plus précisément, on a le théorème suivant :

Théorème 3.1.1 *On considère un $L_{m+1,n}$ et une base $\omega_1, \cdots, \omega_n$ de cet espace, chaque ω_i s'écrivant $\mathrm{d}f_i/f_i$. 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 $\mathbb{P}^1_K$ donnés par les équations $Y_i^p = F_i(X)$ induisent après normalisation un revêtement de $\mathbb{P}^1_K$ 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 3.1.2 *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 $\mathrm{d}f_j/f_j$ avec $f_j =$*

$\prod_{i=1}^{T}(1-x_ix)^{h_{ij}}$ *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* $F_j(X):=\prod_{i=1}^{T}(1-X_iX)^{h_{ij}}$. *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 :*

$$F_j(X)=(1+X\hat{Q}_j(X))^p+U_jX^m(1+X\hat{R}_j(X))+p\hat{S}_j(X) \tag{3.1}$$

Démonstration : On a :

$$f'_j=\frac{u_jx^{m-1}}{\prod_{i=1}^{T}(1-x_ix)}\prod_{i=1}^{T}(1-x_ix)^{h_{ij}}=u_jx^{m-1}(1+xr(x))$$

où $u_j\in k^*$ et $r(x)$ est un polynôme dans lequel on a regroupé tous les termes de degré supérieur. Le polynôme f_j est donc de la forme :

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

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

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

□

Démonstration du théorème : L'approximation (3.1) du Lemme 3.1.2 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 $f:=\sum a_ix^i\in k[t]$ alors on pose $f^{F^{-1}}:=\sum a_i^{1/p}x^i$. 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 $F:=\prod_{i=1}^{T}(1-X_iX)^{h_i}$ soit de la forme :

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

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 :

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

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

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

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 3.1.2 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 :

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

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

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

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

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

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 $T := \lambda^{-p/m}X$.

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

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

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 $\mathbb{P}^1_K$ 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 2.2.3). 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 2.2.2). 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 du Théorème 1.2.1.

□

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 :

$$\begin{cases} z_1^p - z_1 &= u_1 t^m \\ &\vdots \\ z_n^p - z_n &= u_n t^m \end{cases}$$

où les u_i sont $\mathbb{F}_p$-indépendants, car attachés à un espace $L_{m+1,n}$ (cf. remarque 3 du paragraphe 2.2.3).

3.2 Relèvement d'actions de $(\mathbb{Z}/p\mathbb{Z})^2$ sur $k[[z]]$

On s'intéresse ici au relèvement d'action de $G := (\mathbb{Z}/p\mathbb{Z})^2$ ($p \geq 3$) sur $k[[z]]$ en des actions de G sur $R[[Z]]$.

3.2.1 Cas de conducteurs égaux

Tout d'abord, examinons le cas où toutes les sous-extensions de $k[[z]]^G$ de degré p ont le même conducteur $m+1$.

Commençons par le cas $p = 2$:

Théorème 3.2.1 *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 $k[[t]]^G$ 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 $R = W(k)[\lambda^{1/(2n-1)}]$.*

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 3.2.2 *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 :*

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

soit de la forme :

$$(Q(X))^2 + UX^{2n-1} + 2R(X)$$

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

Démonstration : Notons x_i la réduction de X_i modulo l'idéal maximal de $W(k)$. D'après le Théorème 2.2.4 (voir l'équation 2.3), 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 :

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

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

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

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

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

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

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

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

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

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

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

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 $r \geq n$, alors les termes en X^r (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^r $(1 \leq r \leq n-1)$ 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_r le r-ième terme de la série de Taylor de $(-RQ^{-2})$ (i.e $(-RQ^{-2}) = \sum_{r\geq 1}\alpha_rX^r$). Alors la condition que l'on vient d'énoncer se ramène au système :

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

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

□

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 le Théorème 1.4.2, 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 $t' = t(p(t))^{-1/(2n-1)}$. 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 $T' := T(P(T))^{-1/(2n-1)}$ 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 Spec$W(k)[[T]]$. Notons $X = 2^{2/(2n-1)}T^{-1}$. Alors τ induit un automorphisme sur le disque fermé 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 $\tau(X^{-1}) = X^{-1}P(2^{2/(2n-1)}X^{-1})^{-1/(2n-1)}$ et τ est l'identité en réduction. Soit $\tilde{C}_2 : Y_2^2 = 1 + 4/T'^{2n-1}$ un relèvement de C_2 que l'on peut récrire 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 Spec$W(k)\{\{X^{-1}\}\}$. Posons $(1 - X_iX) := \tau^{-1}(1 - X_i'X')$. 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 : Un résultat plus complet (i.e $p = 2$ et conducteurs quelconques) sera montré par la suite (cf. Théorème 5.2.1).

Dans le cas $p > 2$ une généralisation du Théorème 3.2.1 est un problème ouvert. Nous allons voir que la condition $p/(m+1)$ n'est plus suffisante et que les questions d'existence d'espaces $L_{m+1,2}$ ou $L^j_{qp,2}$ sont cruciales.

On se place donc maintenant dans le cas $p \geq 3$. Le cas le plus simple, est $m + 1 = p$. On a alors le théorème suivant :

Théorème 3.2.3 *Soit $G = (\mathbb{Z}/p\mathbb{Z})^2$, $p \geq 3$ 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 $k[[z]]^G$, 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 : Supposons alors que l'action de G se relève en une action de G sur $R[[Z]]$. Dans ce cas, on sait d'après [Gr-Ma 2] Théorème III.3.1 que la géométrie du lieu de branchement de chaque revêtement intermédiaire de degré p est équidistante. La fibre spéciale $\mathcal{D}'_{0,s}$ est alors réduite à une composante. D'après l'étude menée précédemment, il doit apparaître un espace $L_{p,2}$ sur cette composante, ce qui contredit le Théorème 2.2.5.

□

Le deuxième cas le plus simple qui apparaît est le cas $m+1 = 2p$. On peut alors prouver le théorème suivant :

Théorème 3.2.4 *Soit $p \geq 3$ un nombre premier et $G := (\mathbb{Z}/p\mathbb{Z})^2$. On suppose que G est un groupe de k-automorphismes de $k[[z]]$ et que chacune des sous-extensions de $k[[z]]^G$ de degré p a un conducteur égal à $2p$. Supposons que G se relève en un groupe de R-automorphismes de $R[[Z]]$. Alors la géométrie du lieu de branchement du revêtement*

$$\mathrm{Spec}R[[Z]] \to \mathrm{Spec}R[[Z]]^G$$

est équidistante. Il suit que p doit être égal à 3.

Démonstration : On raisonne par l'absurde et on suppose donc que la géométrie est non équidistante. Les espaces qui peuvent apparaître dans les composantes terminales de $\mathcal{D}'_{0,s}$ sont a priori les suivants :

$$L_{m+1,1};\ L_{p,2};\ L^1_{p,2};\ L_{2p,2};\ L^1_{2p,2};\ L^2_{2p,2}.$$

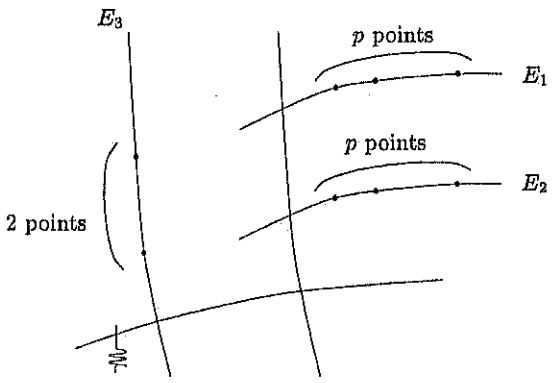
En fait parmi ces six espaces, seuls deux peuvent apparaître car :

- Les espaces $L_{2p,2}$ n'apparaissent pas (cela correspondrait alors à une géométrie du lieu de branchement équidistante).
- On a déjà montré que les espaces $L_{p,2}$ et $L^2_{2p,2}$ n'existaient pas (voir le Théorème 2.2.5 et la fin du chapitre 2).
- Si on a un espace $L^1_{2p,2}$ sur l'une des composantes terminales, cela veut dire qu'au moins un des revêtements intermédiaires de degré p a $2p-1$ points de branchement qui se spécialisent sur une même composante terminale. Le dernier point de branchement de ce revêtement se spécialise alors sur une composante interne, ce qui contredit la Proposition 1.2 dans [Gr-Ma 2]. On n'a donc pas d'espaces $L^1_{2p,2}$.
- Si un espace $L_{m+1,1}$ apparaît sur une composante terminale E_i alors l'un des revêtements intermédiaires Rev_{j_0} de degré p n'est ramifié en aucun des $m+1$ points situés sur E_i. Soit S_{j_0} l'ensemble des points où Rev_{j_0} n'est pas ramifié ; S_{j_0} contient alors deux éléments (voir Lemme 2.1.1). Donc $m+1 = 2$.

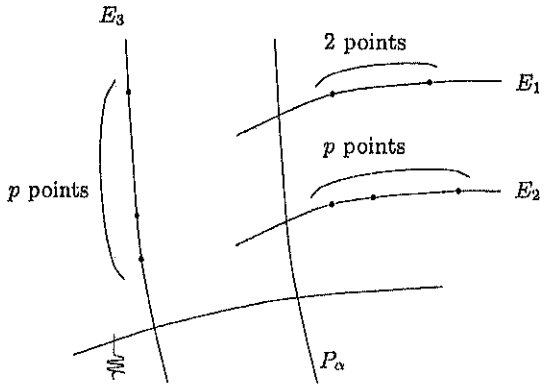
Finalement, dans les composantes terminales de $\mathcal{D}'_{0,s}$ ne peuvent apparaître que des espaces $L^1_{p,2}$ ou $L_{2,1}$. Deux cas sont à considérer :
Premier cas : On a au moins un espace $L^1_{p,2}$ dans une des composantes terminales.

Alors on a forcément un autre espace $L^1_{p,2}$ sur une autre composante terminale. En effet, supposons que l'on ait une seule composante terminale avec un espace $L^1_{p,2}$. Il existe alors un revêtement intermédiaire de degré p (noté Rev_0) qui possède p points de branchement sur cette composante. Les autres points de branchement de Rev_0 se spécialisent sur d'autres composantes terminales sur lesquelles il ne peut exister que des espaces $L_{2,1}$, i.e ces autres points de branchement sont en nombre pair. Le nombre total de points de branchement de Rev_0 serait alors impair, ce qui est absurde.

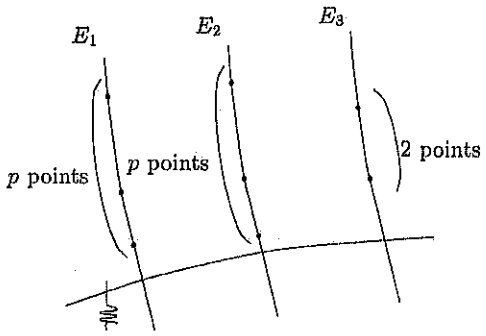
On a donc trois composantes terminales dans $\mathcal{D}'_{0,s}$ avec sur deux d'entre elles des espaces $L^1_{p,2}$ et sur la troisième un espace $L_{2,1}$. Ceci donne lieu à trois géométries envisageables :



Arbre 1



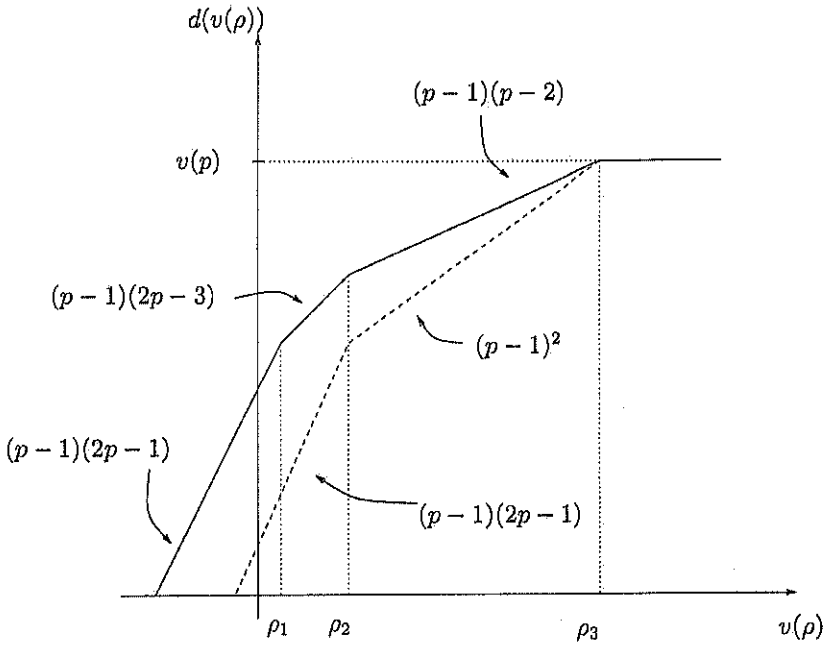
Arbre 2



Arbre 3

- Premier arbre : Soit Rev_0 le revêtement intermédiaire d'ordre p qui n'est pas ramifié en les points situés sur E_3, et Rev_p un autre revêtement intermédiaire d'ordre p. Soit z_0 la spécialisation d'un point de branchement commun à Rev_0 et Rev_p. Pour chacun des

revêtements Rev_0 et Rev_p, traçons les graphes de la valuation de la différente en fonction du rayon ρ d'un disque centré en z_0 :

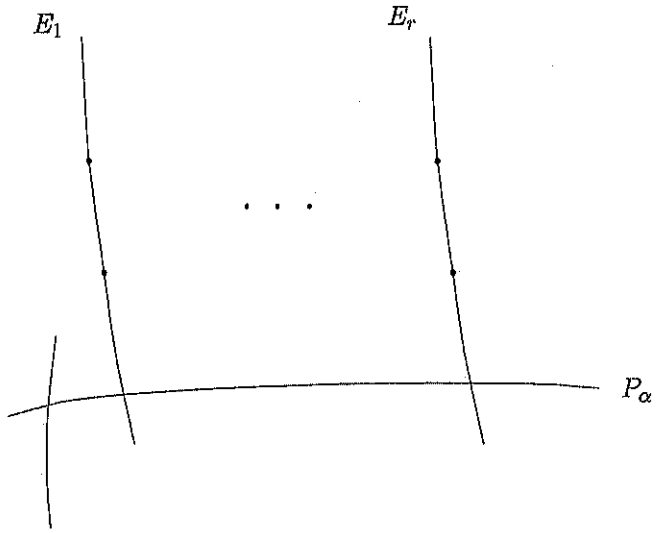


(le graphe correspondant à Rev_0 est tracé en pointillés et celui de Rev_p en traits pleins.)

On voit donc que la valuation de la différente des deux revêtements ne s'annule pas pour le même rayon, ce qui contredit le fait que ces deux revêtement doivent avoir simultanément bonne réduction par rapport à la même valuation de Gauss.

- Deuxième arbre : Le même raisonnement reste valide (i.e un argument sur la variation de la différente), mais on peut conclure ici par un argument plus direct en regardant un revêtement intermédiaire de degré p (que l'on appelle Rev_{i_0}) dont le lieu de branchement se spécialisent en les deux points de E_1 et en $p-1$ points de E_2 et E_3. La forme différentielle induite par Rev_{i_0} sur P_α aurait alors un pôle d'ordre 2 et un pôle d'ordre $p-1$, et ne pourrait alors être exacte.
- Troisième arbre : On utilise le même argument que pour le premier arbre.

Deuxième cas : Il n'y a que des espaces $L_{2,1}$ dans les composantes terminales de $\mathcal{D}'_{0,s}$. Considérons donc une composante interne P_α qui ne porte que des composantes terminales notées $E_1, \cdots, E_r$ (il suffit pour cela de partir d'une composante terminale E_1 à distance maximale de la racine de l'arbre ; la composante interne qui porte E_1 ne peut alors porter que des composantes terminales). On appelle D_α le disque correspondant à la composante P_α.



Montrons que toutes les composantes E_i correspondent à des disques de même rayon. Soient $i, j \leq r$, $i \neq j$ et Rev_i (resp. Rev_j) le revêtement branché en tous les points sauf ceux situés sur E_i (resp. E_j). Soit x_i (resp. x_j) un point de branchement de Rev_j (resp. Rev_i) situé sur E_i (resp. E_j). On trace le graphe de la valuation de la différente pour le revêtement Rev_i (resp. Rev_j) en fonction du rayon d'un disque centré en x_j (resp. x_i). Notons $|\rho_\alpha|$ (resp. $|\rho_i|$, $|\rho_j|$) le rayon du disque correspondant à la composante P_α (resp. E_i, E_j). Alors pour $v(\rho) \leq v(\rho_\alpha)$ ces deux graphes coïncident (puisque le lieu de branchement de Rev_i et Rev_j est le même en dehors des composantes E_i et E_j). Pour $v(\rho_\alpha) \leq v(\rho) \leq v(\rho_j)$ (resp. $v(\rho_\alpha) \leq v(\rho) \leq v(\rho_i)$) la pente du graphe relatif au revêtement Rev_i (resp. Rev_j) est $p-1$. On a donc $d(v(\rho_\alpha)) + (p-1)(v(\rho_i) - v(\rho_\alpha)) = d(v(\rho_\alpha)) + (p-1)(v(\rho_j) - v(\rho_\alpha)) = v(p)$ et donc $v(\rho_i) = v(\rho_j)$.

Pour chaque revêtement intermédiaire de degré p, la valuation de la différente au bord du disque D_α est la même et vaut $d(v(\rho_\alpha)) := v(p) - (p-1)t$ avec $0 < t < v(p)/(p-1)$ (voir Proposition 1.3.1).

Soient Rev_0 et Rev_p deux revêtements intermédiaires d'ordre p donnés respectivement par les équations $Y_0^p = F_0(X)$ et $Y_p^p = F_p(X)$ ($F_0, F_p \in R[[X]]$). Les équations de ces deux torseurs par rapport à un paramètre T du disque D_α sont de la forme :

$$y_0^p = 1 + \pi^t u_0$$

$$y_p^p = 1 + \pi^t u_p$$

où $u_0, u_p \in R[[T]]$ (voir Proposition 1.3.1). Soient $\omega_0 := \mathrm{d}\overline{u}_0$ et $\omega_p := \mathrm{d}\overline{u}_p$ les deux formes différentielles exactes (ω_0 et ω_p n'ont qu'un seul zéro en ∞). Tous les autres revêtements intermédiaires sont donnés par les équations $Y_{i,j} = F_0^i F_p^j$ ce qui donne par rapport au paramètre du disque D_α :

$$y_{i,j}^p = 1 + \pi^t(iu_0 + ju_p).$$

La forme différentielle exacte correspondante est donc $i\omega_0 + j\omega_p$ et on voit apparaître ainsi des $\mathbb{F}_p$-espaces de formes différentielles exactes analogues aux espaces de formes différentielles logarithmiques $L_{m+1,2}$. On peut écrire ω_0 et ω_p sous la forme :

$$\omega_0 = \frac{\mathrm{d}x}{DP} \quad \text{et} \quad \omega_p = \frac{\mathrm{d}x}{DQ}$$

où D, P, Q sont des polynômes n'ayant que des racines doubles (ceci est une conséquence directe du Théorème 1.3.2) et $(P, Q) = 1$. En particulier pour tout $i, j \in \mathbb{F}_p$, $iP + jQ$ n'a pas de racines simples. Or on a le lemme suivant :

Lemme 3.2.5 *On suppose $p \geq 3$. Soit $P, Q \in k[x]$, $(P, Q) = 1$ tels que $P, Q, P+Q$, et $P-Q$ n'aient pas de racine simple. Alors $P' = Q' = 0$.*

Démonstration : On peut supposer que $\deg P \geq \deg Q$. Le polynôme P n'a pas de racine simple donc P divise P'^2,i.e il existe P_0 dans $k[x]$ tel que $P'^2 = P_0 P$. De même il existe Q_0, P_+, P_- dans $k[x]$ tels que $Q'^2 = Q_0 Q$, $(P+Q)'^2 = (P+Q)P_+$ et $(P-Q)'^2 = (P-Q)P_-$. La somme des deux dernières égalités donne :

$$2(P'^2 + Q'^2) = P(P_+ + P_-) + Q(P_+ - P_-)$$

et donc

$$P(P_+ + P_- - 2P_0) + Q(P_+ - P_- - 2Q_0) = 0$$

Or $(P, Q) = 1$ donc P divise $P_+ - P_- - 2Q_0$ ce qui donne $P_+ - P_- - 2Q_0 = 0$ pour des raisons de degré. Cela entraîne aussi que $P_+ + P_- - 2P_0 = 0$ et donc que $P_+ = P_0 + Q_0$, $P_- = P_0 - Q_0$.

Repartons de l'équation $(P+Q)'^2 = (P+Q)P_+$ en remplaçant P_+ par l'expression trouvée, on obtient :

$$P'^2 + Q'^2 + 2P'Q' = (P_0 + Q_0)(P + Q)$$
$$2P'Q' = P_0 Q + Q_0 P.$$

D'où

$$4P'^2 Q'^2 = (P_0 Q + Q_0 P)^2$$
$$4P_0 Q_0 P Q = (P_0 Q + Q_0 P)^2$$
$$\text{i.e} \quad (P_0 Q - Q_0 P)^2 = 0.$$

Donc $P_0 Q = Q_0 P$ et $P_0 = Q_0 = 0$ pour des raisons de degré.

⌟

Remarque : Une autre démonstration de ce résultat consiste à considérer le morphisme :

$$\begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ x & \longmapsto & [P(x) : Q(x)]. \end{array}$$

On suppose que $(P/Q)' \neq 0$ et en utilisant la formule de Hurwitz, on montre que le nombre de points de branchements de ce revêtement est strictement inférieur à 4, ce qui apporte la contradiction attendue.

Revenons à la démonstration du théorème. Comme P et Q n'ont que des racines doubles, cela impose que ces polynômes sont constants. Ceci implique en particulier que les formes différentielles $\omega_0 + i\omega_p$ $(0 \leq i \leq p-1)$ et ω_p ont le même ensemble de pôles. Tous les revêtements intermédiaires d'ordre p seraient alors branchés en tous les points situés sur les E_i $(1 \leq i \leq r)$, ce qui est absurde.

On a donc une géométrie équidistante, i.e une seule composante dans $\mathcal{D}'_{0,s}$. Sur cette composante apparaît un espace $L_{2p,2}$ qui n'existe que dans le cas $p = 3$ (cf. Théorème 2.2.5).

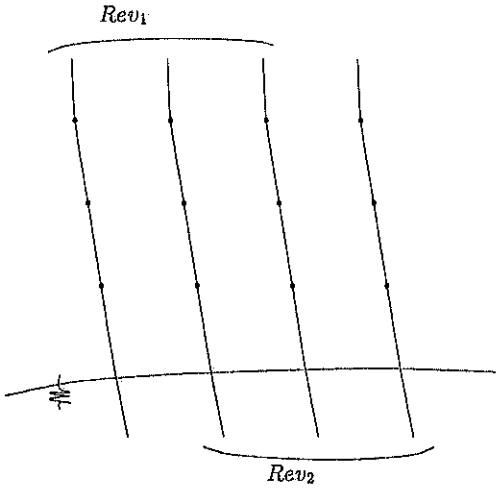
□

Nous donnons un énoncé analogue lorsque $m + 1 = 3p$. Là encore, un seul type de géométrie peut apparaître :

Théorème 3.2.6 *Soit $p \geq 3$ un nombre premier et $G := (\mathbb{Z}/p\mathbb{Z})^2$. On suppose que G est un groupe de k-automorphismes de $k[[z]]$ et que chacune des sous-extensions de $k[[z]]^G$ de degré p a un conducteur égal à $3p$. Supposons que G se relève en un groupe de R-automorphismes de $R[[Z]]$. Alors $p = 3$ et la géométrie du lieu de branchement du revêtement*

$$\mathrm{Spec}R[[Z]] \to \mathrm{Spec}R[[Z]]^G$$

est de la forme suivante :



La démonstration de ce théorème repose sur une analyse exhaustive de toutes les combinaisons d'espaces $L_{m+1,2}$ ou $L^j_{qp,2}$ qui peuvent exister sur les composantes terminales. Les

arguments qui permettent d'écarter certaines géométries sont ensuite identiques à ceux utilisés pour la démonstration du Théorème 3.2.4 (i.e essentiellement des arguments concernant la variation de la différente).

Démonstration : Les espaces qui peuvent apparaître sur les composantes terminales de $\mathcal{D}'_{0,s}$ sont les suivants :

$$L^1_{3p,2};\ L^2_{3p,2};\ L^3_{3p,2};\ L_{2p,2};\ L^1_{2p,2};\ L^1_{p,2};\ L_{2,1};\ L_{3,1}.$$

On regarde alors toutes les répartitions possibles (i.e quels sont les ensembles d'espaces qui peuvent apparaître dans une géométrie) sachant que les points de branchement doivent se partitionner en $p+1$ paquets de 3 points $S_0, \cdots, S_p$ (cf. Lemme 2.1.1). Cet examen (dont nous ne détaillons pas les calculs) donne lieu à sept configurations possibles. Nous donnons pour chacune de ces configurations les espaces qui apparaissent sur les composantes terminales ainsi que la répartition des points de branchement dans les ensembles $S_0, \cdots, S_p$.

1) Un espace $L^2_{3p,2}$ et un espace $L_{2,1}$:

	S_0	S_1	S_2	$\cdots$	$\cdots$	S_p
$L^2_{3p,2}$	1	3	3	$\cdots$	$\cdots$	3
$L_{2,1}$	2	0	0	$\cdots$	$\cdots$	0

Un petit mot d'explication : ce tableau signifie que l'on a deux composantes terminales dans l'arbre $\mathcal{D}'_{0,s}$. Sur une première composante terminale, on a un espace $L^2_{3p,2}$ (et donc $3p+1$ points de branchement sur cette composante se répartissant dans les ensembles S_i, comme indiqué dans le tableau). Sur la deuxième composante, on a un espace $L_{2,1}$ (et donc 2 points de branchement appartenant au même ensemble S_0).

2) Un espace $L^3_{3p,2}$ et un espace $L_{3,1}$:

	S_0	S_1	S_2	$\cdots$	$\cdots$	S_p
$L^3_{3p,2}$	0	3	3	$\cdots$	$\cdots$	3
$L_{3,1}$	3	0	0	$\cdots$	$\cdots$	0

3) Un espace $L^1_{2p,2}$, un espace $L^1_{p,2}$ et un espace $L_{2,1}$:

	S_0	S_1	S_2	$\cdots$	$\cdots$	S_p
$L^1_{2p,2}$	1	2	2	$\cdots$	$\cdots$	2
$L^1_{p,2}$	0	1	1	$\cdots$	$\cdots$	1
$L_{2,1}$	2	0	0	$\cdots$	$\cdots$	0

4) Quatre espaces $L^1_{p,2}$ (uniquement dans le cas $p=3$) :

	S_0	S_1	S_2	S_3
$L^1_{3,2}$	1	1	1	0
$L^1_{3,2}$	1	1	0	1
$L^1_{3,2}$	1	0	1	1
$L^1_{3,2}$	0	1	1	1

5) Trois espaces $L^1_{p,2}$ et un espace $L_{3,1}$:

	S_0	S_1	S_2	$\cdots$	$\cdots$	S_p
$L^1_{p,2}$	0	1	1	$\cdots$	$\cdots$	1
$L^1_{p,2}$	0	1	1	$\cdots$	$\cdots$	1
$L^1_{p,2}$	0	1	1	$\cdots$	$\cdots$	1
$L_{3,1}$	3	0	0	$\cdots$	$\cdots$	0

6) Un espace $L^1_{p,2}$, un espace $L_{3,1}$ et p espaces $L_{2,1}$:

	S_0	S_1	S_2	$\cdots$	$\cdots$	S_p
$L^1_{p,2}$	0	1	1	$\cdots$	$\cdots$	1
$L_{3,1}$	3	0	0	$\cdots$	$\cdots$	0
$L_{2,1}$	0	2	0	$\cdots$	$\cdots$	0
$L_{2,1}$	0	0	2	$\cdots$	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$		$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\ddots$	$\vdots$
$L_{2,1}$	0	0	0	$\cdots$	$\cdots$	2

7) $(p+1)$ espaces $L_{3,1}$:

	S_0	S_1	S_2	$\cdots$	$\cdots$	S_p
$L_{3,1}$	3	0	0	$\cdots$	$\cdots$	0
$L_{3,1}$	0	3	0	$\cdots$	$\cdots$	0
$L_{3,1}$	0	0	3	$\cdots$	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$		$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\ddots$	$\vdots$
$L_{3,1}$	0	0	0	$\cdots$	$\cdots$	3

Examinons chacun des sept cas :

1) La géométrie du lieu de branchement est donnée par la figure 3.1 :
Soit z_0 la spécialisation d'un point de branchement commun à Rev_0 et Rev_p. Pour chacun de ces deux revêtements on étudie la variation de la différente en fonction du rayon d'un disque centré en z_0 ; on s'aperçoit alors que ces deux revêtements ne peuvent avoir simultanément bonne réduction pour la même valuation de Gauss. On a ainsi écarté ce premier cas.

2) On exclut ce cas de la même façon que le premier.

3) Pour ce troisième cas on a quatre géométries possibles ; on montre que chacune de ces géométries conduit à une contradiction par le même argument.

4) Soit P_0 une composante interne qui ne porte que des composantes terminales et E_1, E_2 deux de ces composantes terminales. Soit $|\rho_0|$ le rayon du disque correspondant à la composante P_0. On note Rev_1 (resp. Rev_2) le revêtement intermédiaire de degré p ramifié

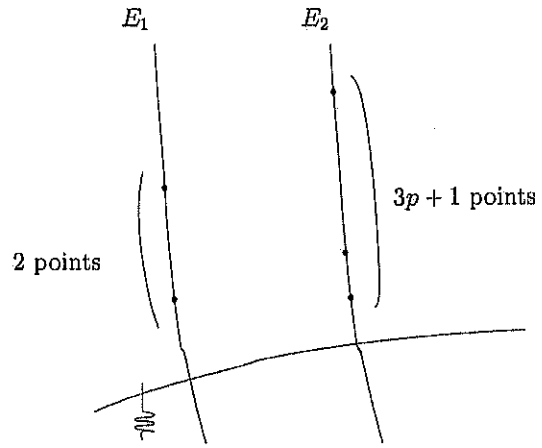


FIG. 3.1 –

en les trois points de E_1 (resp. E_2). Soit x_1 (resp. x_2) un point de branchement commun à Rev_1 et Rev_2 se spécialisant sur E_1 (resp. E_2) (voir figure 3.2).

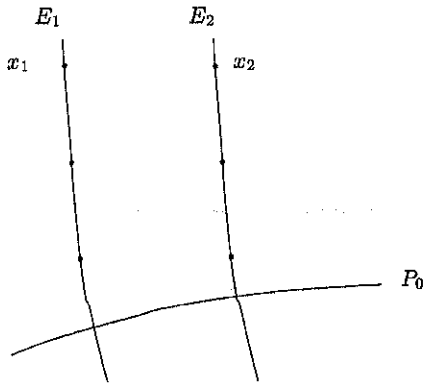


FIG. 3.2 –

Pour chacun des deux revêtements, on étudie la variation de la différente en fonction du rayon d'un disque centré en x_1. On note $d_1(\rho_0)$ (resp. $d_2(\rho_0)$) les valuations respectives associés au rayon ρ_0. On trouve alors $d_1(\rho_0) < d_2(\rho_0)$. Si on fait le même raisonnement en partant du point x_2 on trouve $d_2(\rho_0) < d_1(\rho_0)$. Ce quatrième cas est donc exclu.

5) Comme dans le cas 3), on examine toutes les géométries possibles et on conclut à l'impossibilité de ce cas.

6) C'est le cas le plus délicat en raison du grand nombre d'arrangements possibles. Considérons E_0 la composante terminale portant l'espace $L^2_{p,1}$ et P_0 la composante interne portant E_0.

Étape 1 : On commence par regarder quel espace de formes différentielles apparaît sur la composante P_0.

Soit Rev_0 le revêtement intermédiaire de degré p tel que tous les points de E_0 soient des spécialisations de points de branchement de Rev_0. Soit Rev_p un autre revêtement intermédiaire de degré p et x_0 la spécialisation d'un point de branchement commun à Rev_0 et Rev_p. On note S un paramètre du disque correspondant à P_0. D'après la Proposition 1.3.1, les équations des deux revêtements Rev_0 et Rev_p sont alors de la forme :

$$Y_0^p = 1 + \pi^{t_0} u_0(S) + o(\pi^{t_0})$$

$$Y_p^p = 1 + \pi^{t_p} u_p(S) + o(\pi^{t_p})$$

avec $u_0, u_p \in k(P_0)$ et $t_0, t_p \in \mathbb{N}^*$.

L'étude de la variation de la différente en fonction du rayon d'un disque centré en x_0 montre que $t_0 > t_p$. Tout autre revêtement intermédiaire de degré p (noté Rev_i pour $1 \leq i \leq p-1$) s'écrit alors :

$$Y_i^p = 1 + \pi^{t_p} u_p(S) + o(\pi^{t_p}).$$

En particulier la forme différentielle exacte induite par Rev_i sur P_0 est indépendante de i et vaut $\mathrm{d}\overline{u}_p$ (pour $1 \leq i \leq p$). On note t_α les pôles de $\mathrm{d}\overline{u}_p$ et $m_\alpha + 1$ l'ordre du pôle en t_α.

Étape 2 : Montrons que que la composante P_0 ne porte que deux composantes : E_0 (déjà introduite) et E_1 une autre composante sur laquelle vit un espace $L_{3,1}$.

On note $L_{2,1}^{(i)}$ $(1 \leq i \leq p)$ l'espace dont les deux points de branchement correspondant appartiennent à S_i. Soit P une composante (différente de E_0) portée par P_0 et t_α le point d'intersection de P et P_0. On note Λ l'ensemble des espaces ($L_{2,1}$ ou $L_{3,1}$) qui apparaissent dans le sous-arbre d'origine P. Alors Λ contient tous les espaces $L_{2,1}$ ou n'en contient aucun. En effet, supposons que Λ contienne $L_{2,1}^{(i)}$ mais pas $L_{2,1}^{(j)}$. Soit $|\tilde{B}r_i|$ (resp. $|\tilde{B}r_j|$) le nombre de points de branchement de Rev_i (resp. Rev_j) se spécialisant dans le sous-arbre d'origine P. Alors $|\tilde{B}r_j| = |\tilde{B}r_i| + 2$, ce qui contredit le fait que l'ordre du pôle en t_α reste constant.

En fait, on montre que Λ ne contient que l'espace $L_{3,1}$. On raisonne par l'absurde et on étudie la variation de la différente en fonction du rayon d'un disque centré en x_0. On montre alors que les deux revêtements Rev_0 et Rev_p ne peuvent avoir simultanément bonne réduction par rapport à un même paramètre.

Étape 3 : On conclut à l'impossibilité de ce sixième cas.

On note P_1 la composante interne qui porte P_0 et $|\rho_1|$ le rayon du disque correspondant (cf figure 3.3).

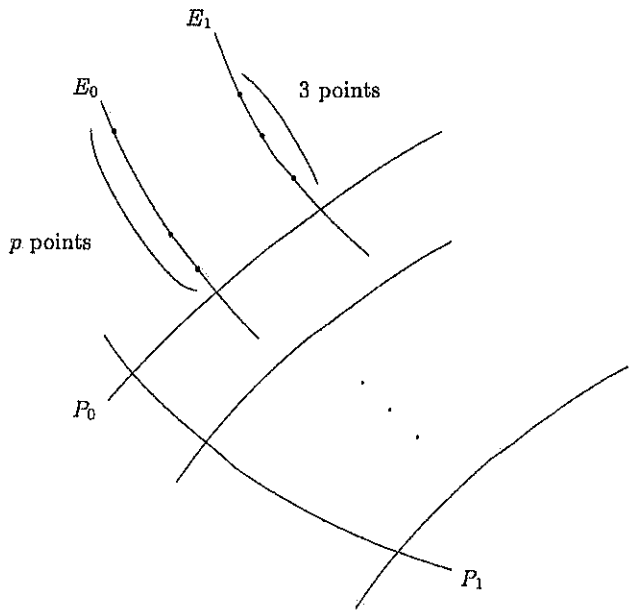


FIG. 3.3 –

Soit d_0 la valuation de la différente associée à Rev_0 et correspondant au rayon ρ_1. On note de même d_1 la valuation associée à Rev_i pour $1 \leq i \leq p$ (en effet d_1 ne dépend pas de i). Montrons que $d_0 = d_1$.

On a tout d'abord $d_0 \leq d_1$, sinon la valuation de la différente serait d_0 pour p revêtements parmi les $p+1$.

Supposons un instant que $d_0 < d_1$. Soit P une composante portée par P_1, et Λ l'ensemble des espaces $L_{2,1}$ qui apparaissent dans le sous-arbre d'origine P. On numérote comme précédemment les espaces $L_{2,1}^{(i)}$. Soit i_0 tel que $L_{2,1}^{(i_0)} \subset \Lambda$. On étudie la variation de la différente en fonction du rayon d'un disque centré en x_0 pour les revêtements Rev_0 et Rev_{i_0}. On constate alors que pour $v(\rho) \leq v(\rho_1)$ les deux graphes se déduisent l'un de l'autre par translation verticale de vecteur $(0, d_1 - d_0)$. Les deux revêtements Rev_0 et Rev_{i_0} ne peuvent avoir simultanément bonne réduction par rapport à un même paramètre.

On a donc $d_0 = d_1$ ce qui implique l'existence d'un $\mathbb{F}_p$-espace vectoriel de dimension deux de formes différentielles exactes sur P_1. Soit ω_i la forme différentielle exacte induite par Rev_i. Notons $t_0, \cdots, t_r$ les pôles de ω_0 en convenant d'appeler t_0 la coordonnée du point d'intersection de P_0 et P_1. Les formes ω_0 et ω_p s'écrivent :

$$\omega_0 = \frac{u\,\mathrm{d}x}{(x-t_0)^p \prod_{j=1}^{r}(x-t_i)^{m_i+1}}$$

$$\omega_p = \frac{v\,\mathrm{d}x}{(x-t_0)^{p+2} \prod_{j=1}^{r}(x-t_i)^{m_i'+1}}$$

avec $u, v \in k^*$, $m_i \in \mathbb{N}^*$ et $m'_i = m_i$ sauf éventuellement pour un i_0 auquel cas on a $m'_{i_0} = m_{i_0} - 2$.
On peut écrire ω_0 et ω_p sous la forme :

$$\omega_0 = \frac{\mathrm{d}x}{DP} \quad \text{et} \quad \omega_p = \frac{\mathrm{d}x}{DQ}$$

où D, P, Q sont des polynômes n'ayant que des racines doubles et $(P, Q) = 1$. En particulier pour tout $i, j \in \mathbb{F}_p$, $iP + jQ$ n'a pas de racines simples. Il ne reste plus qu'à appliquer le Lemme 3.2.5 pour avoir $P' = Q' = 0$ ce qui apporte la contradiction attendue.

7) La démonstration est identique à celle effectuée pour le Théorème 3.2.4 (Deuxième cas). On considère une composante interne P_α qui ne porte que des composantes terminales, et on montre l'existence d'un $\mathbb{F}_p$-espace vectoriel de dimension deux de formes différentielles exactes sur P_α. Cet espace est engendré par deux formes différentielles ω_0 et ω_p qui s'écrivent :

$$\omega_0 = \frac{\mathrm{d}x}{DP} \quad \text{et} \quad \omega_p = \frac{\mathrm{d}x}{DQ}$$

où D, P, Q sont des polynômes n'ayant que des racines triples et $(P, Q) = 1$. En particulier pour tout $i, j \in \mathbb{F}_p$, $iP + jQ$ n'a pas de racines simples. L'application du Lemme 3.2.5 montre que $P' = Q' = 0$ et donc que $p = 3$.
On a donc quatre composantes terminales dans l'arbre $\mathcal{D}'_{0,s}$. Comme dans le cas 5) on examine toutes les géométries possibles et on montre (toujours par un argument sur la variation de la différente) que la seule possible est celle indiquée dans le théorème.

□

On construira par la suite un exemple de revêtement ayant la géométrie indiquée dans le Théorème 3.2.6 (c'est un cas particulier du Théorème 4.2.1).

3.2.2 Cas de conducteurs différents

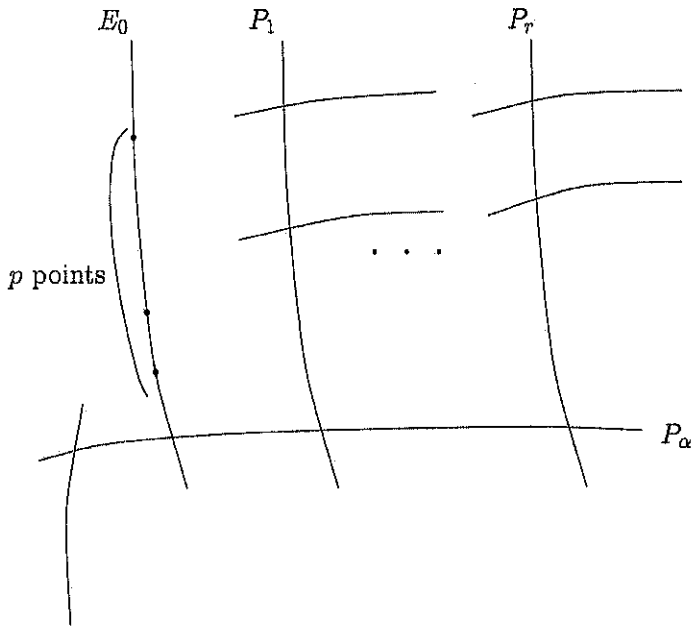
Soit $p \geq 3$. Soit $G := (\mathbb{Z}/p\mathbb{Z})^2$ un groupe de k-automorphismes de $k[[z]]$. On examine le cas particulier où l'extension $k[[z]]/k[[z]]^G$ est donnée par les équations :

$$\begin{cases} x_1^p - x_1 &= f_1\left(\frac{1}{t}\right) \\ x_2^p - x_2 &= f_2\left(\frac{1}{t}\right) \end{cases}$$

avec $\deg(f_1) = m_1$, $\deg(f_2) = m_2$, $m_1 + 1 = p$, et $m_2 > m_1$ (c'est le cas le plus simple qui peut apparaître lorsque l'on considère des extensions intermédiaires ayant des conducteurs différents).

Supposons qu'une telle action se relève. Notons Rev_1 et Rev_2 les revêtements correspondants. Le premier revêtement a un lieu de branchement équidistant (cf. Théorème 3.1 de

[Gr-Ma 2]) et le second a exactement $p-1$ points de branchement communs avec Rev_2. Ce second revêtement Rev_2 ne peut avoir une géométrie équidistante car $m_1 \neq m_2$ et puisque dans le cas équidistant le conducteur détermine le rayon du disque sur lequel se trouve les points de branchement (voir les rappels sur la variation de la différente de la partie 1.3). Le lieu de branchement de Rev_1 et Rev_2 est donc de la forme suivante :



E_0 est la composante terminale qui porte les spécialisations des points de branchement de Rev_1 et P_α est la composante interne liée à E_0. Sur la composante E_0 on a forcément un espace $L^1_{p,2}$ (car les espaces $L_{p,2}$ n'existent pas).

Soit ω_α la forme différentielle exacte sur P_α relative au revêtement Rev_2. Après un choix convenable de paramètre, on peut supposer que ω_α a un pôle d'ordre $p-1$ en 0 et s'écrit :

$$\omega_\alpha = \frac{u\,\mathrm{d}x}{x^{p-1}\prod_{i=1}^{r}(x-x_i)^{n_i+1}}$$

avec $n_i \notin p\mathbb{Z}$, $u \in k^*$ et les x_i distincts deux à deux.

Proposition 3.2.7 *On écrit la décomposition en éléments simples de la fraction rationnelle* $u/(x^{p-1}\prod_{i=1}^{r}(x-x_i)^{n_i+1})$ *:*

$$\frac{u}{x^{p-1}\prod_{i=1}^{r}(x-x_i)^{n_i+1}} = \frac{Q_0}{x^{p-1}} + \sum_{i=1}^{r}\frac{Q_i}{(x-x_i)^{n_i+1}}$$

où $Q_i \in k[x]$ avec $deg(Q_i) \leq n_i$ et $deg(Q_0) \leq p-2$.
Alors le polynôme Q_0 est constant.

Démonstration : Soit X un paramètre tel que la composante P_α corresponde au disque $|X| = 1$ et tel que $X = 0$ soit un point de branchement de Rev_1 mais pas de Rev_2. Soit $|\rho_0|$ le rayon du disque correspondant à la composante E_0 et $X' := X/\rho_0$. On note $0, \theta_1, \cdots, \theta_{p-1}$ les coordonnées des points de branchement de Rev_1 par rapport au paramètre X'. On sait que sur E_0 on a un espace $L^1_{p,2}$, donc d'après l'étude menée précédemment (voir paragraphe 2.2.6), on sait que les θ_i sont proches de ai (pour un a dans R^*).

Posons $F_1(X') := X' \prod_{i=1}^{p-1}(X' - \theta_i)$, $F_2(X') := \prod_{i=1}^{p-1}(X' - \theta_i)^i$, $t := \lambda^{p/(p-1)}$ et $S := tX'$; alors $Y_1^p = u(S)S\prod_{i=1}^{p-1}(S - t\theta_i)$ $(u \in R[[S]]^*)$ est une équation du revêtement Rev_1 et ce revêtement a bonne réduction par rapport au paramètre S. Le revêtement Rev_2 a une équation du type $Y_2^p = v(S)\prod_{i=1}^{p-1}(S - t\theta_i)^i Q(S)$ $(v \in R[[S]]^*)$ où Q est un polynôme dont les racines correspondent aux points de branchement de Rev_2 qui se spécialisent ailleurs que sur E_0. On peut, quitte à compactifier supposer que $u(S) = v(S) = 1$ (voir la Proposition 1.4.1).

Le revêtement Rev_2 doit avoir bonne réduction par rapport au paramètre S, ce qui implique en particulier que

$$v(\rho_0) \;<\; v(t). \tag{3.2}$$

(ceci se voit en regardant le graphe de la différente relatif au revêtement Rev_2).

Posons

$$G_1(T) := T^p F_1\left(\frac{1}{T}\right) = \prod_{i=1}^{p-1}(1 - \theta_i T)$$

et

$$G_2(T) := T^{\frac{p(p-1)}{2}} F_2\left(\frac{1}{T}\right) = \prod_{i=1}^{p-1}(1 - \theta_i T)^i.$$

Alors G_1 s'écrit $1 + \sum_{i=1}^{p-1} s_i T^i$ avec $v(s_i) \geq (p-1-i)v(t)$ pour $i \leq p-2$ et $v(s_{p-1}) = 0$ car le revêtement d'équation $Y^p = G_1$ a bonne réduction par rapport à T/t. Le polynôme G_2 s'écrit aussi $1 + \tilde{s}_1 T + \cdots + \tilde{s}_{p-2}T^{p-2} + \cdots$.

Nous allons montrer que :

$$v(\tilde{s}_i) \geq (p-2-i)v(t) \quad \text{pour } 1 \leq i \leq p-2.$$

Cette démonstration passe par des approximations assez fines des θ_i qui font l'objet du lemme suivant :

Lemme 3.2.8 *Il existe des coefficients $a_{jr} \in R$, $0 \leq j \leq p-3$, $1 \leq r \leq j+1$, tels que :*

$$\theta_i = \sum_{j=0}^{p-3} \alpha_{ij} t^j \mod t^{p-2}$$

avec

$$\alpha_{ij} := \sum_{r=1}^{j+1} a_{jr} i^r.$$

Démonstration : On a :

$$\frac{G_1'}{G_1} = -\sum_{i=1}^{p-1} \frac{\theta_i}{1 - T\theta_i} = \frac{s_1 + \cdots + (p-1)s_{p-1}T^{p-2}}{1 + s_1 T + \cdots + s_{p-1}T^{p-1}}.$$

Après identification entre les deux développements de Taylor des deux termes, on aboutit aux congruences :

$$\sum_{i=1}^{p-1} \theta_i^n \;=\; 0 \mod t^{p-1-n}, \quad 1 \le n \le p-2. \tag{3.3}$$

On va donner des approximations successives de θ_i modulo des puissances de t. Plus précisément, on montre donc par récurrence sur ℓ qu'il existe $a_{jr} \in R$ tels que :

$$\theta_i \;=\; \sum_{j=0}^{\ell-1} \alpha_{ij} t^j \mod t^\ell, \quad 1 \le \ell \le p-2, \quad \text{avec} \quad \alpha_{ij} := \sum_{r=1}^{j+1} a_{jr} i^r. \tag{3.4}$$

- $\ell = 1$: On a $G_1(T) = 1 + s_{p-1}T^{p-1} \mod t$. Soit $a_{01} \in R^*$ une racine $(p-1)$-ème de $-s_{p-1}$. Alors les θ_i sont de la forme $a_{01}i + \beta_i$ avec $v(\beta_i) > 0$. Donc :

$$G_1(a_{01}i) = \prod_{j=1}^{p-1}(a_{01}i - a_{01}j - \beta_j) = -\beta_i \prod_{j \neq i}(a_{01}(i-j) - \beta_j) = 0 \mod t$$

  ce qui implique que $\beta_i = 0 \mod t$. On a finalement $\theta_i = \alpha_{i0} := a_{01}i \mod t$.

- Supposons l'hypothèse (3.4) vraie au rang ℓ, pour $\ell < p-2$. On a alors en reprenant l'équation (3.3) :

$$\begin{aligned}
\sum_{i=1}^{p-1} \theta_i^n \;&=\; 0 \mod t^{\ell+1}, \quad 1 \le n \le p-2-\ell \\
\sum_{i=1}^{p-1} \left(\sum_{j=0}^{\ell} \alpha_{ij} t^j \right)^n \;&=\; 0 \mod t^{\ell+1}, \quad 1 \le n \le p-2-\ell \\
\sum_{i=1}^{p-1} \sum_{r=0}^{\ell} \left(\sum_{j_1+\cdots+j_n=r} \alpha_{ij_1} \cdots \alpha_{ij_n} \right) t^r \;&=\; 0 \mod t^{\ell+1}, \quad 1 \le n \le p-2-\ell.
\end{aligned}$$

Si $\{j_1, \cdots, j_n\} \neq \{0, \cdots, 0, \ell\}$, on peut appliquer l'hypothèse de récurrence, ainsi :

$$\alpha_{ij_1} \cdots \alpha_{ij_n} = \left(\sum_{r=1}^{j_1+1} a_{j_1 r} i^r\right) \cdots \left(\sum_{r=1}^{j_n+1} a_{j_n r} i^r\right) := P_{j_1 \cdots j_n}(i)$$

où $P_{j_1 \cdots j_n}$ est un polynôme de degré inférieur ou égal à $(j_1+1)+\cdots+(j_n+1)$ donc inférieur ou égal à $p-2$. Donc $\sum_{i=1}^{p-1} P_{j_1 \cdots j_n}(i) = 0 \mod p$ et a fortiori $\sum_{i=1}^{p-1} P_{j_1 \cdots j_n}(i) = 0 \mod t^{\ell+1}$ (car $p \equiv 0 \mod t^{p-2}$).

Il reste finalement les termes tels que $\{j_1, \cdots, j_n\} = \{0, \cdots, 0, \ell\}$, ainsi :

$$\sum_{i=1}^{p-1} n\alpha_{i0}^{n-1}\alpha_{il}t^l = 0 \mod t^{\ell+1}, \quad 1 \leq n \leq p-2-\ell$$

$$\text{et donc} \quad \sum_{i=1}^{p-1} i^{n-1}\alpha_{il} = 0 \mod t, \quad 1 \leq n \leq p-2-\ell.$$

Il reste donc à résoudre le système linéaire vérifié par les α_{il}.

Soit $\gamma_1, \cdots, \gamma_{p-2-\ell} \in R$ tels que :

$$\sum_{i=1}^{p-1} i^{n-1}\alpha_{il} = t\gamma_n \quad 1 \leq n \leq p-2-\ell.$$

Posons $a_{lr} := -\sum_{i=1}^{p-1} i^{p-1-r}\alpha_{il}$ pour $1 \leq r \leq \ell+1$ et :

$$A := \begin{pmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 1 & 2 & \cdots & \cdots & (p-1) \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & 2^{p-2} & \cdots & \cdots & (p-1)^{p-2} \end{pmatrix}$$

et

$$B := -\begin{pmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 2^{p-1} & 2^{p-2} & \cdots & \cdots & 2 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ (p-1)^{p-1} & (p-1)^{p-2} & \cdots & \cdots & (p-1) \end{pmatrix}.$$

On $AB = BA = \mathrm{Id} \bmod p$. Notre système s'écrit alors :

$$A \begin{pmatrix} \alpha_{1\ell} \\ \vdots \\ \\ \\ \vdots \\ \alpha_{p-1\ell} \end{pmatrix} = \begin{pmatrix} t\gamma_1 \\ \vdots \\ t\gamma_{p-2-\ell} \\ -a_{\ell\ell+1} \\ \vdots \\ -a_{\ell 1} \end{pmatrix} \tag{3.5}$$

et en multipliant (3.5) à gauche par B, il vient :

$$\alpha_{il} = \sum_{r=1}^{\ell+1} a_{\ell r} i^r \mod t \quad 1 \leq i \leq p-1.$$

⌟

Corollaire 3.2.9 *On a :*

$$\sum_{i=1}^{p-1} i\theta_i^n = 0 \mod t^{p-2-n}, \quad 1 \leq n \leq p-3.$$

Démonstration : Il s'agit d'une simple vérification :

$$\sum_{i=1}^{p-1} i\theta_i^n = \sum_{i=1}^{p-1} i \left(\sum_{r=0}^{p-3-n} \left(\sum_{j_1+\cdots+j_n=r} \alpha_{ij_1} \cdots \alpha_{ij_n} \right) t^r \right) \mod t^{p-2-n}.$$

Or

$$i\alpha_{ij_1} \cdots \alpha_{ij_n} = i \left(\sum_{r=1}^{j_1+1} a_{j_1 r} i^r \right) \cdots \left(\sum_{r=1}^{j_n+1} a_{j_n r} i^r \right) := Q_{j_1 \cdots j_n}(i)$$

où $Q_{j_1 \cdots j_n}$ est un polynôme degré $\leq 1 + (j_1+1) + \cdots (j_n+1) \leq p-2$. Donc pour tout n-uplet $(j_1, \cdots, j_n)$, $\sum_{i=1}^{p-1} Q_{j_1 \cdots j_n}(i)$ est nul modulo p donc nul modulo t^{p-2}. Finalement on trouve :

$$\sum_{i=1}^{p-1} i\theta_i^n = 0 \mod t^{p-2-n}.$$

⌟

Revenons à la démonstration de la proposition. On a les égalités :

$$\frac{G_2'}{G_2} = -\sum_{i=1}^{p-1} \frac{i\theta_i}{1 - T\theta_i} = \frac{\tilde{s}_1 + \cdots + (p-2)\tilde{s}_{p-2} T^{p-3} + \cdots}{1 + \tilde{s}_1 T + \cdots + \tilde{s}_{p-2} T^{p-2} + \cdots}$$

et l'identification des développements de Taylor montre que :

$$v(\tilde{s}_i) \geq (p-2-i)v(t) \quad \text{pour } 1 \leq i \leq p-2.$$

Regardons maintenant la réduction de l'équation de Rev_2 au bord du disque D_α. Notons $\tilde{Q}$ le facteur de Q qui correspond aux points de branchement de Rev_2 se spécialisant dans le sous-arbre d'origine P_α. On peut écrire $\tilde{Q}$ de la façon suivante (en fonction du paramètre X) :

$$\tilde{Q}(X) = \prod_{j=1}^{r} \prod_{i=1}^{n_j+1} (X - X_j - \theta_{ij})^{h_{ij}}$$

où X_j est un centre du disque correspondant à P_j, les θ_{ij} sont des éléments de valuation strictement positive et les h_{ij} des entiers tels que pour tout j, on ait $\sum_{i=1}^{n_j} h_{ij} \equiv 0 \bmod p$.

On a donc :

$$\begin{aligned} F_2(X)\tilde{Q}(X) &= \prod_{i=1}^{p-1}(X-\rho_0\theta_i)^i \prod_{j=1}^{r}\prod_{i=1}^{n_j}(X-X_j-\theta_{ij})^{h_{ij}} \\ &= X^{\frac{p(p-1)}{2}} \prod_{j=1}^{r}(X-X_j)^{(\sum_{i=1}^{n_j} h_{ij})} \left(G_2\left(\frac{\rho_0}{X}\right) . \frac{\prod_{j=1}^{r}\prod_{i=1}^{n_j}(X-X_j-\theta_{ij})^{h_{ij}}}{\prod_{j=1}^{r}(X-X_j)^{(\sum_{i=1}^{n_j} h_{ij})}} \right) \\ &= A^p \left(1+\rho_0\tilde{s}_1\frac{1}{X}+\cdots+\rho_0^{p-2}\tilde{s}_{p-2}\frac{1}{X^{p-2}}+o(\rho_0^{p-2})\right)\left(1+\frac{o(1)}{\prod_{j=1}^{r}(X-X_j)^{(\sum_{i=1}^{n_j} h_{ij})}}\right) \end{aligned}$$

avec $A^p := X^{p(p-1)/2}\prod_{j=1}^{r}(X-X_j)^{(\sum_{i=1}^{n_j} h_{ij})}$ et $o(\rho_0^{p-2})$ désigne un terme de valuation strictement plus grande que $(p-2)v(\rho_0)$. Or $v(\rho_0) < v(t)$ (d'après 3.2), donc $iv(\rho_0)+v(\tilde{s}_i) > (p-2)v(\rho_0)$ pour $i < p-2$. On a donc :

$$F_2(X)\tilde{Q}(X) = A^p\left(1+\rho_0^{p-2}\tilde{s}_{p-2}\frac{1}{X^{p-2}}+o(\rho_0^{p-2})\right)\left(1+\frac{o(1)}{\prod_{j=1}^{r}(X-X_j)^{(\sum_{i=1}^{n_j} h_{ij})}}\right).$$

Mais on sait que cette équation doit être de la forme :

$$F_2(X)\tilde{Q}(X) = \tilde{A}^p(1+\rho_0^{p-2}f+o(\rho_0^{p-2}))$$

avec $\mathrm{d}\overline{f} = \omega_\alpha$. En identifiant les deux expressions, on trouve alors le résultat annoncé dans la proposition.

□

Comme corollaire de cette proposition, on a le théorème suivant qui fournit de nouveaux exemples d'obstruction au relèvement :

Théorème 3.2.10 *Soit $p \geq 5$, un nombre premier et $G := (\mathbb{Z}/p\mathbb{Z})^2$. On suppose que G est un groupe de k-automorphismes de $k[[z]]$ et que l'une des sous-extensions de $k[[z]]^G$ de degré p a un conducteur m_1+1 égal à p tandis que les p autres sous-extensions ont un conducteur m_2+1 tel que $p+1 < m_2+1 < 2p-1$. Alors on ne peut pas relever G en un groupe de R-automorphismes de $R[[Z]]$.*

Démonstration : Si le relèvement est possible, d'après la Proposition 3.2.7 la forme différentielle exacte sur P_α doit s'écrire :

$$\omega_\alpha = \frac{u\mathrm{dx}}{x^{p-1}\prod_{i=1}^{r}(x-x_i)^{n_i+1}}$$

avec

$$\frac{u}{x^{p-1}\prod_{i=1}^{r}(x-x_i)^{n_i+1}} = \frac{Q_0}{x^{p-1}} + \sum_{i=1}^{r}\frac{Q_i}{(x-x_i)^{n_i+1}}$$

et Q_0 est un polynôme constant. Notons $P/Q := \sum_{i=1}^{r} Q_i/(x-x_i)^{n_i+1}$; on obtient par identification :

$$Q_0 Q + x^{p-1}P = u \quad \text{et donc} \quad Q = \frac{u - Px^{p-1}}{Q_0}.$$

On a donc $\deg(Q) \geq p-1$. Si $\deg(Q) = p-1$, alors P est un polynôme constant et $Q = (u - Px^{p-1})/(Q_0)$ est un polynôme n'ayant que des racines simples ce qui contredit le fait que ω_α est exacte. Donc $\deg(Q) \geq p$ et $m_2 + 1 \geq 2p-1$.

□

Remarque : Pour $m_1 + 1 = p$ et $m_2 + 1 = 2p-1$ de tels relèvements sont possibles. En effet, c'est le théorème de la troisième partie dans [Ma].

Chapitre 4

Exemples de revêtements galoisiens de groupe $(\mathbb{Z}/p\mathbb{Z})^n$

Soit k un corps algébriquement clos de caractéristique p et R un anneau de valuation discrète dominant l'anneau des vecteurs de Witt $W(k)$. Dans le Théorème 3.2.6, nous avons montré que si l'action était relevable, la géométrie du lieu de branchement du revêtement correspondant devait avoir une forme particulière. Il est alors intéressant de pouvoir exhiber des exemples de tels revêtements. C'est l'un des buts du chapitre 4.

On montre ainsi que des revêtements ayant la géométrie décrite au Théorème 3.2.6 sont réalisables, et qu'ils appartiennent à une famille plus générale de revêtements. On construit ainsi des réalisations de $(\mathbb{Z}/p\mathbb{Z})^n$ comme groupes d'automorphismes de $k[[z]]$ qui se relèvent en un groupe de R-automorphismes de $R[[Z]]$. Ces réalisations sont différentes de celles présentées dans [Ma] : les conducteurs utilisés ne sont pas les mêmes et la géométrie du lieu de branchement n'est plus équidistante.

4.1 Lemme préliminaire

On a besoin du lemme suivant :

Lemme 4.1.1 *Soit ζ une racine p-ième de l'unité et $\lambda := \zeta - 1$. Soit $\rho \in W(k)^{\mathrm{alg}}$ tel que $|\lambda|^{1/(p-1)} < |\rho| \leq |\lambda|^{1/(2(p-1))}$. Soient $T_1, \cdots, T_r \in R$ tels que $|T_i - T_j| = 1$ pour tout $i \neq j$ et $Q(X) := \prod_{i=1}^{r}(X - T_i)$. Soit $\alpha \in R$ inversible et $h_1, \cdots, h_r \in \mathbb{Z} - p\mathbb{Z}$. Posons $p_i := \alpha^p/(h_i Q'(T_i)^p)$. On définit enfin le polynôme f :*

$$f(X) := \prod_{i=1}^{r}\left[(X - T_i)^p + \rho^{p^2-p} p_i X\right]^{h_i}.$$

Alors le revêtement d'équation $Y^p = f(X)$ a bonne réduction relativement à la valuation de Gauss en $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(pr-1)} X$, cette réduction étant $z^p - z = \overline{\alpha}^p (1/t)^{pr-1}$. La

géométrie du lieu de branchement est donnée par la figure 4.1 :

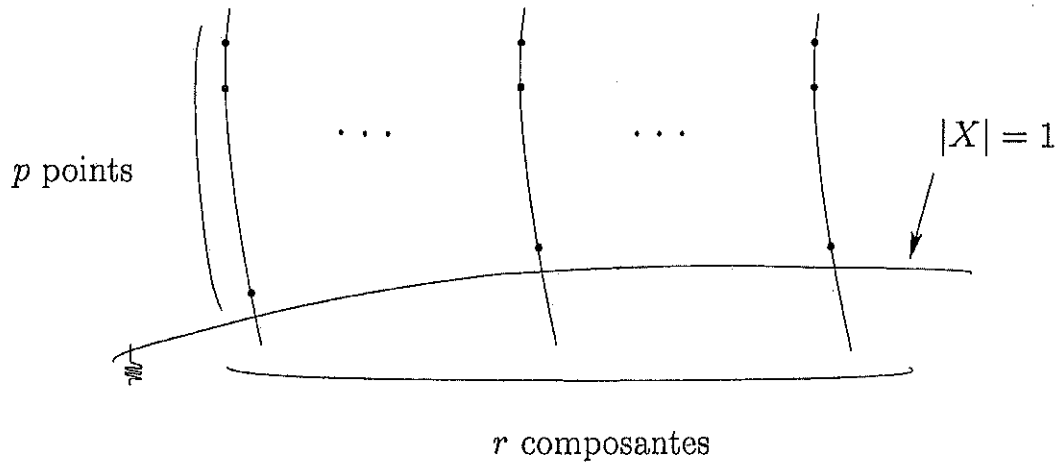


FIG. 4.1 – Géométrie du lieu de branchement

De plus, si on change p_i en $p_i + p\beta_i$ avec $\beta_i \in R$, le lemme reste encore vrai (i.e on ne modifie pas la géométrie du lieu de branchement et on a toujours la bonne réduction.)

Démonstration : On pose $Q_0(X) := \prod_{i=1}^{r}(X - T_i)^{h_i}$ et on écrit $O(\lambda^p)$ pour désigner des termes de valuation supérieure ou égale à $pv(\lambda)$. On a :

$$f(X) = \prod_{i=1}^{r}[(X - T_i)^{ph_i} + h_i p_i \rho^{p^2-p} X(X - T_i)^{p(h_i-1)} + O(\lambda^p)]$$

(cette égalité vient du fait que l'on a pris $|\lambda|^{1/(p-1)} < |\rho| \leq |\lambda|^{1/(2(p-1))}$).

$$\begin{aligned} f(X) &= Q_0^p + \rho^{p^2-p}\sum_{i=1}^{r} p_i h_i X(X - T_i)^{p(h_i-1)} \prod_{j\neq i}(X - T_j)^{ph_j} + O(\lambda^p) \\ &= Q_0^p + \rho^{p^2-p} X\left[\sum_{i=1}^{r} p_i h_i \prod_{j\neq i}(X - T_j)^{p}\right] \prod_{i=1}^{r}(X - T_i)^{p(h_i-1)} + O(\lambda^p) \\ &= Q_0^p + \rho^{p^2-p} X Q^p \left[\sum_{i=1}^{r} p_i h_i \frac{1}{(X - T_i)^p}\right] \prod_{i=1}^{r}(X - T_i)^{p(h_i-1)} + O(\lambda^p) \\ &= Q_0^p + \rho^{p^2-p}\alpha^p X \prod_{i=1}^{r}(X - T_i)^{p(h_i-1)} + O(\lambda^p). \end{aligned}$$

On a donc :

$$\frac{f(X)}{(X^{\sum h_i})^p} = \left(\frac{Q_0}{X^{\sum h_i}}\right)^p + \rho^{p^2-p}\alpha^p \frac{1}{X^{pr-1}} \prod_{i=1}^{r} \left(1 - \frac{T_i}{X}\right)^{p(h_i-1)} + O(\lambda^p).$$

Posons $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(pr-1)} X$ et $A_0(T) := Q_0/X^{\sum h_i}$. Il vient :

$$\begin{aligned}\frac{f(X)}{(X^{\sum h_i})^p} &= A_0(T)^p + \lambda^p\alpha^p \left(\frac{1}{T}\right)^{pr-1} \prod_{i=1}^{r} \left(1 - T_i \left(\frac{\lambda^p}{\rho^{p^2-p}}\right)^{\frac{1}{pr-1}} \frac{1}{T}\right)^{p(h_i-1)} + o(\lambda^p) \\ &= A_0(T)^p + \lambda^p\alpha^p \left(\frac{1}{T}\right)^{pr-1} + o(\lambda^p).\end{aligned}$$

Si on fait les changements de variables $Y/X^{\sum h_i} := \lambda Z + A_0$, on trouve en réduction $z^p - z = \overline{\alpha}^p (1/t)^{pr-1}$. On a ainsi l'égalité entre les différentes générique et spéciale du revêtement, ce qui démontre la bonne réduction (cf. Théorème 1.2.1).

Si on change p_i en $p_i + p\beta_i$ avec $\beta_i \in R$, alors on ne fait que rajouter des termes nuls modulo λ^p, ce qui ne change pas la démonstration.

□

4.2 Revêtements galoisiens de groupe $(\mathbb{Z}/p\mathbb{Z})^2$

Nous commençons par donner des exemples de réalisations de $(\mathbb{Z}/p\mathbb{Z})^n$ pour $n = 2$. Supposons que l'on a un revêtement galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^2$ sur $\mathrm{Spec}R[[Z]]$ obtenu à partir de deux revêtements du même type qu'au Lemme 4.1.1 (donnés par des équations $Y_1^p = f_1(X)$, $Y_2^p = f_2(X)$). Les formes différentielles exactes qui apparaissent sur la composante interne sont de la forme :

$$\omega_1 := \frac{u_1 \mathrm{d}x}{\prod_{i=1}^{r}(x - t_i)^p} \quad \text{et} \quad \omega_2 := \frac{u_2 \mathrm{d}x}{\prod_{i=1}^{r}(x - \hat{t}_i)^p}$$

où u_1 et u_2 sont deux éléments $\mathbb{F}_p$-indépendants de k. Tout autre revêtement intermédiaire d'ordre p est de la forme $Y^p = f_1^i f_2^j$ (pour $1 \leq i, j \leq p-1$), et on montre que la forme différentielle exacte correspondante est $i\omega_1 + j\omega_2$. On doit donc avoir des $\mathbb{F}_p$-espaces vectoriels de formes différentielles exactes (analogues aux $L_{m+1,2}$). La combinatoire sur les t_i est alors la même que pour les $L_{m+1,2}$, i.e :

- r est un multiple de p, disons $r = qp$.
- les t_i se répartissent en $(p+1)$ paquets de q points que l'on renumérote $t^r_{[i,j]}$ pour $1 \leq r \leq q$ et $[i,j] \in \mathbb{P}^1(\mathbb{F}_p)$.

– on note $\sigma^r_{[i,j]}$ la r-ième fonction symétrique des $t^\ell_{[i,j]}$ $(1 \leq \ell \leq q)$. Les $\sigma^r_{[i,j]}$ doivent vérifier les relations homographiques :

$$\sigma^r_{[i,j]} = \frac{iu_1\sigma^r_{[1,0]} + ju_2\sigma^r_{[0,1]}}{iu_1 + ju_2}.$$

On va donc fournir une construction explicite de ces revêtements en suivant les observations faites juste avant. Soient $u_1, u_2 \in k$, $\mathbb{F}_p$-indépendants et $U_1, U_2 \in W(k)$ des relèvements. Soit $q \in \mathbb{N}^*$, soient $t^r_{[1,0]}$, $t^r_{[0,1]}$ $(1 \leq r \leq q)$, $2q$ points distincts de k. Soient $T^r_{[1,0]} \in W(k)$ (resp.$T^r_{[0,1]} \in W(k)$) des relèvements de $t^r_{[1,0]}$ (resp. $t^r_{[0,1]}$). Pour tout $r \in \{1, \cdots, q\}$ et pour tout $[i,j] \in \mathbb{P}^1(\mathbb{F}_p)$ on définit $T^r_{[i,j]}$ à partir des relations :

$$\sigma^r_{[i,j]} = \frac{iU_1\sigma^r_{[1,0]} + jU_2\sigma^r_{[0,1]}}{iU_1 + jU_2}.$$

où $\sigma^r_{[i,j]}$ est la r-ième fonction symétrique des $T^\ell_{[i,j]}$ $(1 \leq \ell \leq q)$. On pose :

$$Q_1(T) := \prod_{j=0}^{p-1}\prod_{r=1}^{q}\left(T - T^r_{[1,j]}\right) \qquad Q_2(T) := \prod_{i=0}^{p-1}\prod_{r=1}^{q}\left(T - T^r_{[i,1]}\right)$$

et

$$p^r_{[i,j]} := \frac{1}{Q_1'\left(T^r_{[i,j]}\right)^p} \quad \text{si } i \neq 0$$

$$\hat{p}^r_{[i,j]} := -\frac{(\frac{U_1}{U_2})^p}{Q_2'\left(T^r_{[i,j]}\right)^p \frac{j}{i}} \quad \text{si } ij \neq 0$$

$$p^r_{[0,1]} := \hat{p}^r_{[0,1]} := \frac{(\frac{U_1}{U_2})^p}{Q_2'\left(T^r_{[0,1]}\right)^p}.$$

Posons enfin $h_{[i,1]} := 1/i \in \mathbb{Z}/p\mathbb{Z}$ si $i \neq 0$ et $h_{[0,1]} := 1$.

On peut maintenant énoncer le théorème suivant :

Théorème 4.2.1 *Posons :*

$$f_1(X) := \prod_{j=0}^{p-1}\prod_{r=1}^{q}\left[(X - T^r_{[1,j]})^p + \rho^{p^2-p}p^r_{[1,j]}X\right]$$

et

$$f_2(X) := \prod_{i=0}^{p-1}\prod_{r=1}^{q}\left[(X - T^r_{[i,1]})^p + \rho^{p^2-p}p^r_{[i,1]}X\right]^{h_{[i,1]}}.$$

Notons $C_j \longrightarrow \mathbb{P}^1$ le revêtement donné par l'équation $Y_j^p = f_j(X)$. Alors le produit fibré de ces deux revêtements induit après normalisation un revêtement de $\mathbb{P}^1_K$ galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^2$ ayant bonne réduction relativement à la valuation de Gauss en $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(qp^2-1)} X$. La fibre spéciale du modèle lisse correspondant est un revêtement étale galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^2$ de la droite affine $\mathbb{A}^1_k$.

Démonstration : Le premier revêtement d'équation $Y_1^p = f_1$ a bonne réduction pour la valuation de Gauss en $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(qp^2-1)} X$ (voir Lemme 4.1.1). Par ce même lemme, on sait que le revêtement d'équation $Y^p = \hat{f}_2$ où :

$$\hat{f}_2(X) := \prod_{i=0}^{p-1}\prod_{r=1}^{q}\left[(X - T^r_{[i,1]})^p + \rho^{p^2-p}\hat{p}^r_{[i,1]}X\right]^{h_{[i,1]}}$$

a bonne réduction pour la même valuation de Gauss. Il suffit donc de montrer les congruences

$$p^r_{[i,j]} \equiv \hat{p}^r_{[i,j]} \mod p \quad \text{si} \quad ij \neq 0$$

pour conclure que le revêtement d'équation $Y_2^p = f_2$ a bonne réduction pour cette valuation (voir la dernière assertion du Lemme 4.1.1). On calcule :

$$\begin{aligned}
\frac{Q_1'\left(T^r_{[i,j]}\right)}{Q_2'\left(T^r_{[i,j]}\right)} &= \frac{\prod_{\ell=1}^{q}\left(T^r_{[i,j]} - T^\ell_{[1,0]}\right)}{\prod_{\ell=1}^{q}\left(T^r_{[i,j]} - T^\ell_{[0,1]}\right)} \\
&= \frac{\sum_{\ell=0}^{q}\left(T^r_{[i,j]}\right)^\ell (-1)^{(q-\ell)}\sigma^{q-\ell}_{[1,0]}}{\sum_{\ell=0}^{q}\left(T^r_{[i,j]}\right)^\ell (-1)^{(q-\ell)}\sigma^{q-\ell}_{[0,1]}} \\
&= \frac{\sum_{\ell=0}^{q}\left(T^r_{[i,j]}\right)^\ell \frac{(-1)^{(q-\ell)}}{iU_1}\left[\sigma^{q-\ell}_{[i,j]}(iU_1 + jU_2) - jU_2\sigma^{q-\ell}_{[0,1]}\right]}{\sum_{\ell=0}^{q}\left(T^r_{[i,j]}\right)^\ell (-1)^{(q-\ell)}\sigma^{q-\ell}_{[0,1]}} \\
&= \frac{-\sum_{\ell=0}^{q}\frac{jU_2}{iU_1}\left(T^r_{[i,j]}\right)^\ell (-1)^{(q-\ell)}\sigma^{q-\ell}_{[0,1]}}{\sum_{\ell=0}^{q}\left(T^r_{[i,j]}\right)^\ell (-1)^{(q-\ell)}\sigma^{q-\ell}_{[0,1]}} \\
&= -\frac{jU_2}{iU_1}
\end{aligned}$$

d'où les congruences annoncées.

Les deux revêtements du théorème ont donc simultanément bonne réduction pour la valuation de Gauss en $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(qp^2-1)} X$, cette réduction étant donnée par les équations :

$$\begin{cases} z_1^p - z_1 &= \frac{1}{tqp^2-1} \\ z_2^p - z_2 &= \left(\frac{u_1}{u_2}\right)^p \frac{1}{tqp^2-1} \end{cases}$$

et ont chacun qp^2 points de branchement. Le nombre de points de branchement en commun est exactement $q(p-1)p$, donc on peut appliquer le Théorème 1.4.2 ce qui achève la démonstration.

□

4.3 Revêtements galoisiens de groupe $(\mathbb{Z}/p\mathbb{Z})^n$

Nous allons donner une généralisation de ce théorème pour n quelconque. Pour ne pas alourdir la démonstration nous ne donnons qu'un exemple où le nombre de points de branchement de chaque revêtement d'ordre p est p^n (on peut en construire avec qp^n points de branchements pour tout $q \geq 1$).

On a d'abord besoin de quelques lemmes. On note $I^n := \{0, 1, \cdots, p-1\}^n$ et $I^n_{jr} := \{(\epsilon_1, \cdots, \epsilon_n) \in I^n, \epsilon_j = \epsilon_r = 0\}$. On notera également $\tilde{\imath}$ le multi-indice $(i_1, \cdots, i_n)$.

Lemme 4.3.1 *Soient $u_1, \cdots, u_n$ des éléments $\mathbb{F}_p$-indépendants de k, $(n \geq 2)$. On pose pour $r \in \{2, \cdots, n\}$:*

$$Ad_{1r}(x) := \prod_{\tilde{\epsilon} \in I^n_{1r}} (x + \sum_{j=1}^{n} \epsilon_j u_j)$$

et $v_r := (Ad_{1r}(u_1))/(Ad_{1r}(u_r))$. Remarquons que $\deg_{u_n}(v_r) = 0$ pour $r < n$ et que $\deg_{u_n}(v_n) = -p^{n-2}$. Posons

$$A_n(u_1, \cdots, u_n) := \begin{vmatrix} 1 & \cdots & 1 \\ v_2 & \cdots & v_2^{p^{n-1}} \\ \vdots & & \vdots \\ v_n & \cdots & v_n^{p^{n-1}} \end{vmatrix}.$$

Alors la fraction rationnelle $A_n(u_1, \cdots, u_n)$ n'est pas identiquement nulle.

Démonstration : On raisonne par récurrence sur n :

- $n = 2$: $A_2(u_1, u_2) = (u_1/u_2)^p - (u_1/u_2) \neq 0$
- Supposons que $A_{n-1}(u_1, \cdots, u_{n-1}) \neq 0$. Le terme de plus bas degré en u_n dans A_n est $v_n^{p^{n-1}} f(u_1, \cdots, u_n)$ en posant :

$$f(u_1,\cdots,u_n) := \begin{vmatrix} 1 & \cdots & 1 \\ v_2 & \cdots & v_2^{p^{n-2}} \\ \vdots & & \vdots \\ v_{n-1} & \cdots & v_{n-1}^{p^{n-2}} \end{vmatrix}.$$

Or $f(u_1,\cdots,u_{n-1},0) = A_{n-1}(u_1,\cdots,u_{n-1})^p \neq 0$, donc le terme de plus bas degré en u_n dans A_n est non identiquement nul et par conséquent A_n aussi.

□

Par la suite, on dira que $(u_1,\cdots,u_n)$ vérifie la condition $(*)$ si $A_n(u_1,\cdots,u_n) \neq 0$.

Lemme 4.3.2 *Soient $t_1,\cdots,t_n$ des éléments distincts de k, et $u_1,\cdots,u_n$, n éléments $\mathbb{F}_p$-indépendants de k. Alors $\exists \beta_1,\cdots,\beta_n \in k$ tels que :*

$$\left\{ \frac{\sum_{j=1}^n i_j u_j \sum_{i=1}^{n-1} \beta_i t_j^i}{\sum_{j=1}^n i_j u_j}, \tilde{i} \in \mathbb{P}^{n-1}(\mathbb{F}_p) \right\}$$

soit de cardinal $p^{n-1}+\cdots+p+1$.

Démonstration : Soit

$$\begin{array}{rccc} \Phi & : & \mathbb{P}^{n-1}(\mathbb{F}_p) & \longrightarrow & \mathbb{P}^{n-1}(k) \\ & & [i_1,\cdots,i_n] & \longmapsto & [\sum_{j=1}^n i_j u_j, \sum_{j=1}^n i_j u_j t_j, \cdots, \sum_{j=1}^n i_j u_j t_j^{n-1}]. \end{array}$$

L'application Φ est injective car sa matrice est de type Vandermonde. De plus les u_i sont $\mathbb{F}_p$-indépendants, donc $Im(\Phi)$ est en bijection avec l'ensemble :

$$E := \left\{ \left(\frac{\sum_{j=1}^n i_j u_j t_j}{\sum_{j=1}^n i_j u_j}, \cdots, \frac{\sum_{j=1}^n i_j u_j t_j^{n-1}}{\sum_{j=1}^n i_j u_j} \right) \right\} \subset k^{n-1},$$

qui est donc un ensemble à $p^{n-1}+\cdots+p+1$ éléments.

Soit

$$\begin{array}{rccc} \Psi & : & k^{n-1} & \longrightarrow & k \\ & & (x_1,\cdots,x_{n-1}) & \longmapsto & \sum_{i=1}^{n-1} \beta_i x_i. \end{array}$$

Alors on peut choisir les β_i tels que $\Psi(E)$ soit un ensemble à $p^{n-1}+\cdots+p+1$ éléments (il suffit de prendre $(\beta_1,\cdots,\beta_{n-1})$ dans le complémentaire de $p^{n-1}+\cdots+p+1$ hyperplans de k^{n-1}).

□

Soient $u_1, \cdots, u_n \in k$, $\mathbb{F}_p$-indépendants vérifiant la condition $(*)$ et $U_1, \cdots, U_n \in W(k)$ des relèvements. Soient $t_1, \cdots, t_n \in k$ des éléments distincts de k et $T_1, \cdots, T_n \in W(k)$ des relèvements correspondants. Soit $\phi \in W(k)[X]$ de degré $\leq n-1$ tel que les

$$\frac{\sum_{j=1}^n i_j u_j \overline{\phi(t_j)}}{\sum_{j=1}^n i_j u_j}$$

soient tous différents pour $\tilde{i} \in \mathbb{P}^{n-1}(\mathbb{F}_p)$ (un tel ϕ existe d'après le lemme précédent). On pose alors :

$$T_{\tilde{i}} := \frac{\sum_{j=1}^n i_j U_j \phi(T_j)}{\sum_{j=1}^n i_j U_j}.$$

Pour $j \in \{1, \cdots n\}$, on pose

$$Q_j(T) := \prod_{\substack{\tilde{i} \in \mathbb{P}^{n-1}(\mathbb{F}_p) \\ i_j \neq 0}} (T - T_{\tilde{i}}).$$

Pour tout $\tilde{i} \in \mathbb{P}^{n-1}(\mathbb{F}_p)$ tel que $i_j \neq 0$, on définit par récurrence sur j les entiers $h_{\tilde{i}}^j$:
- $h_{\tilde{i}}^1 := 1$
- Soit $j \geq 2$:
  - Si $i_r = 0$ pour tout $r < j$, on pose $h_{\tilde{i}}^j := 1$.
  - Sinon on pose $h_{\tilde{i}}^j := i_j / i_r h_{\tilde{i}}^r$ pour tout $r < j$ tel que $i_r \neq 0$ (on vérifie facilement que cette définition ne dépend pas de r).

Soient $V_r \in W(k)$ un relèvement de v_r pour $1 \leq r \leq n$ (on rappelle que v_r est défini au Lemme 4.3.1). Posons $\alpha_1 := 1$ et $\alpha_r := -V_r$ pour $2 \leq r \leq n$. On définit enfin $p_{\tilde{i}}^j$ pour $i_j \neq 0$:

$$p_{\tilde{i}}^j := \frac{\alpha_j^p}{h_{\tilde{i}}^j Q_j'(T_{\tilde{i}})^p}.$$

On a alors le lemme suivant :

Lemme 4.3.3 *Soient $j, r \in \{1, \cdots, n\}$ tels que $j \neq r$ et $\tilde{i} \in \mathbb{P}^{n-1}(\mathbb{F}_p)$ tel que $i_j i_r \neq 0$. Alors $p_{\tilde{i}}^j \equiv p_{\tilde{i}}^r \ mod\ p$.*

Démonstration : On note $J_{ab}^n := \{(\epsilon_1, \cdots, \epsilon_n) \in \mathbb{P}^{n-1}(\mathbb{F}_p), \epsilon_a = 1, \epsilon_b = 0\}$. On a :

$$\frac{Q_j'(T_{\tilde{i}})}{Q_r'(T_{\tilde{i}})} = \frac{\prod\limits_{\substack{\tilde{\epsilon} \in \mathbb{P}^{n-1}(\mathbb{F}_p) \\ \epsilon_j \neq 0, \tilde{\epsilon} \neq \tilde{i}}} (T_{\tilde{i}} - T_{\tilde{\epsilon}})}{\prod\limits_{\substack{\tilde{\epsilon} \in \mathbb{P}^{n-1}(\mathbb{F}_p) \\ \epsilon_r \neq 0, \tilde{\epsilon} \neq \tilde{i}}} (T_{\tilde{i}} - T_{\tilde{\epsilon}})} = \frac{\prod\limits_{\tilde{\epsilon} \in J_{jr}^n} (T_{\tilde{i}} - T_{\tilde{\epsilon}})}{\prod\limits_{\tilde{\epsilon} \in J_{rj}^n} (T_{\tilde{i}} - T_{\tilde{\epsilon}})}.$$

Posons

$$\psi_{jr} := \prod_{\tilde{\epsilon} \in J_{jr}^n} (T_{\tilde{i}} - T_{\tilde{\epsilon}}) \quad \text{et} \quad \psi_{rj} := \prod_{\tilde{\epsilon} \in J_{rj}^n} (T_{\tilde{i}} - T_{\tilde{\epsilon}}).$$

Alors

$$\psi_{jr} = \prod_{\tilde{\epsilon}\in J^n_{jr}} \frac{U_j \sum_{\ell\neq j} i_\ell U_\ell(\phi(T_\ell)-\phi(T_j)) + \sum_{\ell\neq j,r} \epsilon_\ell U_\ell[i_jU_j(\phi(T_j)-\phi(T_\ell)) + i_rU_r(\phi(T_r)-\phi(T_\ell))]}{\left(\sum_{\ell=1}^n i_\ell U_\ell\right)\left(U_j + \sum_{\ell\neq j,r}\epsilon_\ell U_\ell\right)}.$$

Posons

$$A_{jr}(x) := \prod_{\tilde{\epsilon}\in I^n_{jr}} \left(x + \sum_{\ell\neq j,r} \epsilon_\ell U_\ell[i_jU_j(\phi(T_j)-\phi(T_\ell)) + i_rU_r(\phi(T_r)-\phi(T_\ell))]\right)$$

$$Ad_{jr}(x) := \prod_{\tilde{\epsilon}\in I^n_{jr}} \left(x + \sum_{\ell=1}^n \epsilon_\ell U_\ell\right)$$

et

$$M := \left(\sum_{\ell=1}^n i_\ell U_\ell\right)^{p^{n-2}}$$

(A_{jr} et Ad_{jr} sont des polynômes additifs en réduction modulo p).

Alors

$$\psi_{jr} = \frac{A_{jr}\left(U_j \sum_{\ell\neq j} i_\ell U_\ell(\phi(T_\ell)-\phi(T_j))\right)}{M\,Ad_{jr}(U_j)}$$

et de même

$$\psi_{rj} = \frac{A_{jr}\left(U_r \sum_{\ell\neq r} i_\ell U_\ell(\phi(T_\ell)-\phi(T_r))\right)}{M\,Ad_{jr}(U_r)}.$$

Montrons que $B_{jr} := M(\psi_{jr}Ad_{jr}(U_j)i_j + \psi_{rj}Ad_{jr}(U_r)i_r) \equiv 0\ [p]$.

$$\begin{aligned}
B_{jr} &\equiv A_{jr}\left(\sum_{\ell\neq j} i_jU_ji_\ell U_\ell(\phi(T_\ell)-\phi(T_j)) + \sum_{\ell\neq r} i_rU_ri_\ell U_\ell(\phi(T_\ell)-\phi(T_r))\right)\ [p]\\
&\equiv A_{jr}\left(\sum_{\ell\neq j,r} i_jU_ji_\ell U_\ell(\phi(T_\ell)-\phi(T_j)) + i_rU_ri_\ell U_\ell(\phi(T_\ell)-\phi(T_r))\right)\ [p]\\
&\equiv A_{jr}\left(\sum_{\ell\neq j,r} i_\ell U_\ell(i_jU_j(\phi(T_\ell)-\phi(T_j)) + i_rU_r(\phi(T_\ell)-\phi(T_r)))\right)\ [p]\\
&\equiv 0\ [p].
\end{aligned}$$

On en déduit donc que :

$$\frac{Q'_j(T_i)}{Q'_r(T_i)} \equiv -\frac{Ad_{jr}(U_r)i_r}{Ad_{jr}(U_j)i_j} \ [p].$$

Si j et r sont différents de 1, on note $I^n_{1jr} := \{(\epsilon_1, \cdots, \epsilon_n) \in I^n, \epsilon_1 = \epsilon_j = \epsilon_r = 0\}$ et on définit :

$$Ad_{1jr}(x) := \prod_{\bar{\epsilon} \in I^n_{1jr}} (x + \sum_{j=1}^{n} \epsilon_j U_j).$$

On a alors les identités :

$$\begin{aligned} Ad_{jr}(x) &\equiv Ad_{1jr}(x)^p - Ad_{1jr}(x)Ad_{1jr}(U_1)^{p-1} \ [p] \\ Ad_{1r}(x) &\equiv Ad_{1jr}(x)^p - Ad_{1jr}(x)Ad_{1jr}(U_j)^{p-1} \ [p] \\ Ad_{1j}(x) &\equiv Ad_{1jr}(x)^p - Ad_{1jr}(x)Ad_{1jr}(U_r)^{p-1} \ [p] \end{aligned}$$

et donc,

$$\begin{aligned} \frac{Ad_{jr}(U_r)}{Ad_{jr}(U_j)} &\equiv \frac{Ad_{1jr}(U_r)^p - Ad_{1jr}(U_r)Ad_{1jr}(U_1)^{p-1}}{Ad_{1jr}(U_j)^p - Ad_{1jr}(U_j)Ad_{1jr}(U_1)^{p-1}} \ [p] \\ &\equiv -\frac{Ad_{1j}(U_1)}{Ad_{1j}(U_j)}\frac{Ad_{1r}(U_r)}{Ad_{1r}(U_1)} \ [p] \\ &\equiv -\frac{\alpha_j}{\alpha_r} \ [p]. \end{aligned}$$

On obtient donc,

$$\frac{Q'_j(T_i)}{Q'_r(T_i)} \equiv \frac{\alpha_j i_r}{\alpha_r i_j} \ [p]$$

et finalement :

$$p_i^j \equiv \frac{\alpha_j^p}{h_i^j Q'_j(T_i)^p} \equiv \frac{\alpha_j^p}{h_i^j Q'_r(T_i)^p \frac{\alpha_j^p i_r^p}{\alpha_r^p i_j^p}} \equiv \frac{\alpha_r^p}{h_i^r Q'_r(T_i)^p} \equiv p_i^r \ [p].$$

Dans le cas où l'un des deux indices j, r vaut 1, la fin de la démonstration est encore plus directe.

□

Par la suite on notera p_i à la place de p_i^j (p_i est ainsi défini modulo l'addition d'un multiple de p).

En conservant les mêmes notations que pour le lemme précédent, on peut énoncer le théorème suivant :

Théorème 4.3.4 *Posons :*

$$f_j(X) := \prod_{\substack{\tilde{\epsilon}\in\mathbb{P}^{n-1}(\mathbb{F}_p)\\ \epsilon_j\neq 0}} \left[(X-T_{\tilde{\epsilon}})^p + \rho^{p^2-p}p_{\tilde{\epsilon}}X\right]^{h^j_{\tilde{\epsilon}}}.$$

Notons $C_j \longrightarrow \mathbb{P}^1$ le revêtement donné par l'équation $Y_j^p = f_j(X)$. Alors le produit fibré de ces n revêtements induit après normalisation un revêtement de $\mathbb{P}^1_K$ galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^n$ ayant bonne réduction relativement à la valuation de Gauss en $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(p^n-1)} X$. La fibre spéciale du modèle lisse correspondant est un revêtement étale galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^n$ de la droite affine $\mathbb{A}^1_k$.

Démonstration : D'après le Lemme 4.1.1, tous les revêtements $C_j \longrightarrow \mathbb{P}^1$ ont bonne réduction relativement à la valuation de Gauss en $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(p^n-1)} X$, la réduction étant $z_j^p - z_j = \overline{\alpha_j}^p\,(1/t))^{p^n-1}$. Le produit fibré $C_1 \times_{\mathbb{P}^1} \cdots \times_{\mathbb{P}^1} C_n$ induit après normalisation un revêtement $C \longrightarrow \mathbb{P}^1_K$ galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^n$. Vu que les α_j sont $\mathbb{F}_p$-indépendants (cf. Lemme 4.3.1), on a à la fibre spéciale un revêtement galoisien de groupe $(\mathbb{Z}/p\mathbb{Z})^n$.

Il reste à montrer que le revêtement $C \longrightarrow \mathbb{P}^1_K$ a bonne réduction sur R, i.e, à comparer les degrés respectifs des différentes spéciales et génériques du revêtement (que l'on note d_s et d_η).

On a $d_s = (m+1)(p-1)(p^{n-1}+\cdots+p+1)$ avec $m = p^n-1$, donc $d_s = p^n(p^n-1)$. D'autre part, le lieu de branchement de $C \longrightarrow \mathbb{P}^1_K$ est à chercher parmi les racines des polynômes $(X-T_{\tilde{\epsilon}})^p + \rho^{p^2-p}p_{\tilde{\epsilon}}X$ pour $\tilde{\epsilon}\in\mathbb{P}^{n-1}(\mathbb{F}_p)$, ce qui fait au plus $p(p^{n-1}+\cdots+p+1)$ points. Vu que les groupes d'inertie sont cycliques d'ordre p, on en déduit que :

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

On obtient alors la bonne réduction en appliquant le Théorème 1.2.1.

□

Chapitre 5

Relèvement d'actions de $(\mathbb{Z}/2\mathbb{Z})^2$ sur $k[[z]]$

Dans ce chapitre nous montrons qu'il n'y a pas d'obstructions au relèvement d'actions de $(\mathbb{Z}/2\mathbb{Z})^2$ sur $k[[t]]$. On démontre ce résultat en donnant des équations explicites du relèvement. On utilise pour ce faire le Lemme 5.1.2 qui est une variante plus fine du Lemme 4.1.1.

5.1 Deux lemmes

On commence par énoncer les deux lemmes suivants :

Lemme 5.1.1 *1. Soient $t_1, \cdots, t_r \in k$ distincts deux à deux.*
Posons $q(x) := \prod_{i=1}^{r}(x - t_i)$ et

$$\tilde{q}(x) := \sum_{i=1}^{r} \frac{1}{(q'(t_i))^p} \prod_{j \neq i} (x - t_j)^{p-1}.$$

Alors la forme différentielle $\omega := \mathrm{d}x/q(x)^p$ est exacte et vaut $d(\tilde{q}/q^{p-1})$. On a en outre $(\tilde{q}q)'(x) = 1$.

2. Soient $T_1, \cdots, T_r \in R$ distincts deux à deux.
Posons $Q(X) := \prod_{i=1}^{r}(X - T_i)$ et

$$P(X) := \sum_{i=1}^{r} \frac{1}{(Q'(T_i))^p} \prod_{j \neq i} (X - T_j)^{p-1}.$$

Alors il existe $H \in R[X]$ tel que $P(X)Q(X) = X + H(X)^p \mod p$

Démonstration :

1. On part de la décomposition en éléments simples :

$$\frac{1}{q(x)} = \sum_{i=1}^{r} \frac{1}{q'(t_i)} \frac{1}{(x - t_i)}$$

ce qui donne en prenant la puissance p-ième :

$$\frac{1}{q(x)^p} = \sum_{i=1}^{r} \frac{1}{(q'(t_i))^p} \frac{1}{(x-t_i)^p} = \left(\frac{\tilde{q}(x)}{q^{p-1}(x)}\right)'.$$

En particulier $(\tilde{q}q)'(x) = 1$.

2. Le raisonnement effectué juste avant montre que

$$\left(\frac{P}{Q^{p-1}}\right)'(X) = \frac{1}{Q(X)^p} \mod p$$

ce qui implique le résultat annoncé.

□

Lemme 5.1.2 *Soit ζ une racine p-ième de l'unité et $\lambda := \zeta - 1$. Soit $\rho \in W(k)^{\mathrm{alg}}$ tel que $|\lambda|^{1/(p-1)} < |\rho| \leq |\lambda|^{1/(2(p-1))}$ Soient $T_1, \cdots, T_r \in R$ tels que $|T_i - T_j| = 1$ pour tout $i \neq j$ et $Q(X) := \prod_{i=1}^{r}(X - T_i)$. Soit $\alpha \in R$ inversible et $h_1, \cdots, h_r \in \mathbb{Z} - p\mathbb{Z}$. Pour tout i on fait le choix d'une racine p-ième de T_i que l'on note $T_i^{1/p}$. Posons*

$$s_i := \frac{\alpha T_i^{\frac{1}{p}}}{h_i Q'(T_i)}$$

et

$$p_i := \frac{\alpha^p}{h_i Q'(T_i)^p}.$$

On définit enfin le polynôme f :

$$f(X) := \prod_{i=1}^{r} \left[(X-T_i)^p - p\rho^{p-1}s_i(X-T_i)^{p-1} + \rho^{p^2-p}p_i(X-T_i)\right]^{h_i}.$$

Alors le revêtement d'équation $Y^p = f(X)$ a bonne réduction relativement à la valuation de Gauss en $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(pr-1)} X$, cette réduction étant $z^p - z = \overline{\alpha}^p (1/t)^{pr-1}$. De plus la géométrie du lieu de branchement a la forme donnée par la figure 5.1 :

De plus, si on change s_i (resp. p_i) en $s_i + p\beta_i$ (resp. $p_i + p\gamma_i$) avec $\beta_i, \gamma_i \in R$, le lemme reste encore vrai (i.e on ne modifie pas la géométrie du lieu de branchement et on a toujours la bonne réduction.)

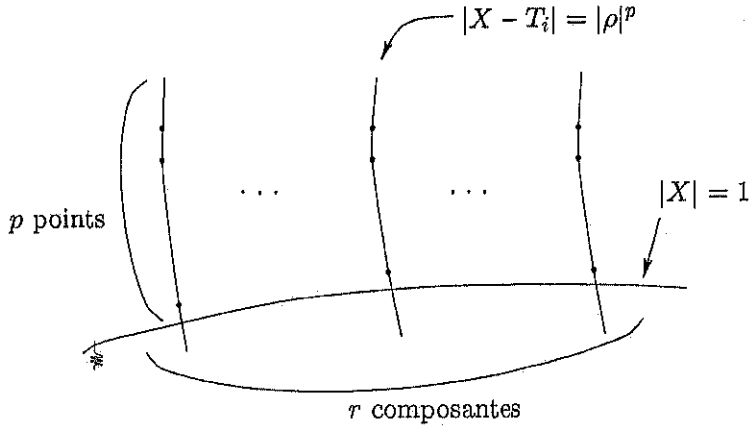


FIG. 5.1 – Géométrie du lieu de branchement

Ce lemme est un peu plus fort que le Lemme 4.1.1 dans la mesure où l'on impose que le revêtement soit branché en les points T_i.
Démonstration : On pose $Q_0(X) := \prod_{i=1}^{r}(X - T_i)^{h_i}$ et on écrit $O(\lambda^p)$ pour désigner des termes de valuation supérieure ou égale à $pv(\lambda)$. On a :

$$f(X) = \prod_{i=1}^{r}[(X - T_i)^{ph_i} + h_i p_i \rho^{p^2-p}(X - T_i)^{1+p(h_i-1)} - p\rho^{p-1}h_i s_i (X - T_i)^{ph_i-1} + O(\lambda^p)]$$

(cette égalité vient du fait que l'on a pris $|\lambda|^{1/(p-1)} < |\rho| \leq |\lambda|^{1/(2(p-1))}$).

$$\begin{aligned} f(X) &= Q_0^p + \rho^{p^2-p}\sum_{i=1}^{r} p_i h_i (X - T_i)^{1+p(h_i-1)} \prod_{j\neq i}(X - T_j)^{ph_j} \\ &\quad -p\rho^{p-1}\sum_{i=1}^{r} s_i h_i (X - T_i)^{ph_i-1} \prod_{j\neq i}(X - T_j)^{ph_j} + O(\lambda^p) \\ &= Q_0^p + \rho^{p^2-p} Q\left[\sum_{i=1}^{r} p_i h_i \prod_{j\neq i}(X - T_j)^{p-1}\right] \prod_{i=1}^{r}(X - T_i)^{p(h_i-1)} \\ &\quad -p\rho^{p-1}Q_0^{p-1}\left[\sum_{i=1}^{r} s_i h_i \prod_{j\neq i}(X - T_j)\right] \prod_{i=1}^{r}(X - T_i)^{(h_i-1)} + O(\lambda^p). \end{aligned}$$

Or d'après le Lemme 5.1.1 on sait que

$$Q\left[\sum_{i=1}^{r} p_i h_i \prod_{j\neq i}(X - T_j)^{p-1}\right] = \alpha^p(X + H(X)^p) \mod p,$$

donc :

$$\begin{aligned} f(X) &= Q_0^p + \rho^{p^2-p}\alpha^p H(X)^p \prod_{i=1}^{r}(X-T_i)^{p(h_i-1)} + \rho^{p^2-p}\alpha^p X \prod_{i=1}^{r}(X-T_i)^{p(h_i-1)} \\ &\quad -p\rho^{p-1}Q_0^{p-1}\left[\sum_{i=1}^{r} s_i h_i \prod_{j\neq i}(X-T_j)\right]\prod_{i=1}^{r}(X-T_i)^{(h_i-1)} + O(\lambda^p) \\ &= (Q_0 + \rho^{p-1}\alpha H(X)\prod_{i=1}^{r}(X-T_i)^{(h_i-1)})^p + \rho^{p^2-p}\alpha^p X\prod_{i=1}^{r}(X-T_i)^{p(h_i-1)} \\ &\quad -pQ_0^{p-1}\rho^{p-1}\alpha H(X)\prod_{i=1}^{r}(X-T_i)^{(h_i-1)} \\ &\quad -p\rho^{p-1}Q_0^{p-1}\left[\sum_{i=1}^{r} s_i h_i \prod_{j\neq i}(X-T_j)\right]\prod_{i=1}^{r}(X-T_i)^{(h_i-1)} + O(\lambda^p) \end{aligned}$$

$$\begin{aligned} f(X) &= A^p - p\rho^{p-1}Q_0^{p-1}\prod_{i=1}^{r}(X-T_i)^{(h_i-1)}\left[\sum_{i=1}^{r} s_i h_i \prod_{j\neq i}(X-T_j) + \alpha H(X)\right] \\ &\quad +\rho^{p^2-p}\alpha^p X\prod_{i=1}^{r}(X-T_i)^{p(h_i-1)} + O(\lambda^p) \end{aligned}$$

avec $A := Q_0 + \rho^{p-1}\alpha H(X)\prod_{i=1}^{r}(X-T_i)^{(h_i-1)}$. Or on sait que $H(T_j)^p + T_j = 0 \bmod p$ (cf. Lemme 5.1.1), donc $H(T_j) = -T_j^{1/p} \bmod \lambda^{(p-1)/p}$. On en déduit que :

$$\sum_{i=1}^{r} s_i h_i \prod_{j\neq i}(X-T_j) + \alpha H(X) = 0 \mod \lambda^{\frac{p-1}{p}}$$

(il suffit de remarquer que ce polynôme évalué en T_i vaut 0 modulo $\lambda^{(p-1)/p}$). On obtient ainsi :

$$f(X) = A^p + \rho^{p^2-p}\alpha^p X\prod_{i=1}^{r}(X-T_i)^{p(h_i-1)} + O(\lambda^p)$$

$$\frac{f(X)}{(X^{\Sigma h_i})^p} = \left(\frac{A}{X^{\Sigma h_i}}\right)^p + \rho^{p^2-p}\alpha^p \frac{1}{X^{pr-1}}\prod_{i=1}^{r}\left(1-\frac{T_i}{X}\right)^{p(h_i-1)} + O(\lambda^p).$$

Posons $T := \left(\lambda^p/\rho^{p^2-p}\right)^{1/(pr-1)} X$ et $A_0(T) := A/X^{\sum h_i}$. Il vient :

$$\begin{aligned}\frac{f(X)}{(X^{\sum h_i})^p} &= A_0(T)^p + \lambda^p \alpha^p \left(\frac{1}{T}\right)^{pr-1} \prod_{i=1}^{r} \left(1 - T_i \left(\frac{\lambda^p}{\rho^{p^2-p}}\right)^{\frac{1}{pr-1}} \frac{1}{T}\right)^{p(h_i-1)} + o(\lambda^p) \\ &= A_0(T)^p + \lambda^p \alpha^p \left(\frac{1}{T}\right)^{pr-1} + o(\lambda^p).\end{aligned}$$

Si on fait les changements de variables $Y/X^{\sum h_i} := \lambda Z + A_0$, on trouve en réduction $z^p - z = \overline{\alpha}^p (1/t)^{pr-1}$. On a ainsi l'égalité entre les différentes générique et spéciale du revêtement, ce qui démontre la bonne réduction.

Si on change s_i (resp. p_i) en $s_i + p\beta_i$ (resp. $p_i + p\gamma_i$) avec $\beta_i, \gamma_i \in R$, alors on ne fait que rajouter des termes nuls modulo λ^p, ce qui ne change pas la démonstration.

□

5.2 Le théorème

Énonçons le théorème :

Théorème 5.2.1 *Soit $G = (\mathbb{Z}/2\mathbb{Z})^2$ un groupe de k-automorphismes de $k[[z]]$. Alors on peut trouver R un anneau de valuation discrète dominant $W(k)$ tel que G se relève en un groupe de R-automorphismes de $R[[Z]]$.*

Ce théorème a déjà été montré dans le cas où chacune des sous-extensions intermédiaires de $k[[z]]^G$ de degré 2 a le même conducteur (voir le Théorème 3.2.1). Dans le cas de conducteurs différents il faut alors envisager des géométries non équidistantes.

Démonstration : L'extension $k[[z]]/k[[z]]^G$ est définie par les équations :

$$\begin{cases} y_1^2 + y_1 &= f_1\left(\frac{1}{t}\right) \\ y_2^2 + y_2 &= f_2\left(\frac{1}{t}\right). \end{cases}$$

On peut choisir t tel que

$$\begin{aligned} f_2\left(\frac{1}{t}\right) &= \frac{1}{t^{m_2}} \\ f_1\left(\frac{1}{t}\right) &= \sum_{j=0}^{\frac{m_1-1}{2}} \frac{c_j}{t^{m_1-2j}} \end{aligned}$$

avec m_1, m_2 impairs, $m_1 \leq m_2$, $c_j \in k$, et $c_0 \neq 0$. On pose $m_1 + 1 = 2m$ et $m_2 + 1 = 2m + 2n$ ($n \geq 0$). On note également $\rho_n := \lambda$, $\rho_m = \lambda^{1+2n/(2m+2n-1)}$, $\rho_0 = \lambda^{1/(2m+2n-1)}$.

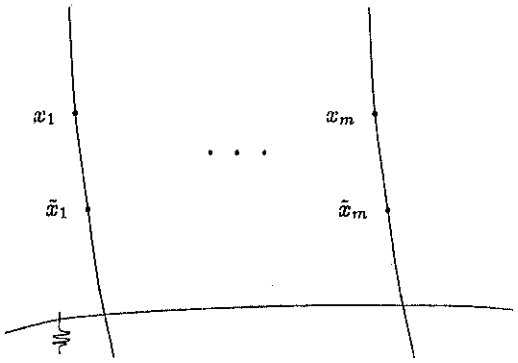


FIG. 5.2 -

Nous allons dans un premier temps exhiber un revêtement du disque ouvert p-adique qui relève le revêtement d'équation $y_1^2+y_1 = f_1\,(1/t)$ et dont la géométrie du lieu de branchement est donnée par la figure 5.2) :

Soient $T_1, \cdots, \cdots, T_m \in W(k)$ tels que $|T_i - T_j| = 1$ pour $i \neq j$. Soit $C_j \in W(k)$ relevant c_j. On applique le Lemme 5.1.2 pour $\alpha = C_0^{1/2}$, $h_i = 1$, $\rho = (\rho_m)^{1/2}$ et $r = m$. Alors il existe $\tilde{T}_1, \cdots, \tilde{T}_m \in R$ (où R est une extension finie de $W(k)$) avec $|T_i - \tilde{T}_i| = |\rho_m|$ tels que le revêtement d'équation

$$Y_1^2 = F_1(X) := \prod_{i=1}^{m}(X - T_i)(X - \tilde{T}_i)$$

a bonne réduction par rapport à la valuation de Gauss en $T = \rho_0 X$. On a donc F_1 de la forme :

$$F_1(X) = A(X)^2 + \rho_m C_0 X + O(4)$$

où $A \in R[X]$ est un polynôme de degré m (on renvoie pour cela à la démonstration du Lemme 5.1.2). Posons :

$$\tilde{F}_1(X) := F_1(X) + \rho_m \sum_{j=1}^{m-1} C_j \rho_0^{2j} X^{2j+1}$$

Posons enfin $T = \rho_0 X$. Alors :

$$\begin{aligned} \frac{\tilde{F}_1(X)}{X^{2m}} &= \left(\frac{A(X)}{X^m}\right)^2 + \rho_m \left(C_0 \left(\frac{1}{X}\right)^{2m-1} + \sum_{j=0}^{m-1} C_j \rho_0^{2j} \left(\frac{1}{X}\right)^{2m-2j-1} \right) \\ &= \tilde{A}(T)^2 + \rho_m \rho_0^{2m-1} \left(\sum_{j=1}^{m-1} C_j \left(\frac{1}{T}\right)^{2m-2j-1} \right) \end{aligned}$$

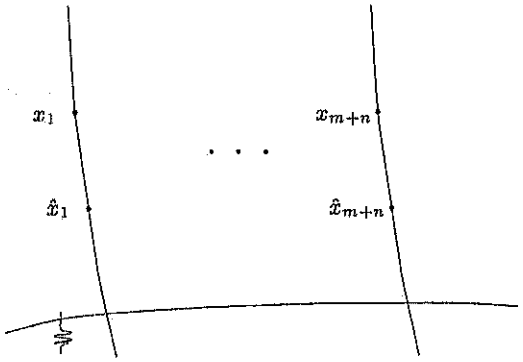
ou $\tilde{A}(T) := A(X)/X^m$. Or $\rho_m \rho_0^{2m-1} = \lambda^2$, donc si on pose $Y_1/X^m = \lambda Z_1 + \tilde{A}(T)$, alors l'équation $Y_1^p = \tilde{F}_1$ donne en réduction $z_1^2 + z_1 = \sum_{j=0}^{m-1} c_j / t^{m_1 - 2j}$. Si on écrit $\tilde{F}_1$ sous sa

forme factorisée, on trouve une expression de la forme :

$$\tilde{F}_1(X) = \prod_{i=1}^{m}(X - X_i)(X - \tilde{X}_i)$$

avec $|X_i - X_j| = 1$ si $i \neq j$ et $|X_i - \tilde{X}_i| = |\rho_m|$ pour $1 \leq i \leq m$.

Nous allons maintenant exhiber un revêtement du disque ouvert p-adique qui relève le revêtement d'équation $y_2^2 + y_2 = f_2(1/t)$ et dont la géométrie du lieu de branchement est de cette forme :



Soient $X_{n+1}, \cdots, X_{n+m} \in W(k)$ tels que $|X_i - X_j| = 1$ si $i \neq j$. On applique alors le Lemme 5.1.2 pour $\alpha = 1$, $\rho = (\rho_n)^{1/2}$ et $r = m + n$. Alors il existe $\hat{X}_1, \cdots, \hat{X}_{m+n} \in R$ avec $|X_i - \hat{X}_i| = |\rho_n|$ tels que le revêtement d'équation

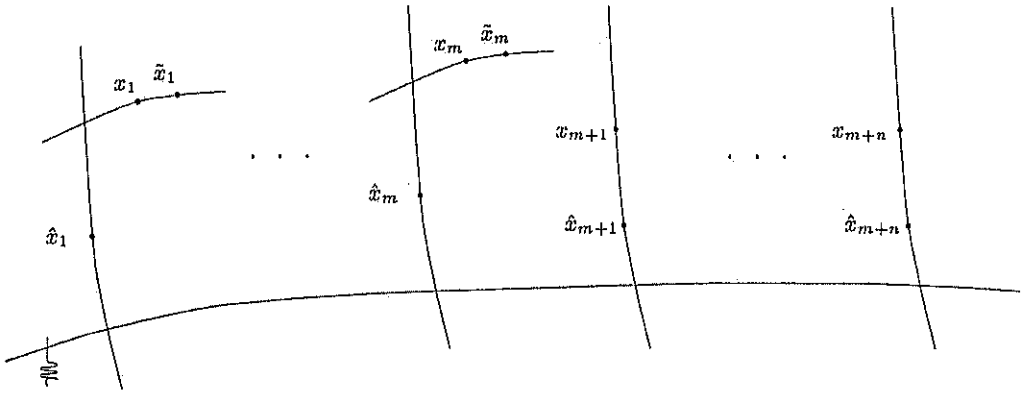
$$Y_2^2 = F_2(X) := \prod_{i=1}^{m}(X - X_i)(X - \hat{X}_i)$$

a bonne réduction par rapport à la valuation de Gauss en $T = \rho_0 X$, cette réduction étant $z_2^2 + z_2 = 1/t^{2m+2n-1}$. En outre on peut s'arranger pour que $\hat{X}_i \neq \tilde{X}_i$ pour $i \leq m$ (car d'après le Lemme 5.1.2, on peut modifier $\hat{X}_i$ par un élément de $2R$). Les deux revêtements ainsi construits ont donc simultanément bonne réduction par rapport au même paramètre et ont exactement m points de branchement en commun. On peut donc appliquer le Théorème 1.4.2, ce qui achève la démonstration.

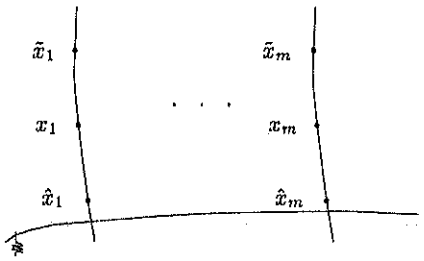
□

On peut préciser la géométrie des lieux de branchements pour les revêtements ainsi exhibés :

- Si $n \neq 0$ le modèle semi-stable minimal qui déploie le lieu de branchement des deux revêtements est :



- Si $n = 0$ alors le modèle semi-stable minimal qui déploie le lieu de branchement des deux revêtements est :



Remarque : Dans le cas où $n = 0$, ce théorème fournit une autre démonstration du Théorème 3.2.1 avec une géométrie du lieu de branchement différente.

En utilisant le principe local-global énoncé dans le Théorème 1.1.3, on a comme corollaire le théorème suivant :

Théorème 5.2.2 *Soit G un groupe et $f : C \to C/G := D$ un revêtement galoisien de groupe G, avec C et D des courbes lisses et propres sur k ($car(k) = 2$). Supposons que les groupes d'inertie en chaque point de C soient $\mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$. Alors on peut trouver R un anneau de valuation discrète dominant $W(k)$ tel que f se relève en un revêtement galoisien de groupe G entre des courbes lisses et propres sur R.*

Bibliographie

[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)

[Be-Me] J.Bertin, A.Mézard : *Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques.* Invent. Math, Vol **141**, 195-238 (2000).

[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, Vol **12**, 269-303 (1999).

[He1] Y.Henrio : *Arbres de Hurwitz et automorphismes d'ordre p des disques et des couronnes p-adiques formels.* à paraître dans Compositio Math.

[He2] Y.Henrio : *Relèvement galoisien des revêtements de courbes nodales.* Manuscripta Math, Vol **106**, 131-150 (2001).

[Ka] N.Katz : *Local-to-global extensions of representations of fundamental groups.* Ann. Inst. Fourier Grenoble, Vol **36**, 69−106 (1986).

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

[Pa] G.Pagot : *$\mathbb{F}_p$-espaces vectoriels de formes différentielles logarithmiques sur la droite projective.* à paraître dans Journal of Number Theory.