Vers un algorithme pour la réduction stable des revêtements p-cycliques de la droite projective sur un corps p-adique *

Michel Matignon

Abstract

In his Ph. D. thesis, C. Lehr offers an algorithm which gives the stable model for p-cyclic covers of the projective line over a p-adic field under the conditions that the branch locus whose cardinal is $m+1$ has the so called equidistant geometry and $m < p$. In this note we give an algorithm also in the equidistant geometry case but without condition on m. In particular we are able to study the reduction at 2 of hyperelliptic curves with equidistant branch locus.

Dédié à Michel Raynaud

0 Introduction

Par corps p-adique nous entendons un corps K d'inégale caractéristique $p > 0$ qui est complet pour une valuation discrète notée v. On note R l'anneau des entiers de K, π une uniformisante et k son corps résiduel que l'on supposera par soucis de commodité algébriquement clos. Nous supposerons de plus que R contient ζ une racine primitive p-ième de l'unité et noterons $\lambda = \zeta - 1$.

Les arithméticiens savent bien qu'il est délicat d'étudier la réduction en 2 d'une courbe elliptique ou plus généralement d'une courbe hyperelliptique. C'est là un avatar d'un problème bien connu des géomètres, à savoir le "mauvais comportement" en p du groupe fondamental algébrique. Nous nous proposons d'examiner plus précisément la géométrie des revêtements p-cycliques de la droite projective sur K; par géométrie nous entendons l'étude du modèle stable.

Une première tentative dans ce sens se trouve dans un exposé de séminaire de Coleman ([Co], §6; voir aussi [Co-Ca]); cette approche s'est développée initialement en vue de comprendre la réduction stable des courbes de Fermat $F_n : X^n + Y^n = Z^n$ lorsque $p|n$; et avec succès dans ce cas parce que l'on se ramène à l'étude des revêtements cycliques de $\mathbb{P}^1$ ramifiés au-dessus de 3 points. Récemment il y a eu un regain d'intérêt sur cette question principalement après les travaux de M. Raynaud qui a introduit dans [Ra 1] des méthodes nouvelles combinant théorie de Galois, géométrie semi-stable et dégénérescence des schémas en groupes. Précisément, pour un revêtement générique galoisien de groupe nilpotent d'une R-courbe relative propre lisse et sous l'hypothèse que le lieu de branchement induit un diviseur relatif étale sur R (c'est ce que nous appelons géométrie équidistante), Raynaud donne un énoncé qualitatif sur la fibre spéciale d'un modèle semi-stable; en particulier il montre qu'il n'y a pas de cycles évanescent (théorème 1' p. 188). Divers auteurs ont depuis contribué à une description qualitative en termes combinatoires et différentiels de la géométrie p-adique des revêtements p-cycliques (cf. [Gr-Ma], [He], [Sa 1,2,3],...), la complexité de la réponse dépendant de la géométrie du lieu de branchement.

Cette note s'inscrit dans un programme qui est de rendre effectif le théorème de Raynaud; pour cela il suffit de partir à la recherche des valuations qui induisent les composantes de genre non nul à la fibre spéciale. Une première tentative a été opérée très récemment dans sa thèse par C. Lehr. Soit

*AMS classification number: 11G20, 14H30 (14Q05)

$C \to \mathbb{P}^1$ un revêtement p-cyclique de la droite projective ramifié en $m+1 \geq 3$ points. Il étudie le cas où la géométrie du lieu de branchement est la plus simple d'un point de vue p-adique: les $m+1$ points sont équidistants i.e. pour un choix convenable de coordonnées sur $\mathbb{P}^1$, ils sont dans des classes distinctes modulo π (c'est l'hypothèse du théorème de Raynaud). Pour cette géométrie et sous la condition supplémentaire $(m-1,p)=1$, C. Lehr donne un critère de potentielle bonne réduction et, sous la condition $m < p$, un algorithme qui décrit le modèle stable. Ces conditions sont très restrictives pour p petit et en particulier si $p=2$, elles éliminent toutes les courbes hyperelliptiques.

Dans cette note, toujours sous l'hypothèse que le lieu de branchement a la géométrie équidistante, nous proposons un algorithme qui fonctionne sans condition.

Passons à une description de la note. Nous espérons que le lecteur partagera le choix de la terminologie et des notations.

Dans la partie 1, nous rappelons les propriétés essentielles à notre propos concernant la dégénérescence des $\boldsymbol{\mu}_p$-torseurs et la géométrie semi-stable. Nous présentons brièvement les algorithmes de Coleman et de Lehr afin de préparer le lecteur à l'introduction dans la partie 2 d'une généralisation des développements de Taylor des polynômes sur un corps p-adique. Brièvement, pour un entier m donné, pour $F(X) \in R[X]$ et $y \in R^{alg}$, on développe $F(X+y) \in R[y][X]$ sous la forme d'une approximation dans $R^{alg}[X]$ à presque $\frac{p}{p-1}v(p)$ près par la puissance p-ième d'un polynôme de manière que les coefficients des monômes restant de degré $\leq m$ et multiple de p aient une taille négligeable dans le sens de l'approximation. Le coefficient $F^{[1]}(y)$ du monôme X est une "fonction multiforme de y" dont la norme $N_m(F^{[1]}(y))$ est une fonction polynôme de y qui modulo p est une puissance $F'(y)^{p^{r(m)}}$ de la dérivée usuelle, pour $r(m)$ convenable.

Soit Br, le lieu de branchement du revêtement supposé de cardinal $m+1 \geq 3$, et $Z^p = F(X) \in R[X]$ une équation du $\boldsymbol{\mu}_p$-torseur au-dessus de $\mathbb{P}^1 - \mathrm{Br}$. Dans ([Le 2], Th. 2) Lehr a montré, sous l'hypothèse $m < p$, que certains zéros de $F'(Y)$ donnent des centres pour les disques fermés de $\mathbb{P}^1_K$ qui induisent des composantes de genre non nul dans le modèle stable du revêtement. La preuve n'est pas difficile et vient d'une comparaison des polygones de Newton de $F(X+y)$ et $F'(X+y)$. Dans le cas général $F'(Y)$ est remplacé par $N_m(F^{[1]}(Y))$ et l'analyse des zéros se fait grâce à une étude fine de la dégénérescence du $\boldsymbol{\mu}_p$-torseur; nous renvoyons le lecteur au théorème 3.2.2 pour un énoncé précis.

La partie 4 est consacrée aux exemples et en premier lieu à la situation où les points de branchement sont en position équidistante et leurs classes modulo π en position générale. Puis le cas des courbes hyperelliptiques $(p=2)$ est plus précisément étudié pour m petit.

La partie 5 donne une généralisation dans le cas des revêtements p-cycliques d'une courbe ayant bonne réduction.

1 Généralités

1.1 Réduction des $\boldsymbol{\mu}_p$-torseurs et la différente

On reprend les notations de l'introduction. La proposition qui suit est un résumé commode pour les applications que nous avons en vue; elle se retrouve dans les travaux de divers auteurs; nous renvoyons à ([He], ou [Sa 3]) pour un exposé complet. Nous devons rappeler la définition du schéma en groupe $\mathcal{H}_n$.

Pour tout entier $n > 0$, on note $\mathcal{G}_n := \operatorname{Spec} R[X, \frac{1}{\pi^n X+1}]$ 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 $\frac{(\pi^n X+1)^p-1}{\pi^{pn}}$ est à coefficients dans R; l'homomorphisme

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

défini par $\Psi_n(Y) = \frac{(\pi^n X+1)^p-1}{\pi^{pn}}$ est une isogénie de degré p; on note $\mathcal{H}_n$ 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 $\boldsymbol{\mu}_{p,K}$. Si $0 < n < v_K(\lambda)$, sa fibre spéciale est le groupe radiciel additif $\boldsymbol{\alpha}_p$ et si $n = v_K(\lambda)$, sa fibre spéciale est le groupe étale isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 1.1.1 ([He], prop. 1.6).— *Soit $X := \operatorname{Spec} A$ 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 $Y_K \to X_K$ un $\boldsymbol{\mu}_p$-torseur étale non trivial, donné par une équation $y^p = f$, où f est inversible dans A_K, et Y le normalisé de X dans Y_K; on suppose que la fibre spéciale de Y est intègre. Soit η (resp. η') le point générique de la fibre spéciale de X (resp. Y). Les anneaux locaux $\mathcal{O}_{X,\eta}$ et $\mathcal{O}_{Y,\eta'}$ sont alors des anneaux de valuation discrète d'uniformisante π. Notons δ la valuation de la différente de $\mathcal{O}_{Y,\eta'}/\mathcal{O}_{X,\eta}$. On distingue alors deux cas suivant la valeur de δ.*

- *Si $\delta = v_K(p)$, Y est un $\boldsymbol{\mu}_{p,R}$-torseur pour la topologie fppf, donc $Y = \operatorname{Spec} B$, avec $B := \frac{A[Y]}{(Y^p-u)}$, où u est une unité de A, unique à la multiplication d'une puissance p-ième d'une unité de A près. On dit 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 $0 \leq \delta < v_K(\lambda)$, et $Y \to X$ 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 $u' = u(\pi^n v+1)^p + \frac{(\pi^n v+1)^p-1}{\pi^{pn}}$.*

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

1.2 Modèle stable

Nous adoptons la terminologie de [Li 1] à savoir qu'une R-courbe propre est *semi-stable* (resp. *stable*) si ses fibres géométriques sont des courbes semi-stables (resp. stables), i.e. sont projectives réduites et connexes et ont pour seules singularités des points doubles ordinaires (resp. semi-stables, de genre arithmétique ≥ 2 et chacune de leurs composantes irréductibles isomorphe à $\mathbb{P}^1$ rencontre les autres composantes en au moins 3 points).

Une R-courbe propre est appelée modèle de sa fibre générique.

On étend la notion de modèle stable au contexte des courbes lisses propres sur K marquées par un ensemble fini $S \subset C(K)$. On appelle *modèle stable de la courbe marquée* (C, S) un modèle $\mathcal{C}/R$ de C tel que les points de S se spécialisent en des points distincts $\bar{S}$ (i.e. la clôture schématique de S est lisse sur R) du lieu lisses de $\mathcal{C}_s$ et tel que les fibres sont semi-stables et chacune de leurs composantes irréductibles isomorphe à $\mathbb{P}^1$ contient au moins 3 points parmi les points de $\bar{S}$ ou les points d'intersection.

Il suit du théorème de réduction semi-stable que si C, resp. (C, S) est une courbe (resp. marquée) propre, lisse et géométriquement irréductible sur K, de genre ≥ 2 (resp. de genre g avec $2g+|S|-1 \geq 2$) il existe une extension finie K'/K telle que $C_{K'} := C \times_K K'$ admet un modèle stable sur la clôture intégrale R' de R dans K' (voir [Ab] ou [Li 1], pour une démonstration du théorème de réduction semi-stable).

Dans ce qui suit (C, G) désigne une courbe C/K munie d'une action par un groupe de K-automorphismes G; on note Ram (resp. Br) le lieu de ramification (resp. branchement) de $f : C \to C/G$; nous dirons que (C, G) admet un modèle stable sur R si $\operatorname{Ram} \subset C(K)$ et si la courbe marquée (C, Ram) admet un modèle stable sur R; nous appelerons alors **modèle stable de** (C, G) **le modèle stable de la courbe marquée** (C, Ram). Supposons pour simplifier que ce modèle stable est défini sur R; alors par l'unicité il est équivariant et le morphisme $f : C \to C/G$ s'étend en un morphisme fini de R-courbes $f : \mathcal{C} \to \mathcal{C}/G$ où $\mathcal{C}/G$ est semi-stable et s'obtient à partir du modèle stable de C/G marquée par Br en éclatant des points fermés de la fibre spéciale; en particulier sa fibre spéciale ne diffère de celle du modèle stable que par des $\mathbb{P}^1_k$ ([Ra 1]).

Définition 1.2.1 .— Nous dirons que le lieu de branchement Br a la *géométrie équidistante* si le modéle stable de la courbe marquée $(C/G, \mathrm{Br})$ est défini et lisse sur R i.e. C/G admet un modèle lisse sur R et les points de Br se spécialisent dans ce modèle en des points distincts.

1.3 L'algorithme de Coleman

Soit C une courbe propre et lisse sur K. Soit $n > 2$ un entier différent de p, on sait (c.f. [Ab], prop. 5.10) que C a un modèle stable sur l'extension K_n de K obtenue en adjoignant les points de n-torsion de sa jacobienne pour un n entier différent de p. Malheureusement étant donnée une équation de C il n'est pas facile de trouver K_n et donc de trouver le modèle stable de C. Dans ([Co], §6) Coleman dit: "It would be desirable to have some efficient algorithm for computing the stable reduction of a curve."

Coleman est principalement interessé par les revêtements galoisien de $\mathbb{P}^1$ et constate que le cas difficile est celui où p divise l'ordre du groupe. Il développe un algorithme dans le cas p-cyclique qui marche dans certains cas. Précisément, il considère une équation $Z^p = F(X) \in K[X]$ avec $\deg F = n$ et V/K la variété affine sur K, Spec $\frac{K[Y, a_i, b_j,\, 0\leq i\leq [\frac{n}{p}], 0<j\leq n,\, (j,p)=1]}{\mathcal{I}}$, où l'idéal $\mathcal{I}$ des équations est codé par l'identité

$$(*)\ F(X+Y) = (\sum_{0\leq i\leq [\frac{n}{p}]} a_i X^i)^p + \sum_{0<i\leq n,\, (i,p)=1} b_i X^i.$$

Même si ce système a trivialement une solution modulo p, il n'est pas sûr qu'il a des solutions; en effet un décompte montre que la dimension de V sur K est en général égale à 1. Si l'on impose la condition supplémentaire $b_1 = 0$; on obtient un ensemble éventuellement vide et au plus fini de valeurs de Y pour lesquelles l'équation (*) permet parfois d'exhiber un modèle entier de la courbe $Z^p = F(X)$ qui est propice à donner des composantes de genre non nul en réduction; ces composantes induisent des disques fermés de la droite projective quotient et les zéros de b_1 en fournissent des centres. La recherche de centres de ces disques est un problème de nature analytique et la méthode de Coleman en propose une attaque algébrique (recherche d'une variété de dimension 0 et éventuellement vide) aussi cette méthode doit être modifiée pour pouvoir espérer aboutir dans le cas général. Nous renvoyons le lecteur à 4.2 pour des exemples traités par la méthode de Coleman.

1.4 L'algorithme de Lehr

Dans sa thèse C. Lehr a étudié la réduction stable des revêtements p-cycliques de la droite projective sur un corps p-adique dans le cas où le lieu de branchement a la géométrie équidistante.

Soit $Z^p = F(X)$ une équation normalisée du revêtement $C \to \mathbb{P}^1$ i.e. $F(X) = \prod_{1\leq i\leq m} (X - x_i)^{e_i} \in R[X]$ de degré N avec $(N, p) = 1$ et $(e_i, p) = 1$ pour $1 \leq i \leq m$. On suppose de plus que $v(x_i) = v(x_i - x_j) = 0$ pour tout $i \neq j$. Ainsi le lieu de branchement $\mathrm{Br} = \{\infty, x_1, .., x_m\}$ a la géométrie équidistante. Dans le cas où $m < p$, C. Lehr montre que les développements de Taylor $F(X + y) = F(y) + F'(y)X + ...$ pour $y \in R^{alg}$ parcourant les zéros de $F'(Y)$ avec $v(F(y)) = 0$ donnent naissance aux composantes du modèle stable de C qui sont de genre non nul (cf. [Le 2], Th. 2).

2 p-développements de Taylor

Les champs respectifs de succès des algorithmes de Coleman et Lehr nous amènent à généraliser la notion de développement de Taylor qui approche dans un sens p-adique le développement idéal de Coleman et présente l'avantage de ne pas être sensible aux petites variations des coefficients.

2.1 Définition

Définition 2.1.1 .— On fixe $K(Y)^{alg}$ une clôture algébrique de $K(Y)$ munie d'une valuation v_Y qui prolonge la valuation de Gauss de $K(Y)$ relative à Y et $R[Y]^{alg}$ désigne la clôture intégrale de $R[Y]$. Soit m, n deux entiers; on note $c_n := 1 + 1/p + ... + 1/p^n$ et $I_{m,n}$ l'idéal $(p^{c_n}X, X^{m+1})$ de $R[Y]^{alg}[X]$. Un *p-développement de Taylor d'ordre m et de niveau n de* $F(X) \in R[X]$ est la donnée d'un couple $(A_{m,n}(X,Y), B_{m,n}(X,Y))$ de polynômes $\in R[Y]^{alg}[X]$ avec

$$A_{m,n}(X,Y) = \sum_{0 \leq i \leq m/p} a_i(Y)X^i, \ B_{m,n}(X,Y) = \sum_{1 \leq j \leq m, \ (j,p)=1} b_j(Y)X^j$$

tels que

$$F(X+Y) - (A_{m,n}(X,Y))^p - B_{m,n}(X,Y) \in I_{m,n}.$$

Remarque 2.1.2 .—

i) Si $m < p$ le développement de Taylor classique induit un p-développement de Taylor d'ordre m et de niveau n pour tout n.

ii) Notez que $c_n v(p) = (1 - 1/p^{n+1})v(\lambda^p)$ est proche de $v(\lambda^p)$. Ainsi un p-développement de Taylor d'ordre m et de niveau n est une approximation de $F(X+Y)$ dans $R[Y]^{alg}[X]$ à presque $\frac{p}{p-1}v(p)$ près par la puissance p-ième d'un polynôme de manière que les coefficients des monômes restant de degré $\leq m$ et multiple de p aient une taille négligeable dans le sens de l'approximation.

2.2 Existence

Si L est un corps algébriquement clos et si $x \in L$, on notera $x^{1/p}$ une racine p-ième de x. On a la proposition suivante:

Proposition 2.2.1 .— *On fixe l'entier m, notons* $F_m(X+Y) = s_0(Y) + s_1(Y)X + ... + s_m(Y)X^m \in R[Y][X]$ *le développement de Taylor à l'ordre m de* $F(X) \in R[X]$. *On définit une suite de polynômes* $\in R[Y]^{alg}[X]$, $(A_{m,n}(X,Y), B_{m,n}(X,Y))$ *par les relations de récurrence suivantes:*

$$\text{(rang 0)} \quad (A_{m,0}(X,Y), B_{m,0}(X,Y)) = (\sum_{0 \leq i \leq m/p} s_{ip}(Y)^{1/p}X^i, \sum_{1 \leq j \leq m, \ (j,p)=1} s_j(Y)X^j).$$

Pour définir la suite au rang $(n+1)$, *on considère le reste au rang n,* $R_n(X,Y) := F_m(X+Y) - (A_{m,n}(X,Y))^p - B_{m,n}(X,Y) = p^{c_n}(r_1(Y)X + ... + r_m(Y)X^m)$ *où* $r_i(Y) \in R[Y]^{alg}$. *Soit* $AR_n := p^{c_n/p} \sum_{1 \leq i \leq m/p} r_{ip}(Y)^{1/p}X^i$ *et* $BR_n := p^{c_n} \sum_{1 \leq j \leq m, \ (j,p)=1} r_j(Y)X^j$, *alors:*

$$(A_{m,n+1}(X,Y), B_{m,n+1}(X,Y)) := (A_{m,n}(X,Y) + AR_n, B_{m,n}(X,Y) + BR_n).$$

Les polynômes $(A_{m,n}(X,Y), B_{m,n}(X,Y))$ *définissent un p-développement de Taylor d'ordre m et de niveau n de* $F(X)$.

Preuve. Avant de passer à la preuve remarquons que la suite précédente dépend à chaque étape du choix de racines p-ièmes et l'énoncé vaut donc pour un choix quelconque. L'étape 0 est une égalité en caractéristique p. Les polynômes mis en jeu à chaque étape sont à coefficients dans l'anneau $R[Y]^{alg}$ muni de la valuation de Gauss v_Y. Il reste à voir qu'au rang $n+1$ on a une approximation modulo $p^{c_{n+1}}$. On calcule le reste $R_{n+1}(X,Y) = F_m(X+Y) - (A_{m,n+1}(X,Y))^p - B_{m,n+1}(X,Y) = F_m(X+Y) - (A_{m,n}(X,Y) + AR_n)^p - B_{m,n}(X,Y) - BR_n = S_1 + S_2$ où $S_1 := R_n(X,Y) - AR_n^p - BR_n$ et $S_2 = A_{m,n}(X,Y)^p + AR_n^p - (A_{m,n}(X,Y) + AR_n)^p$. Puisque $v_Y(R_n(X,Y)) \geq c_n v(p)$ la divisibilité par p des coefficients binomiaux implique que $v_Y(S_1) \geq (c_n+1)v(p)$. De même $v_Y(S_2) \geq v(p) + v_Y(AR_n) \geq (1 + c_n/p)v(p) = c_{n+1}v(p)$.

///

Remarque 2.2.2 .— Puisque les coefficients des polynômes $(A_{m,n}, B_{m,n})$ sont obtenus par extraction de racines p-ièmes, ils vivent dans une extension $L_n/K(Y)$ galoisienne de groupe G_n, un p-groupe. Si $\tau \in G_n$, on note $(A^\tau_{m,n}, B^\tau_{m,n})$ les polynômes obtenus par l'action de τ sur les coefficients; ils donnent donc naissance à un p-développement de Taylor d'ordre m et de niveau n de $F(X)$.

2.3 Unicité

Afin de comparer les p-développements de Taylor d'un polynôme nous établissons un lemme:

Lemme 2.3.1 .— *Soit $\mathcal{R}$, un anneau intégralement clos contenant R^{alg}. Soient $a_i, a'_i, b_j, b'_j \in \mathcal{R}$ alors*

$$(\sum_{0\leq i\leq m/p} a_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b_j X^j = (\sum_{0\leq i\leq m/p} a'_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b'_j X^j \mod (p^{c_n})$$

si et seulement si $a'_i = a_i \mod (p^{c_n/p})$ et $b'_j = b_j \mod (p^{c_n})$.

Preuve. Supposons que $a'_i = a_i + p^{c_n/p} a''_i$ et $b'_j = b_j + p^{c_n} b''_j$ avec $a''_i,\ b''_j \in \mathcal{R}$, on a

$$(\sum_{0\leq i\leq m/p} a'_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b'_j X^j = (\sum_{0\leq i\leq m/p} (a_i + p^{c_n/p} a''_i) X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} (b_j + p^{c_n} b''_j) X^j =$$

$$= (\sum_{0\leq i\leq m/p} a_i X^i + p^{c_n/p} (\sum_{0\leq i\leq m/p} a''_i X^i))^p + \sum_{1\leq j\leq m,\ (j,p)=1} b_j X^j \mod (p^{c_n}) =$$

$$= (\sum_{0\leq i\leq m/p} a_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b_j X^j \mod (p^{c_n})$$

puisque $pp^{c_n/p} = p^{c_{n+1}} \in (p^{c_n})$.

L'implication réciproque se fait par récurrence sur n. Si $n = 0$, on a une égalité modulo p. Supposons donc avoir une égalité

$$(\sum_{0\leq i\leq m/p} a_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b_j X^j = (\sum_{0\leq i\leq m/p} a'_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b'_j X^j \mod (p^{c_{n+1}})$$

la récurrence permet d'écrire $a'_i = a_i + p^{c_n/p} a''_i$ et $b'_j = b_j + p^{c_n} b''_j$ avec $a''_i,\ b''_j \in \mathcal{R}$; et le calcul précédent donne la congruence

$$(\sum_{0\leq i\leq m/p} a'_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b'_j X^j =$$

$$= (\sum_{0\leq i\leq m/p} a_i X^i)^p + p^{c_n} (\sum_{0\leq i\leq m/p} a''_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b_j X^j + p^{c_n} \sum_{1\leq j\leq m,\ (j,p)=1} b''_j X^j \mod (p^{c_{n+1}})$$

et donc

$$p^{c_n} (\sum_{0\leq i\leq m/p} a''_i X^i)^p + p^{c_n} \sum_{1\leq j\leq m,\ (j,p)=1} b''_j X^j = 0 \mod (p^{c_{n+1}})$$

autrement dit

$$(\sum_{0\leq i\leq m/p} a''_i X^i)^p + \sum_{1\leq j\leq m,\ (j,p)=1} b''_j X^j = 0 \mod (p^{1/p^{n+1}})$$

et donc

$$\sum_{0\leq i\leq m/p} a''^p_i X^{ip} + \sum_{1\leq j\leq m,\ (j,p)=1} b''_j X^j = 0 \mod (p^{1/p^{n+1}})$$

ainsi $a''_i = 0 \mod (p^{1/p^{n+2}})$ et $b''_j = 0 \mod (p^{1/p^{n+1}})$. ///

Définition 2.3.2 .— Soit m, n deux entiers. On dit que 2 couples de polynômes $\in R[Y]^{alg}[X]$

$$(A_{m,n}(X,Y) = \sum_{0 \leq i \leq m/p} a_i(Y)X^i,\ B_{m,n}(X,Y) = \sum_{1 \leq j \leq m,\ (j,p)=1} b_j(Y)X^j),$$

$$(A'_{m,n}(X,Y) = \sum_{0 \leq i \leq m/p} a'_i(Y)X^i,\ B'_{m,n}(X,Y) = \sum_{1 \leq j \leq m,\ (j,p)=1} b'_j(Y)X^j),$$

sont équivalents si et seulement si

$$(A_{m,n}(X,Y))^p + B_{m,n}(X,Y) = (A'_{m,n}(X,Y))^p + B'_{m,n}(X,Y) \mod (p^{c_n}).$$

Remarque 2.3.3 .— Revenons à la remarque 2.2.2, les couples $(A_{m,n}, B_{m,n})$ et $(A^{\tau}_{m,n}, B^{\tau}_{m,n})$ sont donc équivalents dans le sens de la définition précédente. En fait une récurrence facile montre que $v_Y(A_{m,n} - A^{\tau}_{m,n}) \geq v(\lambda)$ et $v_Y(B_{m,n} - B^{\tau}_{m,n}) \geq v(\lambda^p)$.

Soit $F(X) \in R[X]$; par le lemme 2.3.1, deux couples de polynômes $\in R[Y]^{alg}[X]$ définissant un p-développement de Taylor d'ordre m et de niveau n de $F(X) \in R[X]$ sont donc équivalents; nous sommes ainsi amenés à la

Définition 2.3.4 .— Soit m, n deux entiers, on appelle *p-développement de Taylor spécial d'ordre m et de niveau n de $F(X) \in R[X]$* un couple $(A_{m,n}, B_{m,n})$ construit comme dans la proposition 2.2.1, en particulier le terme constant dans $A_{m,n}$ vaut $F(Y)^{1/p}$. Par analogie avec le développement de Taylor classique nous écrirons

$$(*)F(X+Y) = E(X,Y)^p + \sum_{1 \leq j \leq m,\ (j,p)=1} F^{[j]}(Y)X^j \mod (p^{c_n}X, X^{m+1})$$

où $E(X,Y) \in (R[Y])^{alg}[X]$, $\deg_X E(X,Y) \leq m/p$ et $F^{[j]}(Y) \in (R[Y])^{alg}$ (notez que la congruence impose l'égalité $E(0,Y)^p = F(Y)$).

On appelle *groupe de Galois attaché au p-développement de Taylor (*)* le groupe de Galois G_n de la p-extension L_n de $K(Y)$ obtenue en adjoignant les racines p-ièmes nécessaires au p-développement de Taylor (cf. remarque 2.2.2).

2.4 Spécialisation

Nous serons amenés à spécialiser la formule $(*)$; précisément si $y \in R^{alg}$ on peut tester sur $F(X+y)$ l'algorithme de la proposition 2.2.1, l'interpétation que l'on doit donner au développement ainsi construit est la suivante: quitte à faire une extension finie on peut supposer que $y \in R$; soit $\mathcal{P}$ une place du corps de fonctions L_n/K au-dessus de $(Y-y)$, on peut regarder l'image de la formule $(*)$ dans le corps résiduel $K(\mathcal{P})$; on a une congruence

$$(**)F(X+y) = E(X,Y)^p(\mathcal{P}) + \sum_{1 \leq j \leq m,\ (j,p)=1} F^{[j]}(Y)(\mathcal{P})X^j \mod (p^{c_n}X, X^{m+1})$$

que par abus de notation compatible avec la stabilité par conjugaison nous écrirons

$$(***)F(X+y) = E(X,y)^p + \sum_{1 \leq j \leq m,\ (j,p)=1} F^{[j]}(y)X^j \mod (p^{c_n}X, X^{m+1}).$$

Les zéros de $F^{[1]}(Y) \in (R[Y])^{alg}[X]$ vont jouer un rôle déterminant dans l'étude de la réduction stable des torseurs $Z^p = F(X)$. Puisque $F^{[1]}(Y)$ n'est bien défini que modulo l'action du groupe G_n (cf. remarque 2.2.2) nous introduisons la norme $N_{L_n/K(Y)}(F^{[1]}(Y)) \in R[Y]$ qui modulo p est une puissance $|G_n|$-ième de la dérivée $F'(Y)$; en fait, m sera déterminé par le lieu de branchement du torseur et n sera l'entier tel que $p^n \leq m < p^{n+1}$. Ainsi on est amené à définir:

Définition 2.4.1 .— Soit m un entier naturel et n, l'entier tel que $p^n \leq m < p^{n+1}$. Nous appellerons *p-développement de Taylor spécial d'ordre m* de $F(X) \in R[X]$ un p-développement de Taylor spécial d'ordre m et de niveau n

$$(*) F(X+Y) = E(X,Y)^p + \sum_{1 \leq j \leq m,\ (j,p)=1} F^{[j]}(Y) X^j \mod (p^{c_n} X, X^{m+1})$$

et nous appellerons *p-dérivée de niveau m* de $F(X) \in R[X]$, le polynôme

$$N_m(F^{[1]}(Y)) := N_{L_n/K(Y)}(F^{[1]}(Y)) \in R[Y].$$

3 p-développements de Taylor et réduction stable

Dans cette partie on fixe un revêtement p-cyclique $C \to \mathbb{P}^1$ de la droite projective sur K ramifié en au moins 3 points (i.e. $g(C) > 0$). Nous nous proposons de décrire le modèle stable de $(C, G = \mathbb{Z}/p\mathbb{Z})$ dans le cas où le lieu de branchement a la géométrie équidistante (cf. 1.2.1). Fixons les notations.

3.1 Notations

i) Si $P(X) \in R[X]$ on note $\bar{P}[X]$ son image dans $k[X]$.

ii) Soit $Z^p = F(X)$ une équation normalisée du revêtement $C \to \mathbb{P}^1$ i.e. $F(X) = \prod_{1 \leq i \leq m} (X - x_i)^{e_i} \in R[X]$ de degré N avec $(N,p) = 1$ et $(e_i, p) = 1$ pour $1 \leq i \leq m$. On suppose de plus que $x_i \in R$ et que $v(x_i) = v(x_i - x_j) = 0$ pour tout $i \neq j$. Ainsi le lieu de branchement $\mathrm{Br} = \{\infty, x_1, .., x_m\}$ a la géométrie équidistante. On note $\bar{\mathrm{Br}} = \{\infty, \bar{x}_1, .., \bar{x}_m\}$ la spécialisation de Br.

iii) Soit n, l'entier tel que $p^n \leq m < p^{n+1}$ et $c_n := 1 + 1/p + ... + 1/p^n$, enfin $N_m(F^{[1]}(Y)) = \prod_{\tau \in G_n} F^{[1]^\tau}(Y)$ désigne la p-dérivée de niveau m de $F(X)$ (cf. 2.4.1) où G_n est défini dans 2.3.4 et $|G_n| = p^{r(m)}$.

Proposition 3.1.1 .— *La p-dérivée de niveau m de $F(X)$, $N_m(F^{[1]}(Y))$ appartient à $R[Y]$; de plus $N_m(F^{[1]}(Y)) = \bar{F}'(Y)^{p^{r(m)}} \mod p$ et $\deg N_m(F^{[1]}(Y)) = \deg \bar{F}'(Y)^{p^{r(m)}}$.*

Preuve. Montrons l'inégalité $\deg N_m(F^{[1]}(Y)) \leq \deg \bar{F}'(Y)^{p^{r(m)}}$. L'idée est d'introduire un poids dans $R[Y]^{alg}$ qui généralise le degré dans $R[Y]$ et de suivre dans l'algorithme qui donne le p-développement de Taylor spécial d'ordre m et de niveau n le poids du coefficient $b_1(Y)$ de X dans $B_{m,n}(X,Y)$.

Précisément $-\deg_Y$ est la valuation discrète de $K(Y)$ au point ∞; cette valuation s'étend sur $K(Y)^{alg}$ en une semi-norme w: si $f \in K(Y)^{alg}$, soit $P_f(X) := \sum_{0 \leq i \leq N} a_i X^i$ le polynôme irréductible unitaire de f sur $K(Y)$; alors $w(f) := \inf_i \frac{1}{N-i}(-\deg_Y a_i)$. On reprend les notations de la prop. 2.2.1. On a $F_m(X+Y) = s_0(Y) + s_1(Y)X + ...$; on remarque que $w(s_i(Y)) \geq (i-N)$ où $N = \deg_X F$ est premier à p, ainsi $i - w(s_i(Y)) \leq N$. Considérons les formules au rang 0. On a $w((s_{ip}(Y))^{1/p}) = (ip - N)/p = i - N/p$ et donc $i - w((s_{ip}(Y))^{1/p}) \leq N/p$. Plus généralement si

$$(A_{m,n}(X,Y) = \sum_{0 \leq i \leq m/p} a_i(Y) X^i,\ B_{m,n}(X,Y) = \sum_{1 \leq j \leq m,\ (j,p)=1} b_j(Y) X^j),$$

on montre par récurrence sur n que $i - w(a_i(Y)) \leq N/p$ et que $j - w(b_j(Y)) \leq N$. Ainsi $-\deg_Y(N_m(F^{[1]}(Y)) = w(N_m(F^{[1]}(Y)) = \sum_{\tau \in G_n} w(F^{[1]^\tau}(Y)) \geq (1-N)p^{r(m)}$ et donc $\deg_Y(N_m(F^{[1]}(Y)) \leq (N-1)p^{r(m)} = \deg \bar{F}'(Y)^{p^{r(m)}}$ puisque $(N,p) = 1$. L'autre inégalité est évidente.

///

3.2 Réduction stable

Lemme 3.2.1 .— *Le modèle $\mathcal{C}'$ de C, obtenu par normalisation de* $\operatorname{Proj} R[X_0, X_1]$, *le modèle de* $\mathbb{P}^1$ *avec* $X = \frac{X_1}{X_0}$, *a une fibre spéciale réduite qui est un revêtement radiciel de* $\mathbb{P}^1_k$; *les singularités sont des cusps et se trouvent au-dessus des zéros* $\in \mathbb{P}^1_k$ *d'une forme différentielle logarithmique* ω *régulière en dehors de* $\bar{\mathrm{B}}\mathrm{r}$. *Le graphe d'intersection de la fibre spéciale* $\mathcal{C}_s$ *du modèle stable* $\mathcal{C}$ *de la courbe marquée* (C, Ram) *est un arbre et le modèle de* $\mathbb{P}^1$ *obtenu par quotient de l'action de* $\mathbb{Z}/p\mathbb{Z}$ *sur* $\mathcal{C}$ *a une fibre spéciale qui est un arbre de droites projectives attachées à* $\mathbb{P}^1_k$ *dans les zéros de* ω.

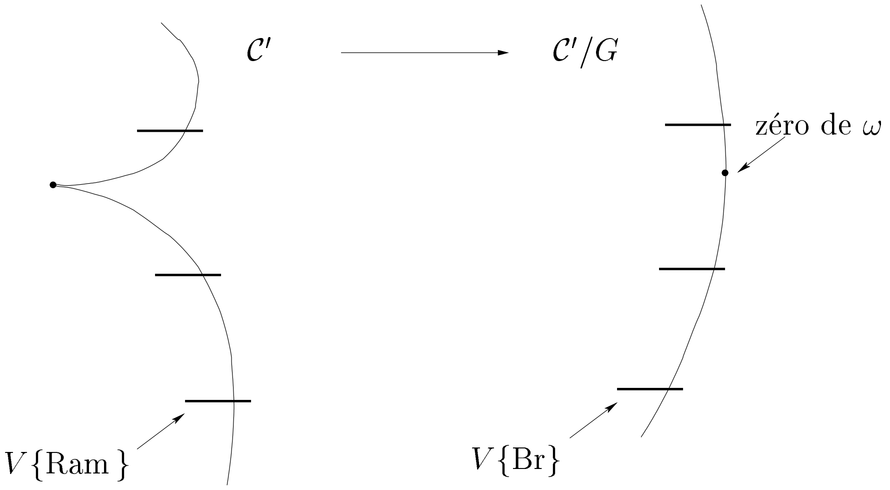


fig. 1

Commentaires. C'est un cas particulier du théorème 1' de Raynaud dans ([Ra 1]. On considère le modèle $\mathcal{C}'$ de C obtenu par clôture intégrale dans $K(C)$ du modèle minimal de $\mathbb{P}^1$ qui déploie le lieu de branchement; ici c'est le modèle lisse de $\mathbb{P}^1$ correspondant à la coordonnée X de l'équation normalisée $Z^p = F(X)$. La fibre spéciale $\mathcal{C}'_s$ est homéomorphe à $\mathbb{P}^1_k$; les singularités sont des cusps. Il reste à faire une étude locale: l'équation $Z^p = F(X)$ induit en réduction une équation $\bar{Z}^p = \bar{F}(X)$; il suit par le critère Jacobien que les cusps sont concentrés au-dessus des zéros de $\bar{F}'(X)$. Soit $x_1 \in \mathrm{Br}$ et $\bar{x}_1$ sa spécialisation; une équation locale de $\mathcal{C}'$ dans la fibre formelle en $\bar{x}_1$ est $Z'^p = (X - x_1) \prod\limits_{2 \leq i \leq m} (X - x_i)^{u_1 e_i}$ où $u_1 e_1 = 1 \mod p$. Cette équation induit un modèle lisse au-dessus de $\bar{x}_1$. On a donc montré que les cusps ne sont pas au-dessus de $\{\infty, \bar{x}_1, ..., \bar{x}_m\}$ et se trouvent au-dessus de zéros de $\bar{F}'(X)$; plus simplement dit ils sont au-dessus des zéros de $\omega = \frac{d\bar{F}}{\bar{F}}$ (cf. fig. 1). Notons (ω_0) (resp. (ω_∞)) le diviseur des zéros (resp. pôles) de ω, alors $\deg(\omega_0) = \deg(\omega_\infty) - 2 = m - 1$). Ainsi le modèle stable est lisse au-dessus de $\mathbb{P}^1$ en dehors des zéros de ω. Soit x un tel zéro, après localisation en x on se retrouve dans la situation locale décrite par Raynaud dans ([Ra 1], démonstration du théorème 1 p. 182), le lemme suit.

Ce lemme montre que dans la situation où le lieu de branchement est équidistant on aura un algorithme pour trouver la réduction stable dès que l'on saura détecter les composantes de genre non nul. Le théorème suivant donne un tel algorithme.

Théorème 3.2.2 *Chaque composante de genre non nul du modèle stable correspond à une valuation de Gauss sur un disque fermé de* $\mathbb{P}^1$ *qui peut être ainsi définie. Pour* $\bar{d}$ *un zéro de* $\bar{F}'(X)$ *qui n'est pas un zéro de* $\bar{F}(X)$, *soit* $m(\bar{d}) - 1 \leq m - 1$, *son ordre et soient* $d_1, ..., d_{\varphi(\bar{d})}$ *les zéros qui se spécialisent dans* $\bar{d}$ *de* $N_m(F^{[1]}(Y))$, *la* p*-dérivée de* $F(X)$ *de niveau* m, *alors* $\varphi(\bar{d}) = p^{r(m)}(m(\bar{d}) - 1)$ *(on a* $\overline{N_m(F^{[1]}(Y))} = \bar{F}'(Y)^{p^{r(m)}}$*). Pour* d_i *avec* $1 \leq i \leq \varphi(\bar{d})$, *considérons* $\tau_i \in G_n$ *tel que* $F^{[1]^{\tau_i}}(d_i) = 0$, *alors*

$$F(X) = E^{\tau_i}(X - d_i, d_i)^p + \sum_{2 \leq j \leq m,\, (j,p)=1} F^{[j]^{\tau_i}}(d_i)(X - d_i)^j \mod (p^{c_n}(X - d_i), (X - d_i)^{m+1}).$$

Soit $\rho(d_i) \in K^{alg}$ tel que

$$(*)\ v(\rho(d_i)) = \max_{2\le j\le m(\bar{d}),\,(j,p)=1} \frac{1}{j} v\left(\frac{\lambda^p}{F^{[j]^{\tau_i}}(d_i)}\right),$$

alors la valuation de Gauss relative au disque $v(X-d_i) \geq v(\rho(d_i))$ induit dans le modèle stable une composante de genre non nul; de plus toutes les composantes de genre non nul sont ainsi obtenues. Soit $\mathcal{P}^1$, le modèle semi-stable minimal de $(\mathbb{P}^1, \mathrm{Br})$ qui induit ces valuations , alors le modèle stable $\mathcal{C}$ de (C,G) est la clôture intégrale de $\mathcal{P}^1$; les bouts de l'arbre d'intersection représentent les composantes de genre non nul et l'origine correspond à la composante induite par le disque $v(X) \geq 0$. Enfin les composantes de genre non nul sont des revêtements étales de la droite affine; en particulier la jacobienne de C a potentiellement bonne réduction supersingulière.

Preuve.

A.— Avant de passer à la preuve il faut remarquer que dans le cas où $m < p$, le développement de Taylor classique suffit (2.1.2.i)); le théorème est alors mot pour mot le théorème 2 de Lehr ([Le 2]). Passons à la preuve dans le cas général; elle présente des difficultés nouvelles à cause de la complexité des p-développements de Taylor lorsque $m \geq p$.

B.— Voyons que les valuations de Gauss relatives au disque $v(X-d_i) \geq v(\rho(d_i))$ induisent une composante de genre non nul dans le modèle stable. Pour simplifier l'écriture nous écrirons ρ_i à la place de $\rho(d_i)$.

Soit $m_i \geq 2$, $(m_i,p)=1$, le maximum des entiers j, $2 \leq j \leq m(\bar{d})+1$ qui satisfont l'égalité dans la relation $(*)$ du théorème. Notons que le p-développement de Taylor spécial induit modulo (p) le développement de Taylor classique; ainsi par définition de $m(\bar{d})$ on a $v(m(\bar{d})F^{[m(\bar{d})]^{\tau_i}}(d_i)) = 0$ et donc $v(\rho_i) \geq \frac{1}{m(\bar{d})} v(\lambda^p) \geq \frac{1}{m} v(\lambda^p) > 0$. On pose $X - d_i = \rho_i T$; l'équation du revêtement devient

$$Z^p = F(X) = E^{\tau_i}(\rho_i T, d_i)^p + \sum_{2\le j\le m,\,(j,p)=1} F^{[j]^{\tau_i}}(d_i)\rho_i{}^j T^j \mod (p^{c_n}\rho_i T, (\rho_i T)^{m+1}).$$

Puisque $v(p^{c_n}\rho_i) \geq c_n v(p) + \frac{1}{m} v(\lambda^p) = (1 - 1/p^{n+1} + 1/m) v(\lambda^p) > v(\lambda^p)$ (**c'est là, la justification de l'approximation modulo p^{c_n} dans les p-développements de Taylor d'ordre** m), le changement $Z = \lambda W + E(\rho_i T, d_i)$ donne une équation entière qui en réduction induit une équation séparable

$$\bar{W}^p - \overline{F(d_i)}^{(p-1)/p}\bar{W} = \sum_{2\le j\le m,\,(j,p)=1} \overline{F^{[j]^{\tau_i}}(d_i)\rho_i{}^j/\lambda^p}\,\bar{T}^j = u_2\bar{T}^2 + \ldots + u_{m_i}\bar{T}^{m_i}$$

où $u_{m_i} \neq 0$. On a ainsi exhibé une composante de $\mathcal{C}_s$ de genre $(m_i-1)(p-1)/2$ et d'invariant de Hasse-Witt nul. ///

C.— Passons au point le plus délicat à savoir que l'on obtient bien ainsi toutes les valuations qui donnent un genre non nul dans le modèle stable; il nous faut montrer que la somme des genres des composantes produites par l'algorithme comme au-dessus est $g(C) = (m-1)(p-1)/2$. Il n'est à priori pas garanti que ce soit le cas car la condition d'annulation de $N_m(F^{[1]}(Y))$ imposée dans l'algorithme est certainement restrictive; on pourrait trouver la même valuation de Gauss trop souvent et ainsi oublier des composantes. Nous allons voir qu'il n'en est rien.

Soit $N(d_i)$ le nombre (avec multiplicité) de zéros d de $N_m(F^{[1]}(Y))$ tels que $v(d-d_i) \geq v(\rho_i)$; nous allons montrer que $N(d_i) = p^{r(m)}(m_i-1)$. La stratégie est la suivante: puisque $N_m(F^{[1]}(Y)) \in K[Y]$ alors pour $y \in R^{alg}$ avec $v(y-d_i) < v(\rho_i)$ et proche de $v(\rho_i)$, il existe $C(d_i) \in \mathbb{Q}$ tel que $v(N_m(F^{[1]}(y))) = N(d_i)v(y-d_i) + C(d_i)$, une fonction linéaire affine de

$v(y-d_i)$. Nous allons utiliser deux p-développements de Taylor spéciaux d'ordre m de $F(X)$. L'un centré en d_i et l'autre en y; ces deux développements donnent un modèle pour l'extension valuée au-dessus de la valuation de Gauss sur le disque fermé $v(X-d_i) \geq v(y-d_i)$; sur chacun de ces modèles on peut lire la différente dans l'extension valuée (dégénérescence de $\boldsymbol{\mu}_p$ à $\boldsymbol{\alpha}_p$) et la comparaison des $\boldsymbol{\alpha}_p$-torseurs induits par chaque modèle permet de conclure (cf. 1.1).

Puisque pour $j \leq m(\bar{d})$, $v(F^{[j]^{\tau_i}}(d_i))+jv(\rho_i) \geq v(F^{[m_i]^{\tau_i}}(d_i))+m_i v(\rho_i) = pv(\lambda)$, avec l'inégalité sticte pour $m_i < j \leq m(\bar{d})$; il suit que pour ρ avec $0 < v(\rho_i/\rho) < \epsilon$ et ϵ suffisament petit on conserve les mêmes inégalités si on remplace ρ_i par ρ. Quitte à faire une extension des scalaires d'uniformisante encore notée π, on peut supposer que $v(F^{[m_i]^{\tau_i}}(d_i))+m_i v(\rho) = ptv(\pi) < pv(\lambda)$. Soit $Z = \pi^t W + E^{\tau_i}(X-d_i, d_i)$ et $X - d_i = \rho T$, puisque $v(\lambda/\pi^t) > 0$ alors $W^p = uT^{m_i} \mod \pi$, et si $w_{\frac{X-d_i}{\rho}}$ désigne la valuation de Gauss associée au disque $v(X-d_i) \geq v(\rho)$, la valuation de la différente dans l'extension valuée correspondante est $v_\pi(p) - (p-1)t$ (cf. 1.1.1).

Pour y avec $v(y-d_i) = v(\rho)$ et $\tau \in G_n$, on a un p-développement de Taylor spécial

$$F(X = X-y+y) = E^\tau(X-y,y)^p + \sum_{(j,p)=1} F^{[j]^\tau}(y)(X-y)^j \mod (p^{c_n}(X-y), (X-y)^{m+1}).$$

Comme précédemment on écrit $\inf_j(v(F^{[j]^\tau}(y)) + jv(\rho)) = pt'v(\pi)$. Puisque y est dans le disque $v(X-d_i) \geq v(\rho)$; la valuation de la différente dans l'extension valuée par $w_{\frac{X-d_i}{\rho}}$ est aussi $v_\pi(p)-(p-1)t'$ (cf. 1.1); ainsi $t = t'$. D'autre part si l'on pose $Z = \pi^t W' + E^\tau(X-y,y)$ et $X - y = \rho S$, il suit que $W'^p \equiv c_0 + c_1 S + \ldots \mod \pi$ qui est à comparer à $W^p \equiv uT^{m_i} \mod \pi$. On a $W - W' = \frac{E^\tau(X-y,y) - E^{\tau_i}(X-d_i,d_i)}{\pi^t}$ ainsi $\bar{W}^p - \bar{W'}^p \in (k[S])^p$ et donc $u(S+(y-d_i)/\rho)^{m_i} - c_0 - c_1 S + \ldots \in k[S^p]$ modulo π. Puisque $(m_i, p) = 1$ et que $v((y-d_i)/\rho) = 0$, il suit que $v(c_1) = 0$ (comparer avec 1.1.1). Ainsi $v(F^{[1]^\tau}(y)) + v(\rho) = ptv(\pi) = m_i v(\rho) + v(F^{[m_i]^{\tau_i}}(d_i))$; et donc il existe $C(d_i)$ avec $v(N_m(F^{[1]}(y))) = (m_i - 1)p^{r(m)}v(\rho) + C(d_i)$; ainsi $N(d_i) = p^{r(m)}(m_i - 1)$. ///

D.— Soit $\bar{d}$, un zéro de $\omega = d\bar{F}/\bar{F}$ de multiplicité $m(\bar{d}) - 1$ et d_i, d_j deux zéros de $N_m(F^{[1]}(Y))$ qui se spécialisent en $\bar{d}$.

Remarquons que la relation $v(d_i - d_j) \geq v(\rho_i)$ implique que $v(\rho_i) = v(\rho_j)$; en effet supposons que $v(d_i - d_j) \geq v(\rho_i) > v(\rho_j)$; on peut alors considérer le p-développement de Taylor spécial d'ordre m de $F(X)$ centré en d_i. Puisque $v(p^{c_n}\rho_i) > v(p^{c_n}\rho_j) > v(\lambda^p)$, le changement de variable $X - d_i = \rho_j T$ induit un $\boldsymbol{\alpha}_p$ torseur en réduction (voir étape C) alors que par définition de d_j et ρ_j l'étape B montre que l'on a un $\mathbb{Z}/p\mathbb{Z}$-torseur! Contradiction.

Nous pouvons donc définir une partition indexée par $I(\bar{d})$ des $\varphi(\bar{d})$ zéros de $N_m(F^{[1]}(Y))$ qui se spécialisent en $\bar{d}$ de la manière suivante: d_i et d_j seront équivalents si et seulement si $v(d_i - d_j) \geq v(\rho_i) = v(\rho_j)$. Notons que cette relation d'équivalence est la même que celle qui range les d_i suivant la valuation de Gauss induite par le disque fermé $v(X - d_i) \geq v(\rho_i)$. Par l'étape C, chaque classe d'équivalence a un cardinal de la forme $p^{r(m)}(m_i - 1)$ et par l'étape B, chaque représentant de cette classe induit une même composante dans le modèle stable de genre $(m_i - 1)(p-1)/2$. Puisque $\varphi(\bar{d}) = p^{r(m)}(m(\bar{d}) - 1) = \sum_{i \in I(\bar{d})} p^{r(m)}(m_i - 1)$, on obtient pour chaque $\bar{d}$ une contribution au genre dans le modèle stable égale à $\sum_{i \in I(\bar{d})} (m_i - 1)(p-1)/2 = (m(\bar{d}) - 1)(p-1)/2$. Enfin puisque $\deg(\omega)_0 = m - 1$, $\sum_{\bar{d} \in (\omega)_0} (m(\bar{d}) - 1) = m - 1$; ainsi la somme des contributions au genre de $\mathcal{C}_s$ est $(m-1)(p-1)/2 = g(C)$.

///

E.— Puisque deux disques $v(X - d_i) \geq v(\rho_i)$ qui sont en inclusion sont confondus il suit qu'ils correspondent à des bouts dans l'arbre d'intersection (voir fig.2); ce dernier point est conforme à [Ra 1], exemple (1) p. 186. Enfin la jacobienne de C a potentiellement bonne réduction supersingulière par ([Ra 2]).

///

Remarque 3.2.3 .—

i) L'exemple qui suit montre que lorsque $m > p$ les zéros de F' ne donnent plus nécessairement des centres des disques qui induisent des composantes de genre non nul. Soit $m > p$ et $(m, p) = 1$ et $F(X) := (1 + X)^p + X^m$ (i.e. on part d'un p-développement exact; ainsi 0 est racine de la p-dérivée de niveau m) alors le disque fermé de centre 0 et de rayon $(p/m)v(\lambda)$ induit la bonne réduction. Les racines de F' sont de valuation $\frac{v(p)}{m-1} = \frac{p-1}{m-1}v(\lambda) < (p/m)v(\lambda)$; elles sont à l'extérieur du disque!

ii) Soit $y \in R^{alg}$ tel que $v(N_m(F^{[1]}(y)) \geq p^{r(m)}c_n v(p)$, il existe $\tau \in G_n$ avec $v(F^{[1]}(y)) \geq c_n v(p)$, alors le p-développement de Taylor de $F(X+y)$ correspondant induit une composante de genre non nul en réduction (même preuve que dans l'étape B); ainsi il existe un zéro d_i de $N_m(F^{[1]}(Y))$ avec $v(d_i - y) \geq v(\rho(d_i))$.

iii) La preuve du théorème montre que le nombre de composantes de genre non nul de la fibre spéciale $\mathcal{C}_s$ du modèle stable est majoré par $m - 1$. Le polynôme $N_m(F^{[1]}(Y))$ est de degré $\deg \bar{F}'(Y)^{p^{r(m)}} = (N-1)p^{r(m)}$ qui peut être très élevé puisque $p^{r(m)}$ est le cardinal du groupe de Galois de l'extension de $K(Y)$ engendrée par les coefficients mis en jeu dans l'algorithme. Dans le cas où $m < p$, on a vu en (2.1.2.i)) que $F'(Y)$ convient et puisque les seuls zéros à retenir sont ceux qui se spécialisent dans les zéros de $\omega = d\bar{F}/\bar{F}$, C. Lehr a introduit le polynôme $N(Y)$ numérateur de la fraction irréductible $F'(Y)/F(Y)$; ainsi $N(Y)$ divise $F'(Y)$, il est de degré $m - 1$ et ses zéros donnent des centres pour les valuations correspondant aux composantes de genre non nul de la fibre spéciale $\mathcal{C}_s$ du modèle stable. Dans le cas général il serait souhaitable d'exhiber un polynôme de degré minimal sur K ayant cette propriété.

Remarque 3.2.4 .— Il est possible de donner (cf. [He], [Sa 1,2,3]), des conditions combinatoires et différentielles qui sont des conditions nécessaires et suffisantes pour qu'une courbe stable sur k soit de la forme $\mathcal{C}_s$ comme dans le théorème (cf. fig. 2) .

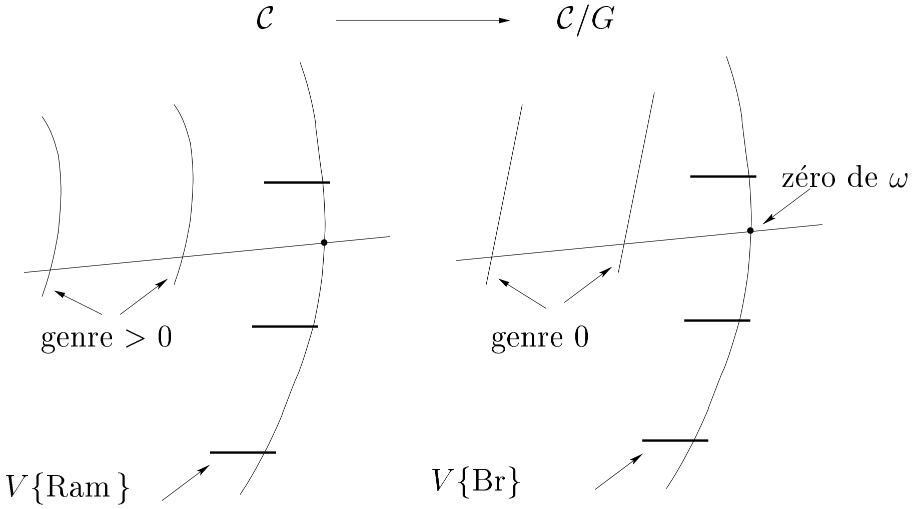


fig. 2

3.3 Bonne réduction

Il suit facilement du théorème 3.2.2 un critère de potentielle bonne réduction.

Théorème 3.3.1 .— *La courbe C a potentiellement bonne réduction si et seulement si le modèle stable $\mathcal{C}$ de (C, G) a 2 composantes à savoir une composante de genre $g(C)$ et une droite projective sur laquelle se spécialise le lieu de branchement en $m+1$ points distincts lisses. C'est le cas si et seulement si les zéros y_i de $N_m(F^{[1]}(Y))$, la p-dérivée de niveau m de $F(X)$, qui ne se spécialisent pas dans les zéros de $F(X)$ sont tels que $v(y_i - y_j) \geq \frac{1}{m} v(\lambda^p)$.*

Preuve. En effet il suffit de reprendre le début de la preuve du théorème 3.2.2. On a potentiellement bonne réduction si et seulement un zéro de $N_m(F^{[1]}(Y))$ qui ne se spécialisent pas dans un zéro de $F(X)$ donne naissance à une composante de genre $(m-1)(p-1)/2$; i.e. de conducteur $m_i = m$. Ceci ne se produit que si $v(\rho(d_i)) = \frac{1}{m} v(\lambda^p)$ et si les racines de $N_m(F^{[1]}(Y))$ donnent naissance à la même valuation. ///

Ce critère nécessite le calcul de $N_m(F^{[1]}(Y))$ et une localisation non triviale de ses racines. Dans un cas particulier C. Lehr a donné un critère simple; nous allons rappeler ce critère et voir qu'il découle naturellement de notre algorithme.

Théorème 3.3.2 ([Le 2], théorème 1).— *Soit $F(X)$ comme au-dessus. Ecrivons $\frac{F'(X)}{F(X)} = \frac{N(X)}{D(X)}$ où $N(X)$ est unitaire et $(N(X), D(X)) = 1$.*

i) Si C a potentiellement bonne réduction, alors $(m, p) = 1$ et il existe $d \in R^{alg}$ tel que $N(X) = (X-d)^{m-1} \mod (\lambda^{p/m})$.

ii) Si $(m-1, p) = 1$, si C a bonne réduction, alors la congruence ci-dessus détermine la classe de $d \mod \lambda^{p/m}$; precisément si $(m-1)d := \sum\limits_i x_i - \frac{1}{\sum\limits_i e_i} \sum\limits_i e_i x_i \in R$, la valuation de Gauss relative à $\frac{X-d}{\lambda^{p/m}}$ induit le modèle lisse sur $R[F(d)^{1/p}]$.

Preuve. Nous remontrons la congruence en utilisant notre algorithme. Le torseur en réduction relativement à v_X, la valuation de Gauss associée à X, ne présente qu'un cusp (cf. lemme 3.2.1); ainsi $\bar{F}'(X)/\bar{F}(X)$ n'a qu'une racine qui est donc d'ordre $m-1$; en particulier $(m, p) = 1$. Soit y une racine de $N_m(F^{[1]}(Y))$ avec $v(F(y)) = 0$, alors $v(F^{[m]}(y)) = 0$ et $v(\rho(y)) = v(\lambda^{p/m})$. Le p-développement de Taylor spécial d'ordre m donne $F(X) = E(X-y, y)^p + F^{[1]}(y)(X-y) + \dots + F^{[m]}(y)(X-y)^m \mod (p^{c_n}(X-y), (X-y)^{m+1})$ et $v(\rho(y)) \geq \frac{1}{j}(v(\lambda^p) - v(F^{[j]}(y)))$ pour $(j, p) = 1$ et $j \leq m$, avec égalité pour $j = m$; ainsi $v(F^{[j]}(y)) \geq (1 - j/m) v(\lambda^p) \geq v(\lambda^{p/m})$ pour $j < m$ et premier à p. On a $F(X) = \prod\limits_{1 \leq i \leq m} (X - x_i)^{e_i}$ et donc avec $N = \sum e_i$

$$N(X) = \frac{1}{N} \frac{F'(X)}{F(X)} \prod_{1 \leq i \leq m} (X - x_i);$$

ainsi il existe $C(X),\ D(X) \in R[X]$ tels que

$$N(X+y) =$$

$$= \frac{1}{N}[pE(X,y)^{p-1}E'(X,y) + \sum_{j \leq m,\ (j,p)=1} F^{[j]}(y) j X^{j-1} + \lambda^{p-1/p^n} C(X) + X^m D(X)] \prod_{1 \leq i \leq m} (y - x_i + X)^{-e_i+1} =$$

$$= X^{m-1} \prod_{1 \leq i \leq m} (1 + X/(y - x_i))^{-e_i+1} \mod (\lambda^{p/m}, X^m) R[[X]]$$

qui donne la congruence du théorème puisque $N(X)$ est un polynôme unitaire de degre $m-1$.

Le reste de la preuve est immédiat.

///

Remarque 3.3.3 . —

i) Si on a un centre y et un rayon candidats il est facile de tester la bonne réduction: il suffit en effet d'appliquer l'algorithme en $Y = y$, ce qui fournit le p-développement de Taylor spécial de niveau m susceptible d'induire la bonne réduction. On peut aussi utiliser la proposition 2.5 de [Le 2].

ii) La condition $(m-1,p) = 1$ est très restrictive en particulier pour les petits p et si $p = 2$; le critère de Lehr est vide.

En fait ce critère admet une version locale que nous devons à une conversation avec C. Lehr.

Proposition 3.3.4 . — *Soit $F(X)$ et $N(X)$ comme au-dessus. Soit $\bar{d}$ un zéro de $\bar{F}'$ d'ordre $m(\bar{d})-1$; on note $d_1, ..., d_{m(\bar{d})-1}$ les zéros de $N(X)$ qui se spécialisent en $\bar{d}$ et $N_{\bar{d}}(X) := (X-d_1)...(X-d_{m(\bar{d})-1})$.*

i) Si la fibre spéciale $\mathcal{C}_s$ du modèle stable $\mathcal{C}$ de la courbe marquée (C, Ram) présente une seule composante de genre non nul passant par $\bar{d}$, alors $(m(\bar{d}), p) = 1$ et il existe $d \in R^{alg}$ tel que $N_{\bar{d}}(X) = (X-d)^{m(\bar{d})-1} \mod (\lambda^{p/m(\bar{d})})$.

ii) Si $(m(\bar{d})-1, p) = 1$, et si la fibre spéciale $\mathcal{C}_s$ du modèle stable $\mathcal{C}$ de la courbe marquée (C, Ram) a une composante irréductible de genre non nul passant par $\bar{d}$, alors la congruence ci-dessus détermine la classe de $d \mod \lambda^{p/m(\bar{d})}$; precisément $(m(\bar{d})-1)d = \sum_{1 \le i \le m(\bar{d})-1} d_i \mod \lambda^{p/m(\bar{d})}R$ et la valuation de Gauss relative à $\frac{X-d}{\lambda^{p/m(\bar{d})}}$ induit la composante de genre non nul passant par $\bar{d}$.

Preuve. Montrons la congruence. Soit y un zéro de $N_m(F^{[1]}(Y))$ qui se spécialise en $\bar{d}$, cette fois-ci le p-développement spécial d'ordre m de $F(X)$ centré en y est tel que $v(F^{[m(\bar{d})]}(y)) = 0$ et donc $v(\rho(y)) = v(\lambda^{p/m(\bar{d})})$. Les mêmes calculs que précédemment conduisent alors à la congruence $N(X) = (X-y)^{m(\bar{d})-1}Q(X) \mod (\lambda^{p/m(\bar{d})})R[X]$ où $Q(X)$ est un polynôme unitaire de $R[X]$. Soit $\tilde{d}$ une racine de $N(X)$ qui ne se spécialise pas en $\bar{d}$, alors $v(\tilde{d}-y) = 0$, ainsi $Q(\tilde{d}) \in (\lambda^{p/m(\bar{d})})R$ et la congruence précédente induit donc la congruence $\frac{N(X)}{X-\tilde{d}} = (X-y)^{m(\bar{d})-1}\frac{Q(X)-Q(\tilde{d})}{X-\tilde{d}} \mod (\lambda^{p/m(\bar{d})})R[X]$; on a donc "divisé" par $X-\tilde{d}$. En réitérant le procédé on obtient la congruence $N_{\bar{d}}(X) = (X-y)^{m(\bar{d})-1} \mod (\lambda^{p/m(\bar{d})})R[X]$. Le reste est immédiat.

///

4 Exemples

Nous reprenons les notations de la partie 3.

Dans cette partie nous illustrons les théorèmes précédents. Comme dans ([Ra 1]), la question de la situation générale se pose. Nous passerons ensuite à des exemples plus spécifiques.

4.1 Le cas de ramification générale

Nous imposons des conditions générales au lieu de branchement (toujours sous l'hypothèse d'équidistance); en fait la condition est que la spécialisation du lieu de branchement est en position générale; la proposition suivante est de ce point de vue un analogue facile de ([Ra 1], cor. 4 p. 194).

Proposition 4.1.1 . — *Soit $Z^p = F(X) = \prod_{1 \le i \le m} (X-x_i)^{e_i}$ avec $(e_i, p) = 1$ et $(\deg F, p) = 1$. On suppose que $v(x_i - x_j) = v(x_i) = 0$ pour tout $i \neq j$. Alors il existe un polynôme $\Delta(X_1, ..., X_m) \in k[X_1, ..., X_m] - \{0\}$ tel que la condition $\Delta(\bar{x}_1, ..., \bar{x}_m) \neq 0$ implique que la forme différentielle $\omega =$*

$d\bar{F}(X)/\bar{F}(X)$ n'a que des zéros simples $z_1, ..., z_{m-1}$. Ainsi la fibre spéciale du modèle stable $\mathcal{C}$ de (C, G) qui déploie le lieu de branchement est constituée d'une part d'une droite projective sur k contenant les $m+1$ spécialisations du lieu de branchement et les $m-1$ zéros de ω; et d'autre part de $m-1$ composantes de genre $(p-1)/2$ si $p > 2$ et de genre 1 si $p = 2$ intersectant la droite projective dans les zéros de ω.

Preuve. Afin de montrer l'existence de Δ nous montrons 2 lemmes suivant que $p > 2$ ou que $p = 2$.

Lemme 4.1.2 .— *Soit $p > 2$, $m \geq 3$ et $f(X) := \prod_{1\leq i\leq m} (X - x_i)^{e_i} \in k[X]$ où $(e_i, p) = 1$ et $(N = \sum_i e_i, p) = 1$. Soit $S_m(x_i, e_i)(X) := \sum_{1\leq i\leq m} e_i \prod_{1\leq j\leq m, j\neq i} (X - x_j)$ alors son discriminant* $\mathrm{Disc}\,(S_m(x_i, e_i)(X)) \in \mathbb{F}_p[x_1, x_2, ..., x_m]$ *n'est pas identiquement nul.*

Preuve. Nous faisons une preuve par récurrence sur m. Si $m = 3$, $x_1 = 0, x_2 = 1$, alors

$$S_3(x_i, e_i)(X) = e_3X(X-1) + e_2X(X - x_3) + e_1(X-1)(X - x_3) =$$

$$= (e_1 + e_2 + e_3)X^2 + (-e_3 - e_2x_3 - e_1 - e_1x_3)X + e_1x_3$$

son discriminant est

$$(-e_3 - e_2x_3 - e_1 - e_1x_3)^2 - 4(e_1 + e_2 + e_3)e_1x_3 =$$

$$= (e_1 + e_2)^2x_3^2 + (2(e_1 + e_3)(e_1 + e_2) - 4e_1(e_1 + e_2 + e_3))x_3 + (e_1 + e_3)^2$$

qui n'est pas identiquement nul.

Pour $m > 3$ nous utilisons un argument de spécialisation: soit $f(X)$ comme dans le lemme; quitte à changer l'ordre des x_i on peut supposer que $e_{m-1} + e_m \neq 0 \mod p$, alors

$$S_m(x_i, e_i)(x_m = x_{m-1})(X) = (X - x_{m-1})S_{m-1}((x_1, e_1), ..., (x_{m-2}, e_{m-2}), (x_{m-1}, e_{m-1} + e_m))(X);$$

de plus

$$S_{m-1}((x_1, e_1), ..., (x_{m-2}, e_{m-2}), (x_{m-1}, e_{m-1} + e_m))(X = x_{m-1}) = (e_{m-1} + e_m) \prod_{1\leq i\leq m-2} (x_{m-1} - x_i)$$

et par récurrence, pour $x_1, ..., x_{m-1}$ en position générale $S_m(x_i, e_i)(x_m = x_{m-1})(X)$ est de degré $m-1$ et n'a que des racines simples; ainsi $\mathrm{Disc}\,(S_m(x_i, e_i)(X))$, n'est pas identiquement nul. ///

Lemme 4.1.3 .— *Si $p = 2$, soit $f(X) := \prod_{1\leq i\leq 2\ell+1} (X - x_i) \in k[X]$, avec $x_1, ..., x_{2\ell+1} \in k^{2\ell+1}$, alors $f'(X) = \Sigma(X)^2$ et* $\mathrm{Disc}\, f(X)\mathrm{Disc}\,\Sigma(X) \in \mathbb{F}_2[x_1, x_2, ..., x_{2\ell+1}]$ *n'est pas identiquement nul.*

Preuve. Soit $\Sigma(X) := \prod_{1\leq i\leq 2\ell+1} (X - y_i) \in k[X]$ avec $y_i \neq y_j$ si $i < j$. Soit $f(X) = 1 + \Sigma(X)^2 + X\Sigma(X)^2$ alors $f'(X) = \Sigma(X)^2$. Ainsi $\mathrm{Disc}\, f(X)\mathrm{Disc}\,\Sigma(X) \neq 0$. ///

Nous passons à la preuve de la proposition.

Si $p > 2$, le lemme 4.1.2 montre qu'il existe $\Delta(X_1, ..., X_m) \in k[X_1, ..., X_m] - \{0\}$ tel que la condition $\Delta(\bar{x}_1, ..., \bar{x}_m) \neq 0$ implique que la forme différentielle $\omega = d\bar{F}(X)/\bar{F}(X)$ dont le numérateur vaut $S_m(x_i, e_i)(X)$ n'a que des zéros simples $z_1, ..., z_{m-1}$; on se retrouve localement avec un conducteur $< p$. Conformément à [Le 2], les zéros y_i de la dérivée F' tels que $F(y_i)$ est une unité fournissent des centres des disques qui induisent un genre non nul dans le modèle stable. Alors pour un tel zéro on a $F(X + y_i) = F(y_i) + \frac{F''(y_i)}{2}X^2 + ...$, il suit du lemme 4.1.2 que $v(F''(y_i)) = 0$. Soit $X = \lambda^{p/2}T$ alors $F(y_i + \lambda^{p/2}T) - F(y_i) \in \lambda^p R^{alg}[T]$ induit un revêtement étale de la droite affine de conducteur $m_i = 2 < p$ comme annoncé (cf. fig. 3)

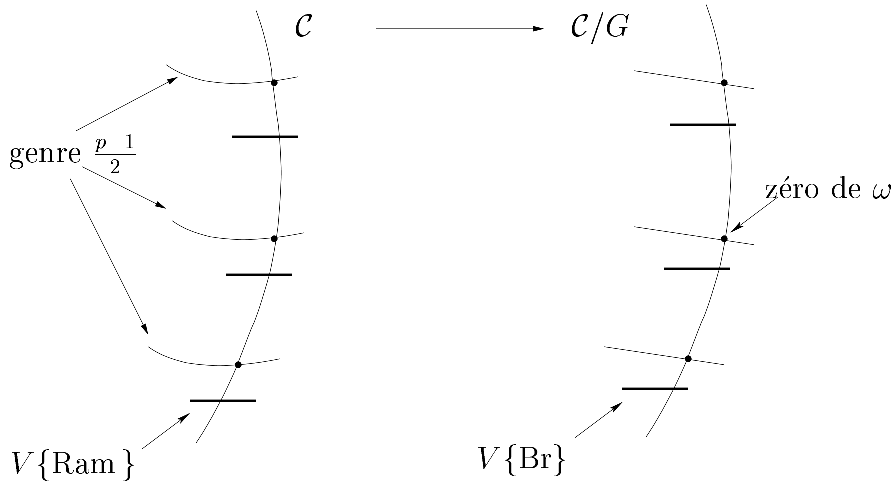


fig. 3

Si $p = 2$, le lemme 4.1.3. montre qu'il existe $\Delta(X_1, ..., X_m) \in k[X_1, ..., X_m] - \{0\}$ tel que la condition $\Delta(\bar{x}_1, ..., \bar{x}_m) \neq 0$ implique que la forme différentielle $\omega = d\bar{F}(X)/\bar{F}(X)$ n'a que des zéros $z_1, ..., z_{(m-1)/2}$ de multiplicité 2; contrairement au cas précédent on se retrouve localement avec un conducteur $> p = 2$. Nous appliquons l'algorithme du théorème 3.2.2. Ecrivons le 2-développement de Taylor spécial de F de niveau 3, on a $F(X+Y) = s_0(Y) + s_1(Y)X + s_2(Y)X^2 + s_3(Y)X^3... = (s_0(Y)^{1/2} + s_2(Y)^{1/2}X)^2 + (s_1(Y) - 2s_0(Y)^{1/2}s_2(Y)^{1/2})X + s_3(Y)X^3...$; la norme du coefficient de X donne $N_3(F^{[1]}(Y)) = s_1(Y)^2 - 4s_0(Y)s_2(Y) = F'^2 - 2FF$". Soit y une racine de $N_3(F^{[1]}(Y))$ qui se réduit sur une racine $\omega = d\bar{F}/\bar{F}$; alors $s_0(y) = F(y)$ et $s_3(y)$ sont des unités et pour un choix convenable de la racine y on obtient: $F(X+y) = (s_0(y)^{1/2} + s_2(y)^{1/2}X)^2 + s_3(y)X^3....$ Soit $X = \lambda^{2/3}T$ et $Z = \lambda W + (s_0(y)^{1/2} + s_2(y)^{1/2}X)$, alors en réduction on obtient l'équation $W^2 - W = \bar{s}_3(y)T^3$. Pour conclure il n'est nul besoin d'invoquer le théorème 3.2.2 puisque chaque zéro de $\omega = d\bar{F}(X)/\bar{F}(X)$ donne naissance à une (seule) composante; il est alors immédiat de vérifier que l'on a le bon genre à la fibre spéciale. (cf. fig. 4)

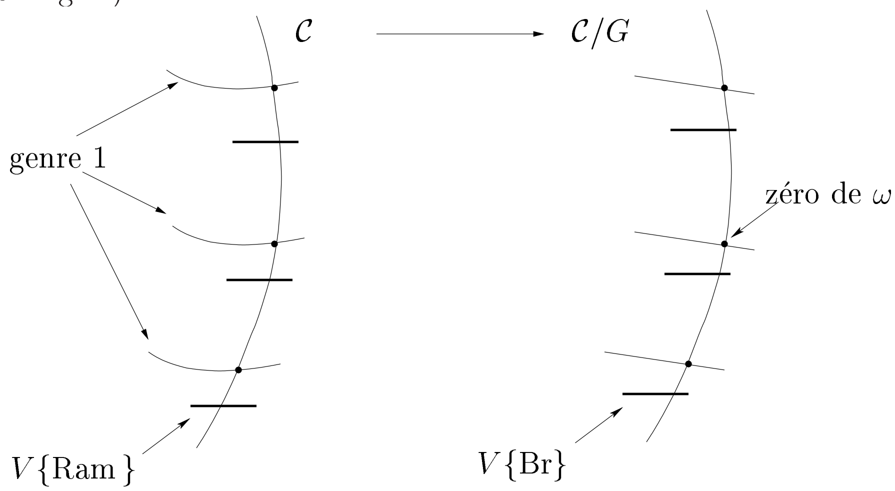


fig. 4

4.2 Les courbes hyperelliptiques en $p = 2$

On a donc $F(X) = s_0 + s_1X + ... + X^m$ avec $(m, 2) = 1$ et $\text{Disc}\,\bar{F} \neq 0$. Nous allons examiner le cas où m est petit.

4.2.1 L'algorithme de Coleman revisité

Dans le cas de petites valeurs de m on peut tenter d'obtenir un 2-développement de Taylor exact de $F(X)$ de niveau m (cf. 2.4.1). Pour $m \leq 7$, nous écrivons les équations de la variété de dimension 0 correspondante et calculons la 2-dérivée qui lui est attachée en calculant comme dans le cas des développements spéciaux. Enfin nous suivons notre algorithme pour calculer la 2-dérivée de niveau m; les deux méthodes donnent des 2-dérivées comparables. Pour $m > 9$, la méthode de Coleman donne naissance à une variété dont nous ne connaissons pas la non vacuité et les calculs via notre algorithme deviennent vite compliqués.

A. $m = 3$ **i.e.** $g = 1$.

On a donc $F(X+Y) = s_0(Y) + s_1(Y)X + s_2(Y)X^2 + X^3 = (a_0 + a_1X)^2 + b_1X + X^3$ que l'on résout en a_0, a_1, b_1; on a $a_0^2 = s_0(Y)$, $a_1^2 = s_2(Y)$, $b_1 = s_1(Y) \pm 2s_0(Y)^{1/2}s_2(Y)^{1/2}$, ainsi la norme dans un sens évident de b_1 est $N_3(b_1) = s_1(Y)^2 - 4s_0(Y)s_2(Y) = F'^2 - 2FF" = -3Y^4 - 4s_2Y^3 - 6s_1Y^2 - 12s_0Y + s_1^2 - 4s_0s_2 = F'(Y)^2 \mod 2$.

Appliquons l'algorithme: $F(X+Y) = (s_0(Y)^{1/2} + s_2(Y)^{1/2}X)^2 + (s_1(Y) - 2s_0(Y)^{1/2}s_2(Y)^{1/2})X + X^3$; c'est un développement exact; ainsi la 2-dérivée de niveau m est aussi $N_3(F^{[1]}(Y)) = F'^2 - 2FF"$.

Soit y une racine de $N_3(F^{[1]}(Y))$ alors la valuation de Gauss relative au disque $v(X-y) \geq \frac{2}{3}v(2)$ induit une courbe elliptique en réduction. On a potentiellement bonne réduction.

B. $m = 5$ **i.e.** $g = 2$.

On a cette fois $(*)$ $F(X+Y) = s_0(Y) + s_1(Y)X + s_2(Y)X^2 + s_3(Y)X^3 + s_4(Y)X^4 + X^5 = (a_0 + a_1X + a_2X^2)^2 + b_1X + b_3X^3 + X^5$ que l'on résout en a_0, a_1, a_2, b_1, b_3. On a $s_0(Y) = a_0^2$, $s_1(Y) = 2a_0a_1 + b_1$, $s_2(Y) = 2a_0a_2 + a_1^2$, $s_3(Y) = 2a_1a_2 + b_3$, $s_4(Y) = a_2^2$.

On utilise le sytème de calcul Maple:

$b_1 := s1 - 2 * RootOf(t^2 - s0, t) * RootOf(t^2 - (s2 - 2 * RootOf(u^2 - s0, u) * RootOf(u^2 - s4, u)), t)$;
la commande $evala(Norm(b_1))$; donne

$N(b_1) = (-64s_4s_0^3 + 16s_0^2s_2^2 - 8s_0s_2s_1^2 + s_1^4)^2 = ((s_1(Y)^2 - 4s_0(Y)s_2(Y))^2 - 64s_0(Y)^3s_4(Y))^2$.

Appliquons l'algorithme, on a cette fois-ci

$F(X+Y) = (s_0(Y)^{1/2} + s_2(Y)^{1/2}X + s_4(Y)^{1/2}X^2)^2 + (s_1(Y) - 2s_0(Y)^{1/2}s_2(Y)^{1/2})X - 2s_0(Y)^{1/2}s_4(Y)^{1/2}X^2 + (s_3(Y) - 2s_2(Y)^{1/2}s_4(Y)^{1/2})X^3 + X^5$;

ce n'est pas un 2-développement de niveau 5; cependant l'étape suivante modifie le coefficient de X par $-2s_0(Y)^{1/2}(-2s_0(Y)^{1/2}s_4(Y)^{1/2})^{1/2}$. Ainsi la 2-dérivée de niveau 5 est $N_5(F^{[1]}(Y)) = Norm((s_1(Y) - 2s_0(Y)^{1/2}s_2(Y)^{1/2} - 2s_0(Y)^{1/2}(-2s_0(Y)^{1/2}s_4(Y)^{1/2})^{1/2})$ que l'on calcule avec Maple; on obtient

$N_5(F^{[1]}(Y)) := (-3072s_4s_0^4s_2s_1^2 + 4096s_4^2s_0^6 - 2048s_2^2s_4s_0^5 - 128s_4s_0^3s_1^4 + 256s_0^4s_2^4 - 256s_0^3s_2^3s_1^2 + 96s_1^4s_2^2s_0^2 - 16s_1^6s_2s_0 + s_1^8)^2$

Cette norme est très proche du carré de la précédente. Ceci illustre le fait que parmi les 2-développements de niveau donné les spéciaux ne sont pas nécessairement les meilleurs. Dans le cas présent la méthode de Coleman est plus avantageuse.

Le théorème 3.2.2 s'applique au 2-développement $(*)$; ainsi soit $y \in R^{alg}$ une racine de $N(b_1)$ qui résiduellement est racine de $\omega = d\bar{F}/\bar{F}$ ou ce qui revient au même de $\bar{F}'(Y)$ (puisque $p = 2$). En particulier $s_0(y)$ est une unité; on peut supposer que $F^{[1]}(y) = 0$. Suivant le théorème 3.2.2 on calcule

$$(**) \quad v(\rho(y)) = \max(\frac{1}{3}v(\frac{2^2}{b_3(y)}), \frac{1}{5}v(2^2)).$$

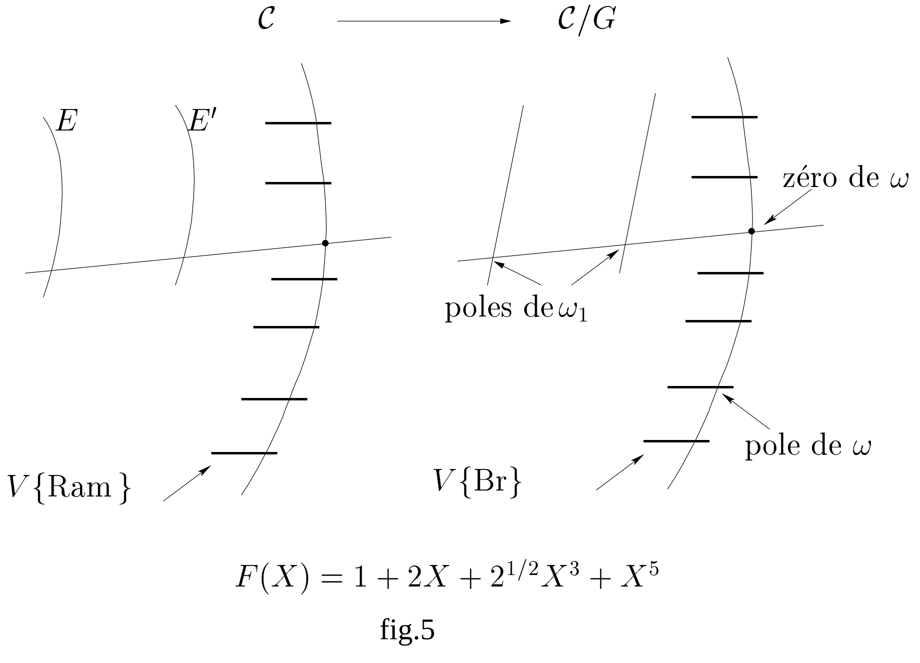
On distingue alors 3 cas de figure:

1.— $\bar{F}'(Y)$ **a un seul zéro qui est d'ordre** 4 **et** C **a potentiellement bonne réduction.** Ce cas se produit si et seulement si l'égalité dans la formule (**) est réalisée pour $j = 5$ i.e. $v(\rho) = \frac{1}{5}v(2^2)$. Par exemple c'est le cas pour $F(X) = 1 + X^5$ (évident) ou pour $F(X) = 1 + 2X + X^5$ et dans ce n'est pas évident (on peut vérifier que c'est bien le cas en calculant les invariants d'Igusa avec l'algorithme de Liu, cf. [Li 2]). On calcule $N(b_1(Y)) = 625 * Y^{16} + 1000 * Y^{12} - 2000 * Y^{11} + 600 * Y^8 - 1600 * Y^7 + 1600 * Y^6 + 160 * Y^4 - 320 * Y^3 - 320 * Y + 16$, un algorithme utilisant le système de calcul PARI montre que ses racines y_i satisfont à $\inf v(y_i - y_j) = (2/5)v(2)$. On a donc potentielle bonne réduction.

2.— $\bar{F}'(Y)$ **a un seul zéro qui est d'ordre** 4 **et** C **n'a pas potentiellement bonne réduction.** L'existence d'une telle configuration (cf. fig. 5) est garantie par le recollement formel dès que les conditions différentielles évoquées en 3.2.4 sont satisfaites: dans la figure 5 considérons la composante $\mathbb{P}^1_k$ horizontale; le torseur dégénère en $\boldsymbol{\alpha}_2$ sur cette composante et les 2 courbes elliptiques E et E' intersectent cette droite en deux points p et p' qui correspondent aux zéros de la forme différentielle additive $\omega_1 = t^2(1+t)^2dt$ dont le pôle est le point d'intersection avec la composante initiale.

Ce cas de figure se produit par exemple pour $F(X) = 1+2^{1/2}X^3+X^5$ puisque le changement $X = 2^{1/2}T$ induit une composante de genre 1. D'autre part le changement $X = 2^{1/4}T$ donne $Z^2 = 1 + 2^{5/4}(T^3 + T^5)$ qui induit un $\boldsymbol{\alpha}_2$ torseur $Z^2 = t^3 + t^5 := f$ et $df = t^2(1 + t)^2dt$. La détermination de l'autre composante de genre 1 nécessite l'algorithme: on calcule $N(b_1(Y)) = -95Y^{16} - 300*2^{1/2}*Y^{14} - 772*Y^{12} + 240*Y^{11} - 376*2^{1/2}*Y^{10} + 200*2^{1/2}*Y^9 + 36*Y^8 - 384*Y^7 + 640*Y^6 + 144*2^{1/2}*Y^5 + 288*Y^2 - 320*Y = Y^{16} + 4*2^{1/2}*Y^{14} + 4*Y^{12} + 4*Y^8 \mod 2^3$; ainsi si y est une racine de valuation $(1/4)v(2)$, puisque $b_3(y) = 2^{1/2} \mod 2$, il suit que le changement $X = y + \rho T$ avec $v(\rho) = (1/2)v(2)$ induit la deuxième composante de genre 1.

Considérons maintenant le cas de $F(X) = 1 + 2X + 2^{1/2}X^3 + X^5$. Contrairement au cas précédent il n'y a pas de zéro évident pour $N(b_1(Y)) = (625 * Y^{16} + 1500 * 2^{1/2} * Y^{14} + 3700 * Y^{12} - 2000 * Y^{11} + 2880 * 2^{1/2} * Y^{10} - 3000 * 2^{1/2} * Y^9 + 3084 * Y^8 - 4480 * Y^7 + (1600 + 1152 * 2^{1/2}) * Y^6 - 1872 * 2^{1/2} * Y^5 + (592 + 960 * 2^{1/2}) * Y^4 - 896 * Y^3 + (288 + 96 * 2^{1/2}) * Y^2 + (-320 - 96 * 2^{1/2}) * Y + 16)^2$ cependant l'analyse du polygone de Newton montre que les racines du polynôme sont de valuation $\frac{1}{4}v(2)$ et se répartissent en 2 classes modulo $2^{1/4}$; ainsi on peut trouver 2 racines y_1 et y_2 avec $v(y_1 - y_2) = v(y_1) = \frac{1}{4}v(2) < \frac{2}{5}v(2)$ ce qui contredit le critère de bonne réduction (cf. Th. 3.3.1).



$F(X) = 1 + 2X + 2^{1/2}X^3 + X^5$

fig.5

3.— $\bar{F}'(Y)$ **a deux zéros qui sont d'ordre** 2. On trouve 2 composantes de genre 1 mais contrairement au cas précédent c'est la configuration générique (cf. fig. 4).

C. $m = 7$ **i.e.** $g = 3$.

On distingue alors 6 cas de figure qui sont numérotés en fonction de la géométrie différentielle sous-jacente en respectant l'application de spécialisation dans un certain espace de modules. Par exemple Δ_0 correspond au cas où la forme différentielle logarithmique ω a 3 zéros de multiplicité 2 (c'est le cas général vu en 4.1). Les cas $\Delta_{01?}$ correspondent au cas où la forme différentielle logarithmique ω a 2 zéros dont l'un est de multiplicité 2 et l'autre de multiplicité 4. Dans le cas général on est dans la situation Δ_{010} qui correspond au cas où la forme différentielle additive sur la droite projective sur laquelle s'appuient les 2 courbes elliptiques a 2 poles d'ordre 2; ce cas lui-même se spécialisant dans Δ_{011}.

On peut verifier que les conditions différentielles sont réalisables et donc via le recollement formel on peut construire des exemples correspondant à chacune des 6 situations (cf. fig. 6). Nous allons donner un exemple numérique sous la forme d'une équation globale $Z^2 = F(X)$ dans chacun des cas. Comme dans le cas du genre 1 on se simplifie la vie en choisissant un exemple pour lequel une valuation qui induit une composante de genre non nul correspond à un disque fermé centré en $X = 0$; on a ainsi $Y = 0$ qui est un zéro évident de la 2-dérivée de niveau 7.

On applique la méthode de Coleman; cette fois

$F(X+Y) = s_0(Y) + s_1(Y)X + s_2(Y)X^2 + s_3(Y)X^3 + s_4(Y)X^4 + s_5(Y)X^5 + s_6(Y)X^6 + X^7 = (a_0 + a_1X + a_2X^2 + a_3X^3)^2 + b_1X + b_3X^3 + b_5X^5 + X^7$

que l'on résout en $a_0, a_1, a_2, a_3, b_1, b_3, b_5$. On a

$$\begin{aligned} s_0(Y) &= a_0^2 \\ s_1(Y) &= 2a_0a_1 + b_1 \\ s_2(Y) &= 2a_0a_2 + a_1^2 \\ s_3(Y) &= 2a_0a_3 + 2a_1a_2 + b_3 \\ s_4(Y) &= 2a_1a_3 + a_2^2 \\ s_5(Y) &= 2a_2a_3 + b_5 \\ s_6(Y) &= a_3^2. \end{aligned}$$

En utilisant le système de calcul Maple on obtient

$N(b_1) := (-4096*s0^5*s1^2*s6+256*s0^4*s2^4-2048*s0^5*s2^2*s4-256*s0^3*s1^2*s2^3+96*s0^2*s1^4*s2^2+4096*s0^6*s4^2+1024*s0^4*s1^2*s2*s4-128*s0^3*s1^4*s4-16*s0*s1^6*s2+s1^8)^2$

Nous utilisons l'algorithme pour exhiber $N_7(F^{[1]}(Y))$, la 2-dérivée de niveau 7. Suivant le même principe que pour $m = 5$, après 2 étapes on obtient comme coefficient de X; $s_1(Y) - 2*s_0(Y)^{1/2}*s_2(Y)^{1/2} - 2*(-2)^{1/2}*s_0(Y)^{1/4}*s_4(Y)^{1/4}$; l'étape suivante le modifie par un terme de taille $2^{1+1/2+1/4}$ et puisque $1+1/2+1/4+2/7 > 2$ on peut le négliger pour exprimer la 2-dérivé de niveau 7; ainsi

$N_7(F^{[1]}(Y)) = (4096*s0^6*s4^2-128*s0^3*s1^4*s4-3072*s0^4*s1^2*s2*s4-2048*s0^5*s2^2*s4+s1^8-16*s0*s1^6*s2+96*s0^2*s1^4*s2^2-256*s0^3*s1^2*s2^3+256*s0^4*s2^4)^8$
les radicaux de $N(b_1)$ et $N_7(F^{[1]}(Y))$ sont de degré 48 en Y et sont égaux modulo 2^{12}.

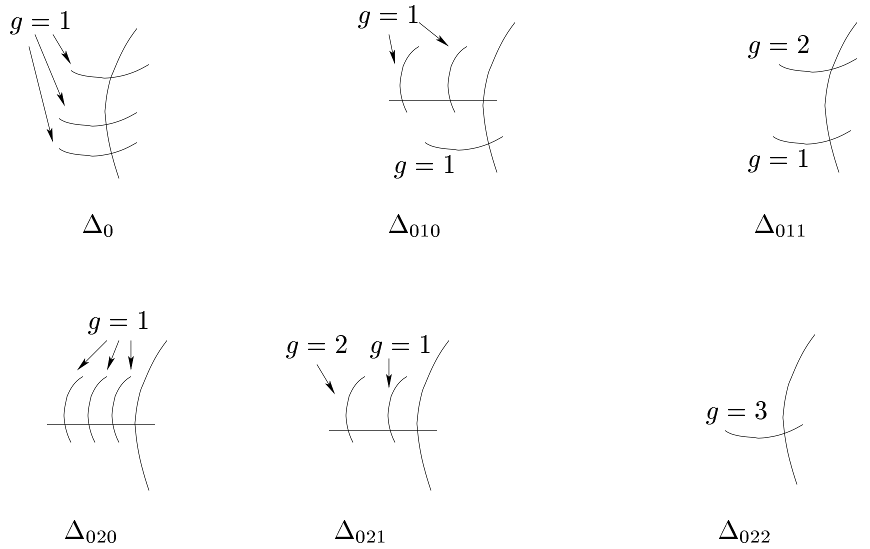


fig.6

1.— Δ_0

On prend $F(X) = 1 + X^3 + X^5 + X^7$; alors $\bar{F}'(X) = (X + X^2 + X^3)^2$ et $X + X^2 + X^3$ a trois racines simples. C'est la situation générale. On calcule $N := N_7(F^{[1]}(Y))$ d'où les congruences $\mathrm{rem}(N, y^9, y) \mod 2^{11} = 1024{*}y^6{+}256{*}y^7{+}256{*}y^4$ et $N\ mod2 = y^{32}{+}y^{16}{+}y^{48}$; les racines sont regroupées dans 3 classes modulo 2 et si y est une racine on a $F^{[3]}(y) = 1{+}y^4$ mod 2 ainsi $v(F^{[3]}(y)) = 0$ et le changement $X = y + 2^{2/3}T$ induit une courbe de genre 1.

2.— Δ_{010}

On part du polynôme $\bar{F}(X) = 1 + X^5 + X^7$ dont la différentielle $X^4(1 + X)^2 dX$ a 2 zéros d'ordre respectifs 4 et 2; on va montrer que $F(X) = 1{+}2^{1/2}X^3{+}X^5{+}X^7$ convient. Remarquons que le changement $X = 2^{1/4}T$ induit une equation $Z^2 = 1 + 2^{5/4}(T^3 + T^5) + 2^{7/4}T^7$ qui induit un $\boldsymbol{\alpha}_2$-torseur $y^2 = t^3 + t^5 := f$ et $df = (t + t^2)^2 dt$ a 2 racines doubles; on trouve (certainement) ainsi la composante qui croise les 2 courbes elliptiques. Pour confirmer cela, on calcule la 7-dérivée $N := N_7(F^{[1]}(Y))$ et on analyse son polygone de Newton, quelques congruences permettent de conclure: $N = Y^{32} + Y^{48} \mod 2$, $\mathrm{rem}(N, Y^3, Y) \mod 2^{13} = 4096{*}Y^2$, $\mathrm{rem}(N, Y^{17}, Y) \mod 2^5 = 16{*}Y^{16}$; ainsi il y a 16 racines de valuation $\geq (4/7)v(2)$; 16 autres de valuation $(1/4)v(2)$ et enfin les 16 autres de valuation nulle. Le premier lot correspond à la valuation sur le disque $v(X - y) \geq 1/2$ qui induit une courbe elliptique (notez que $(4/7)v(2) > (1/2)v(2)$).

3.— Δ_{011}

On prend $F(X) = 1 + X^5 + X^7$; alors $(\bar{F}(X))' = X^4(1 + X)^2$. Le changement $X = 2^{2/5}T$ induit en réduction une composante de genre 2. On calcule $N := N_7(F^{[1]}(Y)) = Y^{48} + Y^{32}$ mod 2; puisque $F^{[3]}(Y) = Y^4 \mod 2$; il suit que la composante de genre 1 est induite par le changement $X = y + \rho T$ où $y = 1 \mod 2$ est racine de $N_7(F^{[1]}(Y))$ et $v(\rho(y)) = (2/3)v(2)$.

4.— Δ_{020}

On va montrer que $F(X) = 1 + 2X^3 + 2^{1/2}X^5 + X^7$ convient. Notons que $(\bar{F}(X))' = X^6$ et que le changement $X = 2^{2/3}T$ induit en réduction une composante de genre 1; enfin le changement $X = 2^{1/4}T$ induit une équation $Z^2 = 1 + 2^{7/4}(T^3 + T^5 + T^7)$ et donc un $\boldsymbol{\alpha}_2$-torseur $y^2 = t^3 + t^5 + t^7 := f$ et puisque $df = t^2(1 + t + t^2)^2 dt$ on prévoit que l'on a là la composante qui supporte les 3 composantes elliptiques: prouvons cela. On calcule la 7-dérivée $N := N_7(F^{[1]}(Y))$ et on analyse son polygone de Newton, quelques congruences permettent de conclure: $N = y^{48} \mod 2$, $\mathrm{rem}(N, y^{33}, y) = 16 * y^{32} \mod 2^5$, $\mathrm{rem}(N, y^3, y) = 8192 * y^2 \mod 2^{14}$, $\mathrm{rem}(N, y^{17}, y) = 256 * y^{16} \mod 2^9$. Il suit que les racines se répartissent en 16 de valuation $\geq 5/14$ puis 16+16 en 2 classes modulo $2^{1/4}$.

5.— Δ_{021}
On prend $F(X) = 1 + 2^{1/2}X^5 + X^7$; alors $(\bar{F}(X))' = X^6$. Le changement $X = 2^{3/10}T$ induit en réduction une composante de genre 2. Le changement $X = 2^{1/4}T$ induit une équation $Z^2 = 1 + 2^{7/4}(T^5 + T^7)$ et donc un $\boldsymbol{\alpha}_2$-torseur $y^2 = t^5 + t^7 := f$ et puisque $df = t^4(1+t)^2dt$; comme précédemment on vérifie que l'on a ainsi la composante qui supporte les 2 composantes de genre respectif 1 et 2.

6.— Δ_{022}
$F(X) = 1 + X^7$ convient!

4.2.2 Illustrations dans le cas $p > 2$.

A. **Un exemple instructif.**

Dans cet exemple $p = 3$, $F(X) = 1 + cX^3 + X^4$; pour $c \in R$. Notons que le discriminant $\mathrm{Disc}\, F(X) = 256 - 27c^4 = 1 \mod 3$; ainsi la géométrie du lieu de branchement est équidistante. Dans ce cas nous avons $m - 1 = p$ et nous allons voir que le critère de bonne réduction de [Le 2] est insuffisant (cf. th. 3.3.2). Nous remarquons que $F'(X) = X^2(3c + 4X)$; suivant le théorème 3.3.2, si la courbe $Y^3 = F(X)$ a bonne réduction il existe $d \in R$ tel que

$$N(X) := \frac{1}{4}F'(X) = (X - d)^3 \mod \lambda^{3/4}$$

Comme $3 \cong \lambda^2$ il suit que la condition de [Le 2] est équivalente à $d^3 = 0 \mod \lambda^{3/4}$ et donc $d = 0 \mod \lambda^{1/4}$. On doit donc tester si il y a bonne réduction pour $\frac{\lambda^{3/4}}{X - \lambda^{1/4}d}$ où d parcourt $R/(\lambda^{1/2})$.

Appliquons l'algorithme.

$$F(X + Y) = 1 + cY^3 + Y^4 + (3cY^2 + 4Y^3)X + (3cY + 6Y^2)X^2 + (c + 4Y)X^3 + X^4$$

la 3-dérivée de niveau 4 vaut

$N_4(F^{[1]}(Y)) = -3^3 s_0(Y)^2 s_3(Y) + s_1(Y)^3 = -44Y^9 - 99cY^8 - 54c^2Y^7 - 216Y^5 - 270cY^4 - 54c^2Y^3 - 108Y - 27c$

Soit $y = d \in R^{alg}$ une racine de $N_4(F^{[1]}(Y)$, alors $v(d) > 0$ et donc $s_0(y)$ est une unité. Alors $F(X + d) = (s_0(y)^{1/3} + s_3(y)^{1/3}X)^3 + (-3s_0(y)^{2/3}s_3(y)^{1/3} + s_1(y))X + (-3s_0(y)^{1/3}s_3(y)^{2/3} + s_2(y))X^2 + X^4 = (s_0(y)^{1/3} + s_3(y)^{1/3}X)^3 + (-3s_0(y)^{1/3}s_3(y)^{2/3} + s_2(y))X^2 + X^4$.

Notons que $s_2(y) = (3cd + 6d^2)$ est divisible par 3; il suit que l'on a bonne réduction pour $X = d + \lambda^{3/4}T$.

///

B. **Des limites de l'algorithme.**

Dans [Ma], on montre que pour $a_1, a_2, ..., a_n \in \mathbb{Z}_2^{nr}$ suffisament généraux et

$$F(X) := \prod_{(\epsilon_1,..,\epsilon_n)\in\{0,1\}^n} (1 + (\sum_{1\leq i\leq n} \epsilon_i a_i)^2 X)$$

il existe $b_0, b_1, ..., b_{n-1} \in \mathbb{Z}_2^{nr}$ tels que

$$F(X) = (1 + \sum_{1\leq i\leq n-1} b_i X^{2^{n-1}-2^{i-1}})^2 + b_0^2 X^{2^n - 1} \mod 4\mathbb{Z}_2^{nr}.$$

Cette dernière congruence fournit un 2-développement de Taylor en $Y = 0$ de $F(X)$ à l'ordre $m = 2^n - 1$ et de niveau quelconque (cf. Déf. 2.4.1).

Soit $R := \mathbb{Z}_2^{nr}[\pi]$ avec $\pi^{2^n-1} = 2^2$, alors l'équation $Z^2 = F(X)$ définit une courbe hyperelliptique ayant bonne réduction sur R relativement à la valuation de Gauss en $S := (2)^{-2/(2^n-1)}X$ avec $m = 2^n - 1$.

Il doit être clair dans l'esprit du lecteur que l'algorithme proposé dans cette note ne permet pas de montrer la congruence qui précède.

5 Réduction stable des revêtements p-cycliques d'une courbe de genre > 0 qui a bonne réduction en p; cas d'un lieu de branchement à géométrie équidistante.

On considère un revêtement p-cyclique $C \to D := C/G$ tel que la courbe quotient D admet un modèle lisse $\mathcal{D}'$ et que le lieu de branchement Br se spécialise en des points distincts $\bar{\mathrm{Br}} \subset \mathcal{D}'_s$. Dans ce cadre, le lemme 3.2.1 se généralise en:

Lemme 5.0.1 .— *Après extension finie de K, le modèle $\mathcal{C}'$ de C, obtenu par normalisation du modèle lisse $\mathcal{D}'$ de D a une fibre spéciale réduite qui est un revêtement radiciel de $\mathcal{D}'_s$; les singularités sont des cusps et se trouvent au-dessus des zéros $\in \mathcal{D}'_s$ d'une forme différentielle logarithmique ω régulière en dehors de* $\bar{\mathrm{Br}}$. *Le graphe d'intersection de la fibre spéciale $\mathcal{C}_s$ du modèle stable $\mathcal{C}$ de la courbe marquée* (C, Br) *est un arbre (il n'y a pas de cycles) et le modèle $\mathcal{D}$ de D obtenu par quotient de l'action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathcal{C}$ a une fibre spéciale qui est un arbre de droites projectives attachées à $\mathcal{D}'_s$ dans les zéros de ω.*

Commentaires. C'est un cas particulier du théorème 1' de Raynaud dans ([Ra 1]. Considérons l'anneau local de $\mathcal{D}'$ au point générique de la fibre spéciale; c'est un anneau de valuation discrète; soit v la valuation correspondante. Soit $\mathcal{C}'$, le modèle de C, obtenu par normalisation du modèle lisse $\mathcal{D}'$ de D. Par [Ep], après une extension finie de K, on peut supposer que la fibre spéciale de $\mathcal{C}'$ est réduite.

Nous allons voir qu'elle est intègre et que le $\boldsymbol{\mu}_p$-torseur au-dessus de $D - \mathrm{Br}$ induit un $\boldsymbol{\mu}_p$-torseur au-dessus de $\mathcal{D}'_s - \bar{\mathrm{Br}}$.

Une équation du revêtement est $Z^p = F \in K(D)$ où $v(F) = 0$; alors F définit un diviseur principal de la R-courbe $\mathcal{D}'$, $(F) := \sum_{1 \le i \le m+1} e_i V(\{x_i\}) + p(D_0)$ où $\mathrm{Br} = \{x_i, 1 \le i \le m+1\}$ et $V(\{x_i\})$ désigne la fermeture schématique de $\{x_i\}$, enfin $e_i \in \mathbb{N}$ avec $(e_i, p) = 1$ et (D_0) est un diviseur horizontal. On a donc modulo π; $(\bar{F}) = \sum_{1 \le i \le m+1} e_i \bar{x}_i + p(D_{0s})$ (cf. [Li 1] Lemma 7.1.29); ainsi $\bar{F}$ n'est pas une puissance p-ième dans $k(\mathcal{D}'_s)$ et donc l'équation $\bar{Z}^p = \bar{F} \in k(\mathcal{D}'_s)$ définit un $\boldsymbol{\mu}_p$-torseur au-dessus de $\mathcal{D}'_s - \bar{\mathrm{Br}}$. La forme différentielle logarithmique $\omega := d\bar{F}/\bar{F}$ est une forme différentielle sur $\mathcal{D}'_s$ (indépendante de F) qui est régulière en dehors de $\bar{\mathrm{Br}}$; c'est la forme différentielle associée au torseur.

La fibre spéciale $\mathcal{C}'_s$ est alors homéomorphe à $\mathcal{D}'_s$ et puisque le diviseur de $\bar{F}$ a une multiplicité en $\bar{x}_1$ première à p; une modification de l'équation du torseur va donner la multiplicité 1 et induire un modèle lisse en $\bar{x}_1$. Ainsi les singularités de la courbe $\mathcal{C}'_s$ sont des cusps situés dans les zéros de ω et en dehors des $\bar{x}_i$.

Si x est un zéro de ω, après localisation en x on se retrouve dans la situation locale décrite par Raynaud dans ([Ra 1], démonstration du théorème 1 p. 182)), le lemme suit. ///

Le théorème 3.2.2 a une généralisation que nous décrivons brièvement.

Soit $\bar{d} \in \mathcal{D}'_s$, un zéro de ω d'ordre $m(\bar{d}) - 1$. Une équation du torseur au-dessus de la fibre formelle en $\bar{d}$ est $Z^p = F(X) \in R[[X]]$; où $F(X)$ est une unité modulo π. Dans le séparé complété du module de différentielle $\Omega_{R[[X]]/R}$ on a alors l'égalité $d\bar{F}/\bar{F} = u(X)X^{m(\bar{d})-1}dX \mod \pi$ où $u(X)$ est une unité modulo π . Comme dans le cas des polynômes, on fait un p-développement de Taylor spécial à l'ordre $m(\bar{d})$ et de niveau n avec $p^n < m(\bar{d}) < p^{n+1}$ (cf. 2.4.1),

$$F(X+Y) = E(X,Y)^p + \sum_{1 \leq j \leq m(\bar{d}),\ (j,p)=1} F^{[j]}(Y)X^j \mod (p^{c_n}X, X^{m(\bar{d})+1})$$

où $E(X,Y) \in (R[[Y]])^{alg}[X]$, $\deg_X E(X,Y) = [m(\bar{d})/p]$ et $F^{[j]}(Y) \in (R[[Y]])^{alg}$ (notez que la congruence impose l'égalité $E(0,Y)^p = F(Y)$). De manière analogue à 2.4.1, on définit la p-dérivée de niveau m,

$$N_{m(\bar{d})}(F^{[1]}(Y)) := N_{L_n/K(Y)}(F^{[1]}(Y)) \in R[[Y]].$$

Par le théorème de préparation de Weierstrass $N_{m(\bar{d})}(F^{[1]}(Y)) = P_{m(\bar{d})}(Y)U_{m(\bar{d})}(Y)$ où $P_{m(\bar{d})}(Y) \in R[Y]$ est un polynôme distingué, $P_{m(\bar{d})}(Y) = Y^{(m(\bar{d})-1)p^{r(m(\bar{d}))}} \mod \pi$, et $U_{m(\bar{d})}(Y) \in R[[Y]]$ est une unité. Les zéros de $P_{m(\bar{d})}(Y)$ donnent des centres des disques fermés de la droite projective qui induisent une composante de genre non nul dans la fibre spéciale $\mathcal{C}_s$ du modèle stable $\mathcal{C}$ de la courbe marquée (C, Br) au-dessus du zéro $\bar{d} \in \mathcal{D}_s$ de ω.

Si D n'est pas la droite projective, il y a plusieurs obstacles pour rendre les calculs locaux précédents algorithmiques.

References

[Ab] A. Abbes, *Réduction semi-stable des courbes d'après Artin, Deligne, Grothendieck, Mumford, Saito, Winters, ...*, Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998), Progr. Math., **187** (2000) Birkhäuser, 59–110.

[Co] R. F. Coleman, *Computing stable reductions*, Séminaire de Théorie des Nombres, Paris 1985–86, Progress in Mathematics **71** (1987), Birkhäuser, 1–18.

[Co-Ca] R. F. Coleman, W. McCallum, *Stable reduction of Fermat curves and Jacobi sum Hecke characters*, J. reine angew. Math. **385** (1988), 41–101.

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

[Gr-Ma] 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.

[He] Y. Henrio, *Arbres de Hurwitz et automorphismes d'ordre p des disques et des couronnes p-adiques formels* , Compositio Mathematica, to appear.

[Le 1] C. Lehr, *Reduction of wildly ramified covers of curves*, Thèse University of Pennsylvania, (2001).

[Le 2] C. Lehr, *Reduction of p-cyclic Covers of the Projective Line*, Manuscripta Math. 106 (2001) 2, 151-175.

[Li 1] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics, 6 (2002), Oxford University Press.

[Li 2] Q. Liu, *Courbes stables de genre 2 et leur schéma de modules*, Mathematische Annalen 295 (1993), 201-222.

[Ma] M. Matignon, *p-groupes abéliens de type $(p, \cdots, p)$ et disques ouverts p-adiques*, Manuscripta Math. 99 (1999), no. 1, 93–109.

[Mi] J. S. Milne, *Étale Cohomology*, Princeton Mathematical Series, **33**, (1980).

[Ra 1] M. Raynaud, *p-groupes et réduction semi-stable des courbes*, The Grothendieck Festschrift, Vol III, Progress in Mathematics **88** (1990), Birkhäuser, 179–197.

[Ra 2] M. Raynaud, Mauvaise réduction des courbes et p-rang, C.R. Acad. Sci. Paris, 316, Série I, (1994), 1279–1282.

[Sa 1] M. Saïdi, *Galois covers of degree p: semi-stable reduction and Galois action*, math.AG/0106249.

[Sa 2] M. Saïdi, *Wild ramification and a vanishing cycles formula*, math.AG/0106248.

[Sa 3] M. Saïdi, *Torsors under finite and flat group schemes of rank p with Galois action*, math.AG/0106246.

Michel MATIGNON
Laboratoire de Théorie des Nombres et d'Algorithmique Arithmétique, UMR 5465 CNRS
Université de Bordeaux I, 351 cours de la Libération, 33405 Talence Cedex, France
e-mail : `matignon@math.u-bordeaux.fr`