p-groupes abéliens de type $(p,\ldots,p)$ et disques ouverts p-adiques

Par

Michel Matignon

Abstract: Let k be an algebraically closed field of characteristic $p>0$, $W(k)$ its ring of Witt vectors, and R a complete discrete valuation ring dominating $W(k)$. Consider finite groups $G\simeq(\mathbb{Z}/p\mathbb{Z})^n$, $p\geq 2, n>1$. In a former paper we showed that a given realization of such a G as a group of k-automorphisms of $k[[z]]$ must satisfy some conditions in order to have a lifting as a group of R-automorphisms of $R[[Z]]$. In this note, we give for every G (all $p\geq 2, n>1$) a realization as an automorphism group of $k[[z]]$ which can be lifted as a group of R-automorphisms of $R[[Z]]$ for suitable R.

1991 AMS Subject Classification. Primary 12F12, 14G20, 14L27; Secondary 14D15, 14E22.

Key Words: abelian p-groups, order p automorphisms of open p-adic discs, fixed points, Hurwitz data, additive polynomials, semi-stable model, good reduction for $(\mathbb{Z}/p\mathbb{Z})^n$-covers of $\mathbb{P}^1$.

0. Introduction.

Soit k un corps algébriquement clos de caractéristique $p>0$ et C/k une courbe lisse complète et irréductible de genre $g=g(C)$. Dans cette note R désigne un anneau de valuation discrète complet extension finie de l'anneau des vecteurs de Witt $W(k)$ et π un paramètre uniformisant de R. Ce travail est une contribution à l'étude de la question suivante:

Relèvement global: *Soit G un sous-groupe fini de $\mathrm{Aut}_k(C)$ et soit*

$$C \longrightarrow D = C/G$$

le revêtement quotient de courbes lisses sur k. Est-il possible de trouver R comme au-dessus et un revêtement galoisien fini de courbes relatives lisses sur R, $\mathcal{C} \longrightarrow \mathcal{D} = \mathcal{C}/G$ qui relève le revêtement $C \longrightarrow D$?

Résultats:

- Si $(|G|,p)=1$ la réponse est oui pour tout R, par Grothendieck, SGA I.
- If $|G|>84(g(C)-1)$ la réponse est non due à une contradiction utilisant les bornes d'Hurwitz.
- Si G est cyclique d'ordre pe (resp. p^2e), avec $(e,p)=1$, la réponse est positive ([O-S-S], resp. [G-M 1]).
- Si G n'est pas cyclique il est facile de donner des obstructions combinatoires au relèvement portant sur la ramification supérieure des groupes d'inertie, ceci même dans le cas abélien ([G-M 1], [B]); on est ainsi amené à considérer la question suivante:

Relèvement local: *Soit G un sous-groupe fini de $\mathrm{Aut}_k k[[z]]$ est-il possible de trouver R comme au-dessus et un relèvement de G en un groupe de R-automorphismes de $R[[Z]]$? i.e. a-t-on un diagramme commutatif:*

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

Dans ([G-M 1]), utilisant les techniques de la géométrie rigide, nous avons établi un principe local-global (voir [B-M], pour une interpretation cohomologique utilisant la théorie des déformations à la Schlessinger), ce qui conduit à examiner seulement la question locale. Dans le cas où G est cyclique on a une conjecture (cf. [O1] I.7 et [O2]) qui semble raisonnable, en particulier après [G-M 1].

Conjecture. *1. Si G est cyclique d'ordre $p^n e$, avec $(e,p)=1$, la réponse (aux questions de relèvement) est positive.*
2. Pour R, on peut prendre $W(k)[\zeta_{(n)}]$ où $\zeta_{(n)}$ désigne une racine primitive n-ième de l'unité.

Dans ce travail nous nous intéressons à la forme "Galois Inverse" de cette conjecture, elle a l'avantage d'être encore une vraie question même pour les p-groupes.

Problème Galois Inverse. *Soit G un p-groupe fini, existe-t-il une réalisation de G comme groupe de k-automorphismes de $k[[z]]$ qui se relève en un groupe de R-automorphismes de $R[[Z]]$ pour un anneau de valuation discrète R fini sur $W(k)$ convenable?*

Dans ([G-M 2] II. 3.3.3) on a utilisé des groupes formels de Lubin-Tate et leurs endomorphismes pour construire des exemples d'automorphismes du disque sans inertie en π et d'ordre p^n pour tout

n ; ainsi le problème Galois Inverse a une réponse positive dans le cas cyclique (cette méthode se limite au cas cyclique puisque les sous-groupes finis, pour la composition, de l'anneau des endomorphismes d'un tel groupe formel sont cycliques!).

Nous montrons le

Théorème. *Le problème Galois Inverse a une réponse positive dans le cas des p-groupes abéliens de type $(p,p,...,p)$.*

Ce théorème est montré dans [G-M 1,2] dans le cas de $(\mathbb{Z}/p\mathbb{Z})^2$ seulement pour $p=2$ ou 3.

Afin de bien situer les difficultés nous allons d'abord rappeller les obstructions (sous forme de conditions nécessaires et suffisantes) au relèvement local dans le cas où $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$ et telles qu'elles ont été dégagées dans [G-M1] (voir aussi [B] pour une généralisation des congruences nécessaires dans le cas d'un groupe quelconque, et [G-M2] Chap. IV pour des exemples non abéliens).

Dans ce qui suit on supposera que R contient ζ, une racine primitive p-ième de l'unité, alors:

Théorème [G-M 1]. *Soit G un groupe abélien de type (p,p). Soient G_i, $1 \leq i \leq p+1$, les $p+1$ sous-groupes d'ordre p. Supposons que G est un groupe de k-automorphismes de $k[\![z]\!]$ et que les G_i sont arrangés de telle sorte que les extensions $k[\![z]\!]^{G_i}/k[\![z]\!]^G$ ont pour conducteurs m_i+1,* [1]) *avec $m_1 \leq m_2 \leq \ldots \leq m_{p+1}$. Soit $m_i'+1$ le conducteur de l'extension $k[\![z]\!]/k[\![z]\!]^{G_i}$, alors si l'on peut relever G en un groupe de R-automorphismes de $R[\![Z]\!]$ les deux cas suivant peuvent se présenter:*
1er Cas: Supposons que $m_1 < m_2$. Alors $m_1 \equiv -1 \bmod p$, $m_1' = m_2 p - m_1(p-1)$, $m_i = m_2$, et $m_i' = m_1$, pour $2 \leq i \leq p+1$.
2eme Cas: Supposons que $m_1 = m_2$. Alors $m_i = m_1 \equiv -1 \bmod p$, et $m_i' = m_1$ pour $1 \leq i \leq p+1$. Dans chacun des cas les deux revêtements $R[\![Z]\!]^{G_i}/R[\![Z]\!]^G$ for $i=1,2$ ont $(p-1)(m_1+1)/p$ points de ramification géométriques en commun.

Inversement si $m_1 \equiv -1 \bmod p$ et si l'on peut relever $k[\![z]\!]^{G_i}/k[\![z]\!]^G$ pour $i=1,2$ de manière que les revêtements correspondant aient $(p-1)(m_1+1)/p$ points de ramification géométriques en commun, alors la normalisation du compositum de ces deux revêtements relève $k[\![z]\!]/k[\![z]\!]^G$.

Contrairement à ce que l'on pourrait croire cette dernière condition n'est pas seulement de type combinatoire puisque la géométrie des points fixes d'un automorphisme σ d'ordre p du disque $X := \operatorname{Spec} R[\![Z]\!]$ obéit à des conditions métriques et différentielles (cf. [G-M 2]), par exemple supposons pour simplifier que σ n'est pas l'identité modulo π, qu'il a $m+1$ points fixes géométriques $Z = Z_i$, ($Z_0 = 0$ par exemple) avec $m < p$ alors ([G-M 2] Th. III.3.1.) ces $m+1$ points se répartissent en $m+1$ classes distinctes dans le disque fermé centré en 0 et de rayon $v(p)/m(p-1)$, de plus si l'action de σ dans l'espace tangent en Z_i est donnée par $\sigma(Z-Z_i) = \zeta^{(h_i)^{-1}}(Z-Z_i) \bmod (Z-Z_i)^2$, les entiers $h_i \bmod p$ (appelés données d'Hurwitz) régissent les équations sur la droite affine sur k définissant ces classes modulo $(\zeta-1)^{1/m}$; les solutions sont alors en nombre fini modulo les k-automorphismes de la droite affine. En fait les automorphismes qui doivent rentrer en jeu dans nos réalisations sont necessairement de grand conducteur $m+1$ (voir par exemple les congruences dans le théorème), les possibilités géométriques pour les points fixes sont alors plus difficiles à décrire et contraignantes. Dans le cas $p=2$ puisque la seule possibilité pour les données d'Hurwitz est $h_i = 1$ on peut espérer une solution avec une géométrie simple; c'est ce qui se passe et c'est un guide pour le cas général.

Je remercie Jean Marc Couveignes pour l'interêt qu'il a porté à ce travail.

[1]) Si $G_i = <\sigma_i>$, $m_i + 1 = v_z(\sigma_i(z) - z)$

I. Construction de polynômes auxiliaires

Dans ce paragraphe p désigne un nombre premier quelconque.

Pour $n \in \mathbb{N}^*$ on note $I_n := \{(\epsilon_1,...,\epsilon_n) \in \{0,1,..,p-1\}^n - (0,..,0)\}$ et $\bar{I}_n := \{0,1,..,p-1\}^n$. Dans ce qui suit nous utiliserons les polynômes suivants:

$$\pi_n(X_1,...,X_n) := \prod_{(\epsilon_1,..,\epsilon_n)\in I_n} \sum_{1\leq i\leq n} \epsilon_i X_i \in \mathbb{Z}[X_1,...,X_n]$$

$$\mathrm{Ad}\,_n(X_1,..,\hat{X}_i,..,X_n)(X_i) := \prod_{(\epsilon_1,..,\hat{\epsilon}_i,..,\epsilon_n)\in \bar{I}_{n-1}} (X_i + \sum_{1\leq j\leq n, j\neq i} \epsilon_j X_j) \in \mathbb{Z}[X_1,..,\hat{X}_i,..,X_n][X_i]$$

et

$$\Pi_n(X_1,...,X_n) := \prod_{(\epsilon_1,..,\epsilon_n)\in I_n} \sum_{1\leq i\leq n} \epsilon_i \pi_{n-1}(X_1,.,\hat{X}_i,..,X_n)(\mathrm{Ad}\,_n(X_1,..,\hat{X}_i,..,X_n)(X_i))^{p-2}$$

où $\hat{X}_i$ signifie que l'on omet X_i.

Avertissement. Le lecteur pourra lors d'une première lecture admettre ce lemme et se reporter directement à la condition (*) ci-dessous, l'utilité n'apparaissant qu'au moment de la preuve du théorème.

Lemme. *Les polynômes* $\pi_n(X_1,...,X_n)$ *et* $\Pi_n(X_1,...,X_n) \in \mathbb{Z}[X_1,...,X_n]$ *ne sont pas identiquement nuls modulo* p.

Preuve. La preuve se fait en évaluant les monômes de plus haut degré en X_n. Puisque $\mathrm{Ad}\,_n(X_1,..,\hat{X}_i,..,X_n)(X_i)$ est modulo p un polynôme additif en X_i ([Se] Chap. 5 §5), on a

$$\mathrm{Ad}\,_n(X_1,..,X_{n-1},\hat{X}_n)(X_n) = b_0X_n + b_1X_n^p + ... + X_n^{p^{n-1}} ;$$

ainsi

$$\pi_n(X_1,...,X_n) = \pi_{n-1}(X_1,...,X_{n-1}) \prod_{1\leq j\leq p-1} \mathrm{Ad}\,_n(X_1,..,X_{n-1},\hat{X}_n)(jX_n) =$$

$$-\pi_{n-1}(X_1,...,X_{n-1})[\mathrm{Ad}\,_n(X_1,..,X_{n-1},\hat{X}_n)(X_n)]^{p-1} \bmod p$$

$$= -\pi_{n-1}(X_1,...,X_{n-1})X_n^{p^{n-1}(p-1)} + ... ,$$

D'autre part pour $i < n$, on a:

$$\mathrm{Ad}\,_n(X_1,..,\hat{X}_i,..,X_n)(X_i) =$$

$$\prod_{0\leq j\leq p-1} \mathrm{Ad}\,_{n-1}(X_1,..,\hat{X}_i,..,X_{n-1})(X_i + jX_n) =$$

$$\prod_{0\leq j\leq p-1} (\mathrm{Ad}\,_{n-1}(X_1,..,\hat{X}_i,..,X_{n-1})(X_i) + j\mathrm{Ad}\,_{n-1}(X_1,..,\hat{X}_i,..,X_{n-1})(X_n)) \bmod p =$$

$$-\mathrm{Ad}\,_{n-1}(X_1,..,\hat{X}_i,..,X_{n-1})(X_i)[\mathrm{Ad}\,_{n-1}(X_1,..,\hat{X}_i,..,X_{n-1})(X_n)]^{p-1} + ... \bmod p =$$

$-\mathrm{Ad}\,_{n-1}(X_1,..,\hat{X}_i,..,X_{n-1})(X_i)X_n^{p^{n-2}(p-1)} + ... \bmod p$. Ainsi

$$\Pi_n(X_1,...,X_n) \bmod p = E \prod_{\epsilon_n\in\{0,1,..,p-1\}} \{ \prod_{(\epsilon_1,..,\epsilon_{n-1})\in I_{n-1}} [\sum_{1\leq i\leq n-1} \epsilon_i[\pi_{n-2}(X_1,.,\hat{X}_i,..,X_{n-1})$$

$$(\mathrm{Ad}_{n-1}(X_1,..,\hat{X}_i,..,X_{n-1})(X_i))^{p-2}X_n^{p^{n-2}(p-1)^2}+...]+\epsilon_n(\pi_{n-1}(X_1,...,X_{n-1})X_n^{p^{n-1}(p-2)}+...)]\}$$

et $E := \prod_{(\epsilon_1,..,\epsilon_n)=(0,...,0,\epsilon_n)\in I_n} [\epsilon_n\pi_{n-1}(X_1,...,X_{n-1})X_n^{p^{n-1}(p-2)}+...]$, d'où le lemme par récurrence sur n .

La condition (*)

Un n-uplet $(a_1,a_2,...,a_n)\in(\mathbb{Z}_p^{nr})^n$ satisfait la condition $(*)$ si: $\Pi_n(a_1,...,a_n)\neq 0 \bmod p$.
Nous utiliserons le lemme précédent sous la forme suivante:
Il existe une infinité de uples $(a_1,a_2,...,a_n)\in(\mathbb{Z}_p^{nr})^n$ satisfaisant $(*)$; i.e. les n éléments de $\mathbb{F}_p^{alg}$, $\pi_{n-1}(a_1,.,\hat{a}_i,..,a_n)(\mathrm{Ad}_n(a_1,..,\hat{a}_i,..,a_n)(a_i))^{p-2} \bmod p$ sont linéairement indépendants sur $\mathbb{F}_p$.

II. Réalisation de $(\mathbb{Z}/p\mathbb{Z})^n$, $p\geq 2, n>1$

Terminologie. Comme dans [G-M2] nous dirons qu'un revêtement de $\mathbb{P}_k^1$ est de type A_m si c'est un revêtement étale de la droite affine $\mathbb{A}_k^1$ avec conducteur $m+1$ à l'infini.

Dans ce paragraphe p est un nombre premier quelconque et $n>1$.

0. La méthode.

Expliquons la genèse des équations. Examinons d'abord les obstructions présentées dans le théorème rappelé dans l'introduction. Supposons construits deux revêtements $Y_i^p = f_i(X)$ pour $i=1,2$ de conducteur $m_1+1=m_2+1=m+1$ et qui satisfont les conditions du théorème. Des équations des $p-1$ autres revêtements de degré p dans le compositum sont $Y^p=f_1(X)f_2^i(X)$ avec $i=1,..,p-1$; puisque le conducteur est aussi $m+1$; ceci implique des compatibilités entre les données d'Hurwitz des deux revêtements, i.e. les racines de $f_1(X)f_2^i(X)=0$ de multiplicité première à p dans le disque ouvert sont au nombre de $m+1$.

Dans [G-M2 chap. IV] on trouve le revêtement p-cyclique de $\mathbb{P}^1$ avec des données d'Hurwitz non triviales, d'équation $Y^p=(1+X)(1+\alpha X)^h(1+\alpha^2X)^{h^2}...(1+\alpha^{p-2}X)^{h^{p-2}} := f_0(X)$ ($h\in\mathbb{N}$ est une racine primitive $p-1$ ième de l'unité modulo p et $\alpha\in\mathbb{Z}_p^{nr}$ est la racine $(p-1)$-ième de l'unité telle que $\alpha\equiv h \bmod p$); on montre que ce revêtement a potentiellement bonne réduction en p du type A_{p-2}, malheureusement le conducteur est trop petit pour satisfaire les conditions du théorème. En fait cette dernière équation vue modulo p s'écrit (modulo des puissance p-ièmes) $\overline{f_0(X)}=\prod_{v\in V}(1+vX)^{\varphi(v)}$ où $V=\mathbb{F}_p\subset k$ et φ relève une $\mathbb{F}_p$-forme linéaire non nulle, c'est cette dernière forme qui se généralise pour des $\mathbb{F}_p$-espaces vectoriels de dimension quelconque. Les conditions combinatoires suivent alors la combinatoire des sous-$\mathbb{F}_p$-espaces vectoriels. Précisément, nous construisons n revêtements cycliques de degré p, $f_i: C_i\to\mathbb{P}^1_{\mathbb{Q}_p^{nr}}$, $1\leq i\leq n$, ramifiés en $Br_i\subset\mathbb{P}^1(\mathbb{Q}_p^{nr})$. Les conditions combinatoires et géométriques que nous réalisons sont $\#Br_i=p^{n-1}(p-1)$, $\#(Br_{i_1}\cap....\cap Br_{i_k})=p^{n-k}(p-1)^k$ (analogues aux conditions rappelées dans l'introduction pour $n=2$), le produit fibré $C_1\times_{\mathbb{P}^1}...\times_{\mathbb{P}^1}C_n$ induit après normalisation un revêtement galoisien intègre $f: C\to\mathbb{P}^1$ de groupe $(\mathbb{Z}/p\mathbb{Z})^n$ ayant bonne réduction sur $R:=\mathbb{Z}_p^{nr}[\zeta][\pi]$ où ζ est une racine primitive p-ième de l'unité, $\lambda:=\zeta-1$ et $\pi^{p^{n-1}(p-1)-1}=\lambda$. Plus précisément on obtient modulo π un revêtement étale de la droite affine qui est totalement ramifié au-dessus de l'infini (i.e. le groupe d'inertie est $(\mathbb{Z}/p\mathbb{Z})^n$). Ainsi ce revêtement induit au niveau des fibres formelles à l'infini une réalisation de $(\mathbb{Z}/p\mathbb{Z})^n$ comme groupe de R-automorphismes de $R[[Z]]$.

1. Bonne réduction de revêtements p-cycliques de $\mathbb{P}^1$.

Lemme 1. *Soit $p>2$ et $d:=p(p-1)/2$, alors il existe $H(A,B)\in\mathbb{F}_p[A,B]$ homogène de degré $d-p+1$ tel que:*

$$\prod_{i\in\{1,...,p-1\}}(A+iB)^i=A^d+2^{-1}A^{d-p+2}B^{p-2}+B^{p-1}H(A,B)\in\mathbb{F}_p[A,B].$$

Preuve. C'est un cas particulier de [G-M 2], Th. 4.2); nous en rappelons la preuve dans ce cas. On peut supposer que $A=1,B=X$; soit $h\in\mathbb{Z}$ une racine primitive $p-1$-ième de l'unité $\bmod p$. Alors $f(X):=\prod_{i\in\{1,...,p-1\}}(1+iX)^i\equiv\prod_{j\in\{0,...,p-2\}}(1+h^jX)^{h^j}$ modulo puissances p-ièmes, ainsi $f'(X)/f(X)=\sum_{j\in\{0,...,p-2\}}\dfrac{h^{2j}}{1+h^jX}=\sum_{\substack{j\in\{0,...,p-2\}\\ k\in\{0,...,p-4\}}}h^{2j}(-h^jX)^k+\sum_{j\in\{0,...,p-2\}}\dfrac{h^{2j}(-h^jX)^{p-3}}{1+h^jX}=\sum_{j\in\{0,...,p-2\}}\dfrac{h^{2j}(-h^jX)^{p-3}}{1+h^jX}$.

Cette dernière somme s'exprime sous la forme $\dfrac{(X)^{p-3}N(X)}{\prod_{j\in\{0,...,p-2\}}(1+h^jX)}$ où $N(X)$ est un polynôme. Comparant les degrés à l'infini on voit que $N(X)$ est une constante qui vaut $\sum_{j\in\{0,...,p-2\}}h^{2j}(-h^j)^{p-3}=-1\in\mathbb{F}_p$; le lemme suit alors par intégration.

Lemme 2. *Ici p est quelconque. Soient $a_1,a_2,...,a_n\in\mathbb{F}_p^{alg}$ et*

$$\tilde{P}(X):=\prod_{(\epsilon_1,..,\epsilon_n)\in\{0,...,p-1\}^n}(1+(\sum_{1\le i\le n}\epsilon_ia_i)X)^{\epsilon_1}$$

alors il existe $u:=\pi_{n-1}(a_2,...,a_n)[\mathrm{Ad}_n(a_2,...,a_n)(a_1)]^{p-2}$, $Q(X),R(X)\in\mathbb{F}_p^{alg}[X]$ et $m_n:=p^{n-1}(p-1)-1$ tels que $\tilde{P}(X)=(1+XQ(X))^p+uX^{m_n}(1+XR(X))$.

Preuve. Considérons le polynôme $\mathrm{Ad}(X):=\prod_{(\epsilon_2,..,\epsilon_n)\in\{0,...,p-1\}^{n-1}}(X+\sum_{2\le i\le n}\epsilon_ia_i)$, c'est un polynôme additif; ainsi $\mathrm{Ad}(X)=b_0X+b_1X^p+...+X^{p^{n-1}}\in\mathbb{F}_p^{alg}[X]$ et $b_0=\pi_{n-1}(a_2,...,a_n)$; alors $\tilde{P}(X)=X^{\deg\tilde{P}}\prod_{i\in\{1,...,p-1\}}(\mathrm{Ad}(\frac{1}{X})+i\mathrm{Ad}(a_1))^i$.

Si $p>2$, le lemme 1 appliqué à $A:=X^{p^{n-1}}\mathrm{Ad}(\frac{1}{X})=1+b_{n-2}X^{p^{n-1}-p^{n-2}}+...+b_0X^{p^{n-1}-1}$ et $B:=\mathrm{Ad}(a_1)X^{p^{n-1}}$ montre que le monôme de plus bas degré de $\tilde{P}(X)$ qui n'est pas une puissance p-ième provient de $2^{-1}A^{d-p+2}B^{p-2}$ et c'est $2^{-1}(d-p+2)b_0X^{p^{n-1}-1}\mathrm{Ad}(a_1)^{p-2}X^{p^{n-1}(p-2)}=$
$=b_0\mathrm{Ad}(a_1)^{p-2}X^{m_n}$.

Si $p=2$, $\tilde{P}(X)=X^{2^{n-1}}\mathrm{Ad}(\frac{1}{X})+X^{2^{n-1}}\mathrm{Ad}(a_1)$ est encore de la forme annoncée.

Lemme 3. *Soient $a_1,a_2,...,a_n\in\mathbb{Z}_p^{nr}$ et*

$$P(X):=\prod_{(\epsilon_1,..,\epsilon_n)\in\{0,...,p-1\}^n}(1+(\sum_{1\le i\le n}\epsilon_ia_i)^pX)^{\epsilon_1}$$

alors il existe $u\in\mathbb{Z}_p^{nr}$ avec $u=\pi_{n-1}(a_2,...,a_n)[\mathrm{Ad}_n(a_2,..,a_n)(a_1)]^{p-2}\bmod p$, $Q(X),R(X),S(X)$, $T(X)\in\mathbb{Z}_p^{nr}[X]$ et $m_n:=p^{n-1}(p-1)-1$ tels que $P(X)=(1+XQ(X))^p+u^pX^{m_n}(1+XR(X))+pX^{(m_n+1)/p}S(X)+p^2T(X)$.

Preuve. Considérons $\tilde{P}(X):=\prod_{(\epsilon_1,..,\epsilon_n)\in\{0,...,p-1\}^n}(1+(\sum_{1\le i\le n}\epsilon_ia_i)X)^{\epsilon_1}$; alors

$P(X^p)=\prod_{j\in\{0,...,p-1\}}\tilde{P}(\zeta^jX)$. Le lemme 2 appliqué à $\tilde{P}\mathrm{mod}\ p$ donne

$\tilde{P}(X)=(1+XQ(X))^p+uX^{m_n}(1+XR(X))+pS(X)=(1+XQ(X))^p(1+uX^{m_n}(1+X\tilde{R}(X))+p\tilde{S}(X))$ où

$\tilde{R}(X),\tilde{S}(X)\in\mathbb{Z}_p^{nr}[\![X]\!]$. Ce qui donne

$P(X^p)=\prod_{j\in\{0,...,p-1\}}(1+\zeta^jXQ(\zeta^jX))^p\prod_{j\in\{0,...,p-1\}}(1+u(\zeta^jX)^{m_n}(1+\zeta^jX\tilde{R}(\zeta^jX))+p\tilde{S}(\zeta^jX))$ que nous regardons modulo p^2. On a

$\prod_{j\in\{0,...,p-1\}}(1+\zeta^jXQ(\zeta^jX))\in 1+X^p\mathbb{Z}_p^{nr}[X^p]$ et

$\prod_{j\in\{0,...,p-1\}}(1+u(\zeta^jX)^{m_n}(1+\zeta^jX\tilde{R}(\zeta^jX))+p\tilde{S}(\zeta^jX))=$

$\prod_{j\in\{0,...,p-1\}}(1+u(\zeta^jX)^{m_n}(1+\zeta^jX\tilde{R}(\zeta^jX))+$

$p\sum_{j\in\{0,...,p-1\}}(\tilde{S}(\zeta^jX)\prod_{k\in\{0,...,p-1\},k\neq j}(1+u(\zeta^kX)^{m_n}(1+\zeta^kX\tilde{R}(\zeta^kX)))\,\mathrm{mod}\,p^2$. De la rationalité sur $\mathbb{Z}_p^{nr}$ de la dernière somme et de $(\zeta-1)\mathbb{Z}_p^{nr}[\zeta,X]\cap\mathbb{Z}_p^{nr}[X]=p\mathbb{Z}_p^{nr}[X]$, il suit que:

$\sum_{j\in\{0,...,p-1\}}(\tilde{S}(\zeta^jX)\prod_{k\in\{0,...,p-1\},k\neq j}(1+u(\zeta^kX)^{m_n}(1+\zeta^kX\tilde{R}(\zeta^kX)))=0\,\mathrm{mod}\,p$. Enfin

$\prod_{j\in\{0,...,p-1\}}(1+u(\zeta^jX)^{m_n}(1+\zeta^jX\tilde{R}(\zeta^jX))\in\mathbb{Z}_p^{nr}[\![X^p]\!]\cap(1+X^{m_n}\mathbb{Z}_p^{nr}[\![X]\!])=1+(X^p)^{(m_n+1)/p}\mathbb{Z}_p^{nr}[\![X^p]\!]$; le lemme suit.

Remarques. 1. Le relèvement simpliste du polynôme considéré dans le lemme 2 n'est pas suffisament proche d'une puissance p-ième pour induire un automorphisme du disque ouvert sans inertie au bord. **2.** Dans le cas $p=2$, on peut donner une autre famille de polynômes qui donnent naissance à une meilleure approximation par une puissance 2-ième et conduit comme dans la construction qui suit à une réalisation de $(\mathbb{Z}/2\mathbb{Z})^n$, ($n>1$). Précisément, on montre la proposition suivante dont la preuve est laissée au lecteur:

Proposition 1. *Soient* $a_1,a_2,...,a_n\in\mathbb{Z}_2^{nr}$ *et* $P(X):=\prod_{(\epsilon_1,..,\epsilon_n)\in\{0,1\}^n}(1+(\sum_{1\leq i\leq n}\epsilon_ia_i)^2X)$ *alors il existe* $b_0:=\pi_n(a_1,...,a_n)$ *et* $b_1,...,b_{n-1}\in\mathbb{Z}_2^{nr}$ *tels que* $P(X)=(1+\sum_{1\leq i\leq n-1}b_iX^{2^{n-1}-2^{i-1}})^2+b_0^2X^{2^n-1}\,\mathrm{mod}\,4\mathbb{Z}_2^{nr}$. *Soit* $R:=\mathbb{Z}_2^{nr}[\pi]$ *avec* $\pi^{2^n-1}=2^2$ *Alors l'équation* $Y^2=P(X)$ *définit une courbe hyperelliptique ayant bonne réduction sur* R *relativement à la valuation de Gauss en* $S:=(2)^{-2/(2^n-1)}X$ *de type* A_m *avec* $m=2^n-1$.

Proposition 2. *Ici* p *est quelconque. Soient* $a_1,a_2,...,a_n\in\mathbb{Z}_p^{nr}$ *avec* $\pi_{n-1}(a_2,...,a_n)\mathrm{Ad}_n(a_1,a_2,...,a_n)^{p-2}\neq 0\,\mathrm{mod}\,p$ *et* $P(X)\in\mathbb{Z}_p^{nr}[X]$ *comme dans le lemme 3. Soit* $R:=\mathbb{Z}_p^{nr}[\zeta][\pi]$ *où* ζ *est une racine primitive* p*-ième de l'unité,* $\lambda:=\zeta-1$ *et* $\pi^{m_n}=\lambda$ *où* $m_n:=p^{n-1}(p-1)-1$. *Alors l'équation* $Y^p=P(X)$ *définit une courbe ayant bonne réduction sur* R *relativement à la valuation de Gauss en* $S:=(\lambda)^{-p/m_n}X$ *de type* A_{m_n}.

Preuve. Dans l'estimation du lemme 3 les changements $Y=\lambda Z+1+XQ(X)$ et $X=(\lambda)^{p/m_n}S$ donnent en réduction pour la valuation de Gauss relative à S; $Z^p-Z=\overline{u}^pX^{m_n}$ (noter que p/λ^{p-1} est une unité); ainsi le degré de la différente spéciale vaut $d_s=(m_n+1)(p-1)=p^{n-1}(p-1)^2$ et puisque le revêtement est ramifié en $p^{n-1}(p-1)$ points au-dessus du disque ouvert $|S|>1$ (noter que le degré de P est multiple de p) le degré de la différente générique vaut $d_\eta=p^{n-1}(p-1)(p-1)$, le résultat suit alors du critère local de bonne réduction ([G-M1]) ou bien; puisque la ramification est concentrée dans la fibre formelle à l'infini, de l'égalité des genres (géométriques) aux fibres génériques et spéciales.

2. La construction

Théorème. *Le problème "Galois Inverse" a une réponse positive dans le cas des p-groupes abéliens de type $(p,p,...,p)$.*

Preuve. Soient $a_1,a_2,...,a_n \in \mathbb{Z}_p^{nr}$ satisfaisant la condition (*). Pour $i \in \{1,...,n\}$ on définit $P_i(X) := \prod_{(\epsilon_1,...,\epsilon_n)\in\{0,...,p-1\}^n} (1+(\sum_{1\leq j\leq n} \epsilon_j a_j)^p X)^{\epsilon_i} \in \mathbb{Z}_p^{nr}[X]$ et soit $C_i \to \mathbb{P}^1$ le revêtement galoisien d'équation $Y_i^p = P_i(X)$. Il suit immédiatement de la proposition précédente que les n revêtements $C_i \to \mathbb{P}^1$ ont simultanément bonne réduction (en p) de type A_{m_n} avec $m_n = p^{n-1}(p-1)-1$ et ce relativement à la même valuation de Gauss définie par $S := (\lambda)^{-p/m_n}X$, d'équation $Z_i^p - Z_i = {u_n}^p S^{m_n}$ où $u_n = \pi_{n-1}(a_1,..,\hat{a}_i,..,a_n)[\mathrm{Ad}\,_n(a_1,..,\hat{a}_i,..,a_n)(a_i)]^{p-2} \bmod p$.

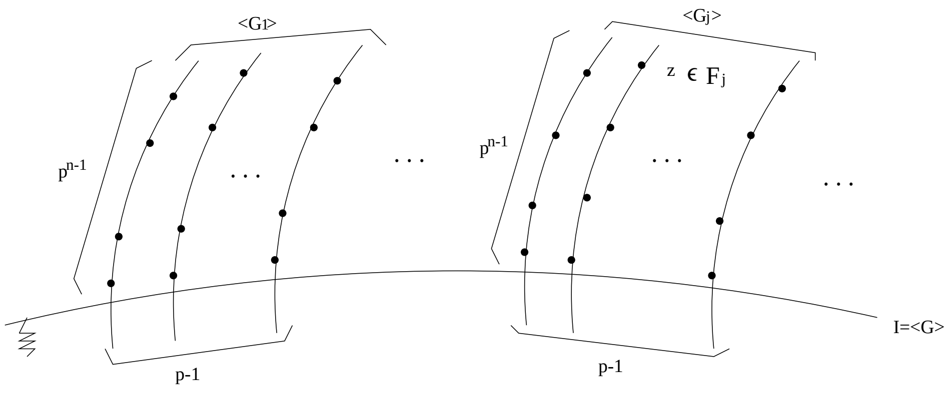
Considérons alors le produit fibré $C_1 \times_{\mathbb{P}^1} ... \times_{\mathbb{P}^1} C_n$, il induit après normalisation un revêtement galoisien $f: C \to \mathbb{P}^1$ de groupe $(\mathbb{Z}/p\mathbb{Z})^n$. Par la condition (*) les n éléments $\overline{u}_n{}^p$ sont linéairement indépendants sur $\mathbb{F}_p$, il s'en suit que C est intègre. Montrons qu'il a bonne réduction sur $R := \mathbb{Z}_p^{nr}[\pi]$ avec $\pi^{m_n} = \lambda$.

En effet, le degré d_s de la differente du compositum des n extensions $Z_i^p - Z_i = {u_n}^p S^{m_n}$ est $d_s = (m_n+1)(p-1)(1+p+p^2+...+p^{n-1}) = p^{n-1}(p-1)(p^n-1)$ (voir par exemple [G-M 1] I. th.5.1).

D'autre part pour calculer le degré d_η de la differente génerique du revêtement $C \to \mathbb{P}^1$ au-dessus du disque ouvert $|S| > 1$, on remarque qu'il est ramifié uniquement en $x = (\sum_{1\leq j\leq n} \epsilon_j a_j)^{-p}$ avec les ϵ_j non tous nuls (ce qui donne au plus $p^n - 1$ points du disque ouvert $|S| > 1$ de $\mathbb{P}^1$) et que les groupes d'inertie sont cycliques d'ordre p, ainsi $d_\eta \leq p^{n-1}(p^n-1)(p-1) = d_s$. On conclut à la bonne réduction en appliquant le critère local de bonne réduction ([G-M1]). Plus précisément on obtient modulo π un revêtement étale de la droite affine qui est totalement ramifié au-dessus de l'infini (i.e. le groupe d'inertie est $(\mathbb{Z}/p\mathbb{Z})^n$). Ainsi ce revêtement induit au niveau des fibres formelles à l'infini une réalisation de $(\mathbb{Z}/p\mathbb{Z})^n$ comme groupe de R-automorphismes de $R[[Z]]$. C'est le théorème.

Géométrie du lieu de ramification.

On note $D^o := \mathrm{Spec}\, R[\![Z]\!]$ la fibre formelle à l'infini de C, alors f induit un revêtement galoisien $D^o \to D^o/G$ où $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Soit Ram le lieu de ramification; si $z \in \mathrm{Ram}$, le groupe d'inertie de z est un sous-groupe d'ordre p de G, ainsi si l'on note $\{G_i =<\sigma_i>, 1 \leq i \leq (p^n-1)/(p-1)\}$ les sous-groupes d'ordre p de G; on a une partition de $\mathrm{Ram} = \coprod \mathrm{F}_i$ par les groupes d'inertie des points. Soit $\mathcal{D}^o$ le modèle minimal semi-stable de D^o qui déploie Ram en des points lisses modulo π (cf. [G-M 2]); nous représentons dans le schéma qui suit la fibre spéciale de $\mathcal{D}^o$; c'est un arbre de droites projectives pointées par les spécialisations du lieu ramification Ram.



Ce dessin mérite quelques explications: les groupes indiqués entre crochets $<.>$ représentent les groupes d'inertie des composantes. Pour voir que celui de la composante interne est G tout entier on procède ainsi: la composante interne correspond à la réduction de D^c, le plus petit disque fermé dans $D^o_{(K)}$ contenant Ram ; pour des raisons de symétrie son groupe d'inertie est G ou bien le groupe trivial. Dans ce dernier cas le passage au quotient par $<\sigma_1>$ induirait à la fibre spéciale de D^c un revêtement p-cyclique de $\mathbb{P}^1$ qui est aussi $\mathbb{P}^1$; ce qui via la formule d'Hurwitz montre que la ramification est concentrée au point à l'infini i.e. le point correspondant à l'exterieur de D^c dans $D^o_{(K)}$; mais σ_1 laisse au moins une classe de D^c fixe (celle d'un point fixe de σ_1), d'où une contradiction. Voyons que D^c est l'image inverse de $|X|\geq 1$, soit $x_1\in \mathrm{Ram}$, fixé par σ_1 ; la classe de x_1 dans D^c est donc globalement invariante par G, en particulier cette classe contient l'orbite Gx_1 i.e. la fibre au dessus d'un point de branchement; ainsi par définition de D^c, dans le disque fermé quotient D^c/G le lieu de branchement Ram/G se trouve réparti en au moins deux classes distinctes; la seule possibilité est que D^c/G soit le disque fermé $|X|\geq 1$. Le lieu de branchement se répartit alors en p^n-1 classes distinctes et les classes correspondant au groupe d'inertie $G_1=<\sigma_1>$ sont données par $1+(\epsilon_1 a_1)^pX=0$ pour $\epsilon_1=1,..,p-1$. Il reste à montrer que les points fixes de σ_1 dans une même fibre sont équidistants. Pour cela considérons dans D^c le disque ouvert D^o_1 correspondant à la classe de x_1 dans D^c ; dans ce disque on considère le plus petit disque fermé D^c_1 contenant les points fixes de $\sigma_1\in D^o_1$; ils se trouvent répartis en au moins deux classes distinctes; ainsi l'un des automorphismes agit non trivialement sur la specialisation et par symetrie, les $\sigma_i, i>2$ agissent non trivialement.

III. Une autre réalisation de $(\mathbb{Z}/p\mathbb{Z})^2$, $p>2$

Dans ce paragraphe p est un nombre premier >2.

Nous exhibons 2 revêtements p-cycliques de $\mathbb{P}^1$ qui satisfont les conditions du théorème de [G-M 1], rappelé dans l'introduction. L'intérêt de cet exemple réside dans la méthode et la géometrie qu'il induit.

Théorème. *Soit* $h\in\mathbb{N}$, *une racine primitive* $p-1$*-ième de l'unité modulo* p *et* $\alpha\in\mathbb{Z}_p^{nr}$ *la racine* $(p-1)$*-ième de l'unité telle que* $\alpha\equiv h \bmod p$ *et soit* $f_0(X):=(1+X)(1+\alpha X)^h(1+\alpha^2X)^{h^2}...(1+\alpha^{p-2}X)^{h^{p-2}}=1+uX^{p-2}+pXP(X)+X^{p-1}Q(X)$ *où* $u\in\mathbb{Z}_p^{nr*}$ *et* $P(X),Q(X)\in\mathbb{Z}_p^{nr}[X]$. *Pour* $i=1,2$, *considérons les deux revêtements* $f_i:C_i\to\mathbb{P}^1_{\mathbb{Q}_p^{nr}[\zeta]}$ *d'équation* $Y_1^p=1+X^{p-1}$ *et* $Y_2^p=f_0(X)((1+\dfrac{X}{\lambda})^p-uX^{p-2})$ *(* $\lambda=\zeta-1$ *et* ζ *est une racine primitive* p*-ième de l'unité), alors ces deux revêtements ont simultanément potentiellement bonne réduction pour la valuation de Gauss en* S *si* $S:=\lambda^{-p/(p-1)}X$ *respectivement de type* A_{m_1} *(* $m_1=p-1$ *) et* A_{m_2} *(* $m_2=2p-2$ *); les deux revêtements ont en commun* $[(m_1+1)/p](p-1)$ *points de ramification; ainsi le produit* $C_1\times_{\mathbb{P}^1_{\mathbb{Q}_p}}C_2$ *des deux revêtements induit après normalisation un revêtement galoisien* $f:C\to\mathbb{P}^1$ *de groupe* $(\mathbb{Z}/p\mathbb{Z})^2$ *qui a potentiellement bonne réduction et induit par restriction à la fibre formelle à l'infini une réalisation de* $(\mathbb{Z}/p\mathbb{Z})^2$ *comme groupe des* R*-automorphismes de* $R[[Z]]$ *pour* $R:=\mathbb{Z}_p^{nr}[\theta]$ *où* $\theta^{p-1}=\zeta-1$.

Preuve. L'estimation $f_0(X)=1+uX^{p-2}+pXP(X)+X^{p-1}Q(X)$ a été expliquée au lemme 1.

Nous allons en déduire une estimation du même type pour $f_2(X):=f_0(X)((1+\dfrac{X}{\lambda})^p-uX^{p-2})$; posons pour cela

$X=\theta^pS$, avec $\lambda=\theta^{p-1}$ ainsi $p/\theta^{(p-1)^2}$ est une unité,

$\dfrac{X}{\lambda}=\theta S$, $A:=pXP(X)+X^{p-1}Q(X)$ i.e. $f_0(X)=1+uX^{p-2}+A$

$B := (1+\dfrac{X}{\lambda})^p - 1 = (1+\theta S)^p - 1$

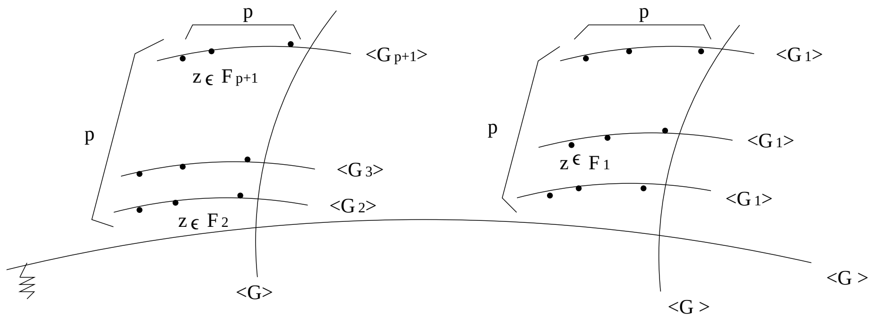
Nous mettrons dans la $\theta^{p(p-1)}$ *"poubelle"* les termes $\in \mathbb{Z}_p^{alg}[S]$ dont les coefficients sont en valeur absolue strictement plus petits que $|\lambda^p| = |\theta^{p(p-1)}|$. Suivant ce principe on peut écrire $A = \theta^{p(p-1)}(Q(0)+poubelle)$, alors $f_2(X) = (1+\dfrac{X}{\lambda})^p + (f_0(X)-1)(1+\dfrac{X}{\lambda})^p - uX^{p-2}f_0(X) = (1+\theta S)^p + (uX^{p-2}+A)(1+B) - (1+uX^{p-2}+A)uX^{p-2} = (1+\theta S)^p + \theta^{p(p-1)}(Q(0)S^{p-1} + uS^{2p-2} + poubelle)$.

Si l'on pose $Y_2 = \theta^{p-1}Z + 1 + \theta S$ l'équation de C_2 devient $\dfrac{(\theta^{p-1}Z+1+\theta S)^p - (1+\theta S)^p}{\theta^{p(p-1)}} = Q(0)S^{p-1} + uS^{2p-2} + poubelle \in R[[S]]$ qui est à coefficients entiers et donne modulo π l'équation $Z^p - Z = \overline{Q(0)}S^{p-1} + \overline{u}S^{2p-2}$ i.e. un revêtement étale de la droite affine de type A_{m_2} ($m_2 = 2p-2$).

Maintenant, nous remarquons que le revêtement f_2 est ramifié uniquement au-dessus des racines $p-1$-ième de -1 ainsi qu'au dessus des racines de $(1+\dfrac{X}{\lambda})^p - uX^{p-2}$ ce qui donne $2p-1$ points de ramification et prouve qu'il y a potentiellement bonne réduction relativement à la valuation de Gauss en S. Pour le reste du théorème on vérifie facilement les conditions du theorème de [G-M 1] rappelées dans l'introduction. On peut vérifier cette fois que l'arbre de la réduction de $\mathbb{P}^1$ qui déploie le lieu de ramification de f_2 a 2 bouts.

Géométrie du lieu de ramification.

Comme dans le paragraphe II, nous représentons la fibre spéciale du modèle minimal semi-stable qui déploie le lieu de ramification en des points lisses.



Remarque. La méthode que nous venons d'utiliser pour passer de $f_0(X)$ à $f_2(X)$ a eu pour effet de grossir le lieu de ramification tout en conservant la potentielle réduction (du type A_{p-2} au type A_{2p-2}), elle peut être reitérée sous une forme adaptée afin de produire des automorphismes d'ordre p du disque dont le modèle semistable minimal qui déploie les points fixes en des points lisses induit un arbre de longueur arbitrairement grande (notons que des arbres de longueur arbitrairement grande sont aussi exhibés via les groupes formels de Lubin-Tate dans [G-M 2] II. 3.3.3).

IV. p-groupes finis et $\mathrm{Aut}_R R[\![Z]\!]$

Dans ce paragraphe nous montrons que tout p-groupe fini peut être réalisé comme sous-groupe de $\mathrm{Aut}_R R[\![Z]\!]$ pour un anneau de valuation discrete R fini sur $\mathbb{Z}_p$ convenable. Bien que ces realisations mettent en évidence la richesse de $\mathrm{Aut}_R R[\![Z]\!]$ nous sommes loin de répondre au problème Galois inverse, puisque elles correspondent à des actions libres sur le disque ouvert qui induisent l'identité modulo π.

Théorème. *Soit G un p-groupe fini alors il existe un anneau de valuation discrète fini sur $\mathbb{Z}_p$ et une injection $G \to \mathrm{Aut}_R R[\![Z]\!]$ qui induit une opèration libre de G sur $\mathrm{Spec}\, R[\![Z]\!] \times K$ et l'automorphisme identité modulo π ; en particulier l'extension d'anneaux de valuation discrète $R[\![Z]\!]_{(\pi)}/R[\![Z]\!]^G_{(\pi)}$ est férocement ramifiée.*

Preuve. Fixons $\alpha_1, ..., \alpha_g$ un système de générateurs de G avec $g \geq 2$. Quitte à grossir g on peut supposer qu'il existe une courbe propre et lisse C sur $\mathbb{F}_p$ de genre g telle que le p-rang de $\pi_1(C \times \mathbb{F}_p^{alg})$ soit nul i.e. $C \times \mathbb{F}_p^{alg}$ n'admet pas de revêtement étale p-cyclic (on peut prendre pour C par exemple un revêtement p-cyclic étale de la droite affine de conducteur $m+1 > 2$ à l'infini avec m suffisament grand). Considérons une courbe relative sur $\mathbb{Z}_p$ propre et lisse $\mathcal{C}$ qui relève C (SGA 1); puisque la fibre générique géométrique $\mathcal{C}_{\overline{\eta}}$ est une courbe propre lisse de genre g en caractéristique zéro il suit que $\pi_1(\mathcal{C}_{\overline{\eta}})$ est le compléte profini du groupe $< a_1, b_1, ..., a_g, b_g, | \prod_{1 \leq i \leq g} [a_i, b_i] = 1 >$; ainsi il existe un homomorphisme surjectif $\rho : \pi_1(\mathcal{C}_{\overline{\eta}}) \to G$ (envoyer par exemple a_i et b_i sur α_i). Soit $f : \mathcal{D}_{(K)} \to \mathcal{C}_{(K)}$, le revêtement Galoisien étale de groupe G de $\mathcal{C}_{\overline{\eta}}$ correspondant à ρ ; il est défini sur une extension finie K de $\mathbb{Q}_p$, on note R l'anneau de valuation de K. Notons $\mathcal{D}$ la normalisation de $\mathcal{C}$ dans le corps de fonctions de $\mathcal{D}_{(K)}$. Quitte à grossir R, on peut supposer que la fibre spéciale $\mathcal{D}_s$ de $\mathcal{D}$ est réduite (cf. [E]); d'autre part puisque G est un p-groupe il résulte de [R], cor. 1 p. 181, que $\mathcal{D}_s$ est géométriquement unibranche et donc en particulier intègre. Soit s le point générique de $\mathcal{D}_s$ dans $\mathcal{D}$ et $I \subset G$ le groupe d'inertie en s ; montrons que $I = G$. En effet si ce n'est pas le cas on peut trouver $I \subset H \subset G$ avec $H \neq G$ normal dans G et d'indice p ; alors $\mathcal{D}/H \to \mathcal{C} \times R$ est étale par le théorème de pureté; ce qui contredit la nullité du p-rang de $\pi_1(C \times \mathbb{F}_p^{alg})$. Quitte à grossir R, on peut supposer qu'il existe un point lisse $z \in D_s$; alors G est groupe de R-automorphismes de $\hat{\mathcal{O}}_{\mathcal{D},z}$, l'anneau local complété en z de $\mathcal{D}$ qui est isomorphe à $R[\![Z]\!]$. Par construction l'extension $R[\![Z]\!]/R[\![Z]\!]^G$ est uniquement ramifiée en (π) et G est le groupe d'inertie en (π).

Remarque. Dans le cas des p-groupes abéliens, on peut montrer le théorème en utilisant des groupes formels de dimension 1 (cf. [H] p. 465), nous en esquissons la preuve. Soient K une extension finie de $\mathbb{Q}_p$, R l'anneau des entiers de K et $F(X,Y) \in R[\![X,Y]\!]$, un groupe formel sur R de hauteur h. On note $F(K^{alg})$ l'ensemble $m(K^{alg}) \subset K^{alg}$ des éléments topologiquement nilpotents (i.e. les éléments de K^{alg} de valuation strictement positive) muni de la loi de groupe induite par $F(X,Y)$. Soit $\Lambda \subset F(K^{alg})$ son groupe de torsion. Pour $a \in \Lambda \cap R$ on definit un R-automorphisme de $R[\![Z]\!]$ par $\sigma(Z) := F(Z,a)$; on remarque que l'application $\Lambda \cap R \to \mathrm{Aut_R} R[\![Z]\!]$ ainsi definie est un homomorphisme injectif ([H] p. 465). Comme $\Lambda \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^h$ ([H] p. 462), cela donne plein de réalisations des p-groupes abeliens comme sous-groupes de $\mathrm{Aut_R} R[\![Z]\!]$ pour R et h suffisament grands, malheureusement ces groupes d'automorphismes comme dans la construction précédente donnent l'identite modulo π (dans un groupe formel on a $F(Z,0) = Z$). D'autre part il est facile de vérifier que l'extension $R[\![Z]\!]/R[\![Z]\!]^G$ est uniquement ramifiée en (π).

Bibliographie

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

[B-M] J. Bertin, A. Mézard, *Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques*, Prépublication $n^0 439$ de l'Institut Fourier, (1998).

[E] H. P. Epp, *Eliminating wild ramification*, Invent. Math. 19 (1973), 235-249.

[G-M 1] B. Green, M. Matignon, *Liftings of Galois Covers of Smooth Curves*, Compositio Math., Vol 113 (1998), 239–274.

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

[H] M. Hazewinkel, *Formal Groups and Applications*, Pure and Applied Mathematics 78, Academic Press, 1978.

[O1] F. Oort, *Lifting Algebraic Curves, Abelian Varieties, and their Endomorphisms to Characteristic Zero*, Proceedings of Symposia in Pure Mathematics, Vol 46 (1987).

[O2] F. Oort, *Some questions in algebraic geometry*, Utrecht Univ., Math. Dept. Preprint Series, June 1995.

[O-S-S] F. Oort, T. Sekiguchi, N. Suwa, *On the deformation of Artin-Schreier to Kummer*, Ann. scient. Éc. Norm. Sup., 4e série, t. 22 (1989), 345–375.

[R] M. Raynaud, *p-groupes et réduction semi-stable des courbes*, The Grothendieck Festschrift, Vol III, Progress in Mathematics 88 (1990), Birkhaüser, 179–197.

[S] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

M. Matignon
Mathématiques Pures de Bordeaux
UPRS-A 5467 CNRS
Université de Bordeaux I
351, cours de la Libération
33405 – Talence, Cedex
France
email: matignon@math.u-bordeaux.fr