Wild monodromy and automorphisms of curves *

Claus Lehr and Michel Matignon

0 Introduction

These proceedings notes are mainly inspired by a joint work in progress with C. Lehr [Le-Ma]. They reproduce the text of the conference given by Michel Matignon on the 28-08-02. For a complete presentation of motivations and references we refer to [Le 1,2] and [Ma].

Let us fix the notations for the introduction.

$K/\mathbb{Q}_l^{nr}$ is a finite extension, v the K valuation, O_K the valuation ring and π a uniformizing parameter for K.

Note that the residue ring $k := \frac{O_K}{\pi O_K} = \mathbb{F}_l^{alg}$.

Consider the 2-cyclic cover of $\mathbb{P}^1_K$, the projective line over K

$$(*) \quad C: \quad Z^2 = X(X-1)(X-\rho) = F(X) \in O_K[X]$$

where $\rho \notin \{0,1\}$.

We consider the

Problem. Reduction of C mod (π)

Case A. $l \neq 2$

We assume that $v(\rho) = v(\rho - 1) = 0$, i.e. the branch locus has equidistant geometry.

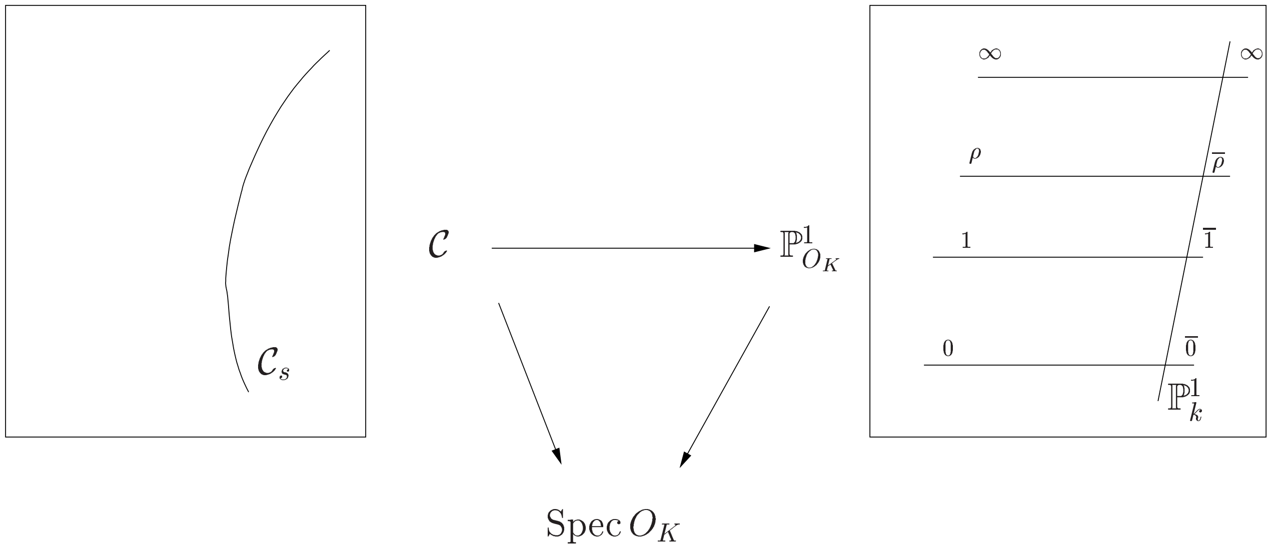


Fig.1

*The second author thanks the organizors T. Sekiguchi and N. Suwa for inviting him to give a talk and the nice atmosphere during his visit to Tokyo

$\mathcal{C}$ is the integral closure of $\mathbb{P}^1_{O_K}$ in $K(X,Z)$

$\mathcal{C}_s := \mathcal{C} \times_{O_K} \mathbb{F}_l^{alg}$: $\quad z^2 = x(x-\bar{1})(x-\bar{\rho})$ is a smooth genus 1 curve; we say that C has good reduction at l over K.

Twisted form: here (*) is replaced by

$$(**) \quad \pi Z^2 = X(X-1)(X-\rho)$$

Set $L := K(\sqrt{\pi})$. Replace Z by $\sqrt{\pi}Z$, then (**) gives again (*) but this time over L; we say that C has potentially good reduction at l over K. Moreover L is the minimal extension of K such that $C \times L$ has good reduction over L. We say that $\mathrm{Gal}(L/K)$ is the finite monodromy.

Note that there is an induced homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Aut}_k\mathcal{C}_s$ which assigns to the automorphism $\sqrt{\pi} \to -\sqrt{\pi}$, the hyperelliptic involution.

Case B. $l = 2$.

$$(*) C : \quad Z^2 = X(X-1)(X-\rho) = F(X) \in O_K[X]$$

where $K = \mathbb{Q}_2^{nr}(\rho)$

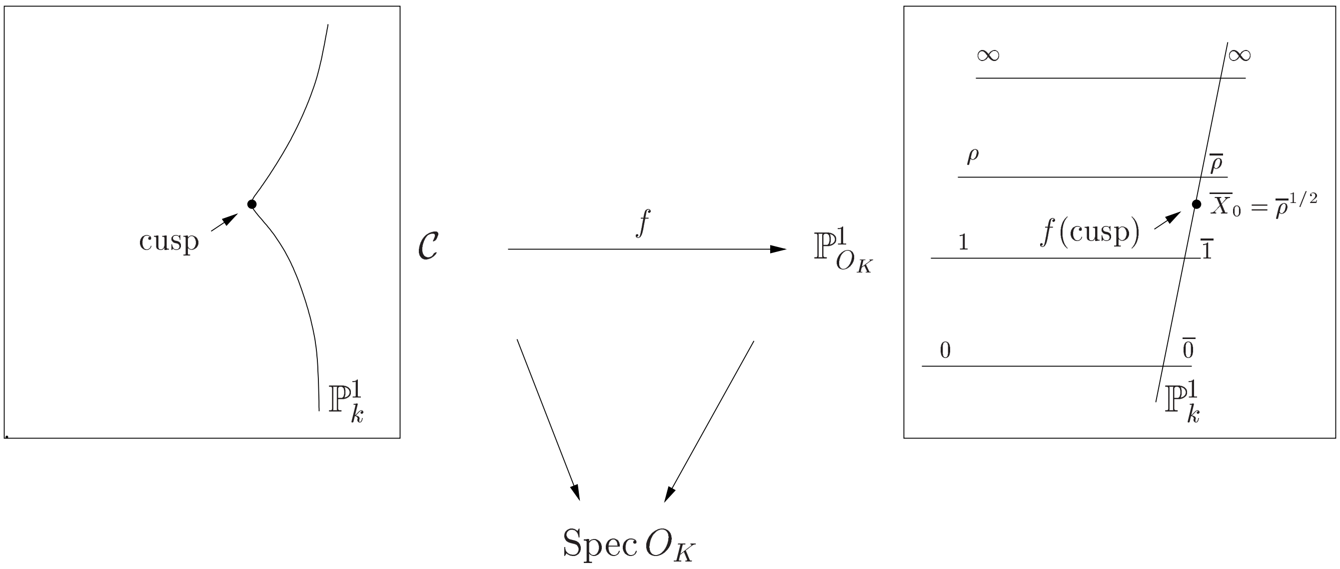


Fig.2

The jacobian criterium says that $\bar{X}_0 = \bar{\rho}^{1/2}$ is a root of $\bar{F}'(X)$ and the residual local equation at $\bar{X}_0$ is $z^2 = s_0(x-\bar{X}_0)^2 + (x-\bar{X}_0)^3$ which is the equation of a cusp.

Now we apply Deuring's desingularisation method. Write

$$F(X+Y) = s_0(Y) + s_1(Y)X + s_2(Y)X^2 + X^3$$

We look for a Y such that $F(X+Y) = (...)^2 + X^3$. Consider $\Delta := s_1^2 - 4s_0s_2 = (Y - \bar{\rho}^{1/2})^4$ mod 2

Let $Y := Y_0$ be a root of Δ then

$$Z^2 = F(X+Y_0) = (F(Y_0)^{1/2} + s_0(Y_0)^{1/2}X)^2 + X^3$$

Let $E := F(Y_0)^{1/2} + s_0(Y_0)^{1/2}X$, $Z = 2W + E$ and $X = 2^{4/3}T$ then,

$Z^2 + EZ = T^3$ over $L := K(Y_0, 2^{4/3}, F(Y_0)^{1/2}$ so

$$z^2 + F(\bar{Y}_0)^{1/2}z = t^3$$

and so C_s is the unique supersingular elliptic curve in Θ.

Geometrically: blowing along ideal $(2^{4/3}, X - Y_0)$; we get

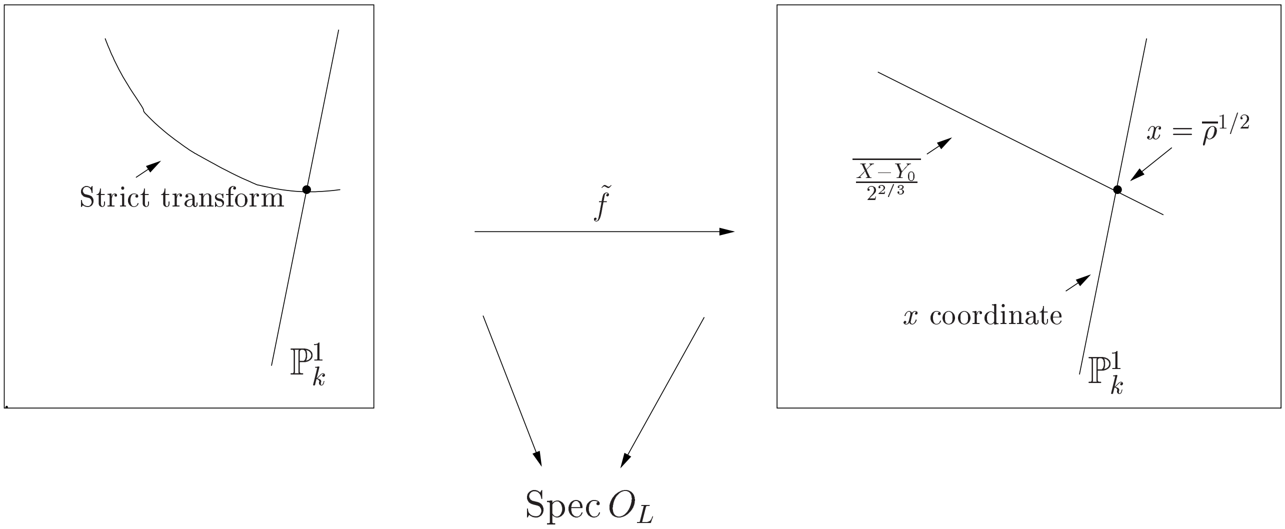


Fig.3

Note that the automorphism group $\operatorname{Aut} C_s$ has a unique 2-Sylow subgroup that we call the wild automorphism group $(\operatorname{Aut} C_s)_w \simeq H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, the quaternion group.

1 (Potentially) good reduction, finite wild monodromy.

Let p be any prime, $K/\mathbb{Q}_p^{nr}$ a finite extension and $\lambda = \zeta_p - 1$ where ζ is a primitive root of 1.

Let C be a projective smooth curve over K given by the following Kummer equation

$$(*)C : \ Z^p = F(X) = \prod_{1 \leq 1 \leq m} (X - X_i)^{e_i}$$

where $X_i \in K$, $(e_i, p) = 1$, $(\sum e_i, p) = 1$ so the branch locus is $\mathrm{Br} := \{X_1, ..., X_m, \infty\}$.

Moreover we will assume that Br has the equidistant geometry i.e. $v(X_i) = v(X_i - X_j) = 0$.

Note that the case $p = 2$ correspond to hyperelliptic curves and the introduction presents the case $m = 3$ i.e. the elliptic case.

We shall assume that $g(C) \geq 1$. We look for a criterium for potentially good reduction over K.

Définition 1.1 .— We say the curve C has good reduction over K if there is $\mathcal{C}/O_K$ a projective smooth relative curve such that $\mathcal{C} \times K \simeq C$ and if $\mathcal{C} \times k$ is smooth.

Définition 1.2 .— We say the curve C has potentially good reduction over K if there is L/K a finite extension such that $\mathcal{C} \times L$ has good reduction over L.

The following theorem is the key ingredient in order to get information on the monodromy. A modern reference is Liu's book [Li], chapter 10, especially theorem 4.44.

Théorème 1.3 .— *Assume that C has potentially good reduction over K. There is a minimal extension L/K such that $C \times L$ has good reduction over L; moreover L/K is Galois. The Galois group* $\operatorname{Gal}(L/K)$ *is called the finite monodromy group; its unique p-Sylow subgroup* $\operatorname{Gal}(L/K)_w$ *is called the wild monodromy group.*

The base change L/K induces an into homomorphism

$$\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}_{\,k} C_s$$

where C_s is the special fiber. Moreover if $q \in C(K)$ and if $\bar{q} \in C_s$ is its specialisation then the above homomorphism goes into the decomposition group $G_{0,\bar{q}}$ at $q \in C_s$ and $\mathrm{Gal}(L/K) \hookrightarrow G_{1,\bar{q}}$, where $G_{1,\bar{q}}$ is the wild ramification group at $\bar{q}$.

We can apply this to our situation. Let C be defined by (*) and q the K rational point ($X = \infty, Z = \infty$) on C.

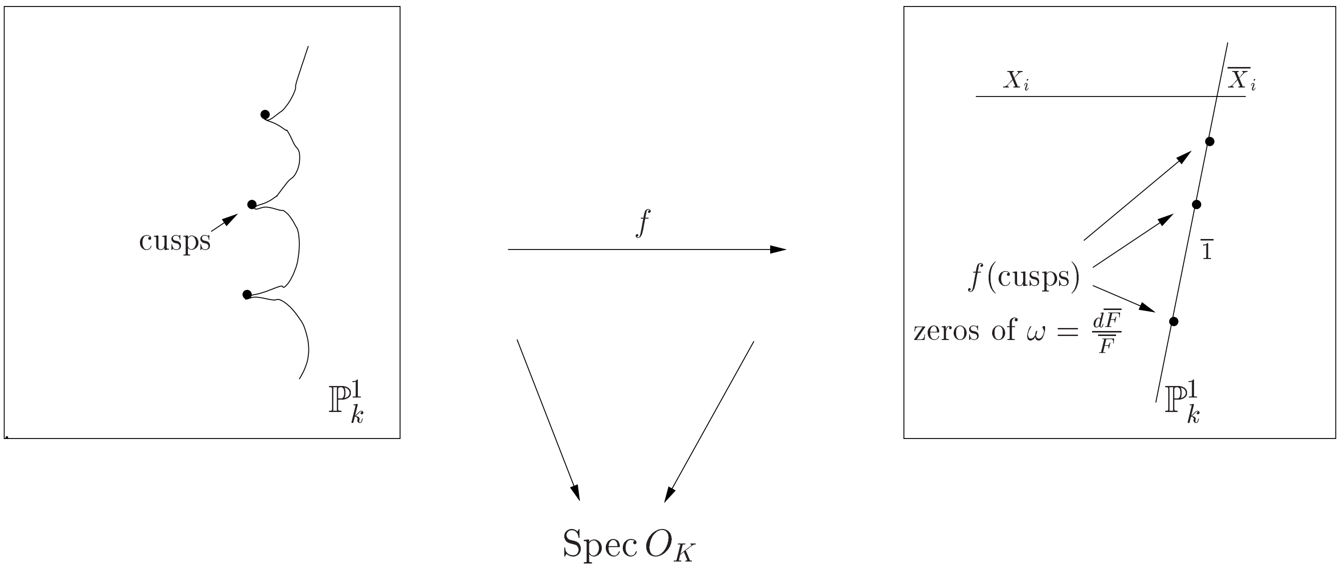


Fig.4

We have the following criterium for good reduction ([Le],[Ma]) illustrated in figure 5.

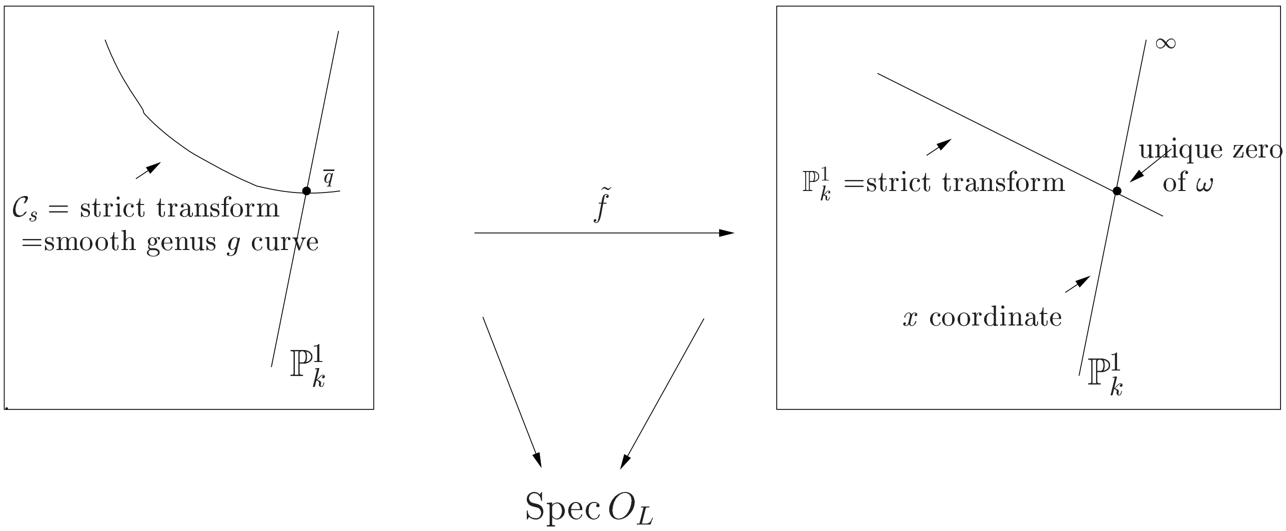


Fig.5

Proposition 1.4 .— *The curve C has potentially good reduction iff*

i) $\omega = \frac{dF}{F}$ has only one zero (order is necessarily $m-1$)

ii) The blowing up along the ideal $(\lambda^{p/m}, X - Y_0)$

Problem. Find $Y_0 \mod \lambda^{p/m}$
The Clue. $Gal(L/K)_w \hookrightarrow G_{1,\infty=\bar{q}}$

2 Automorphism group of Artin-Schreier cover of the projective line

Consider the cover $C_s: \ y^p - y = f(x) := \sum_{(t,p)=1, t>0} a_t x^t \in k[x]$. Let $m := \deg f$ so $(m,p) = 1$

We have the following theorem

Théorème 2.1 (St 1,2) *a)* $\operatorname{card} G_{\infty,1} \leq p(m-1)^2$.

b) If $(m-1,p) = 1$ then $\operatorname{card} G_{\infty,1} = p$.

c) If $f(x) = x^m$, then $\operatorname{card} G_{\infty,1} = p$ *if $m - 1 \neq p^k$ and* $\operatorname{card} G_{\infty,1} = p^{2k+1}$ *if $m - 1 = p^k$.*

d) [**Le-Ma**] *If $m - 1 = qp^k$ where $k > 0$, $q > 1$ and $(q,p) = 1$ then for $p > 2$,* $\operatorname{card} G_{\infty,1} \leq p^{k+1}$, *and for $p = 2$,* $\operatorname{card} G_{\infty,1} \leq 2^k$. *Moreover in these two cases the bound is optimal.*

Sketch proof. for b), c) and d).

Let $\sigma \in G_{\infty,1}$, it stabilizes the two linear spaces $L(p\infty)$ and $L(m\infty)$. In the sequel we will consider only the case where $m > p$.

Note then that $1, x$ resp. $1, x, ..., x^{[\frac{m}{p}]}, y$ is a k-basis for $L(p\infty)$, resp. $L(m\infty)$. So $\sigma(x) = x + c$ for $c \in k$ and $\sigma(y) = y + Q(x)$ for $Q(x) \in k[x]$ with degree $\leq \frac{m}{p}$.

Moreover

$$(**) \quad Q(x)^p - Q(x) = f(x+c) - f(x)$$

If $c \neq 0$ then as $(m,p) = 1$, $\deg(f(x+c) - f(x)) = m - 1$ and so $p | m - 1$; this proves b).

For c) here we will only consider the case $m = 1 + p$.

When $p = 2$ by the case presented in the introduction we know that $G_{\infty,1} \simeq H_8$.

When $p > 2$ then C_s is birationnal to the Fermat curve

$$F_{1+p}: \ x^{1+p} + y^{1+p} + z^{1+p} = 0$$

It is a classical fact (Leopoldt, [L]) that the automorphism group is the projective unitary group $PU(3,p^2)$ relative to the hermitian form $x.x^F + y.y^F + z.z^F$ where F is the Frobenius map of the extension $\mathbb{F}_{p^2}/\mathbb{F}_p$. One can see in this case that $G_{1,\infty} \simeq$ is isomorphic to the strict triangular subgroup in $GL(2,p)$; this is the unique non abelian p-group of order p^3 and exponent p.

d) Assume now that $m - 1 = qp^k$ where $k > 0$ and $(q,p) = 1$ then

$$f(x+c) - f(x) = \sum_{(t,p)=1} a_t (\sum_{0 \leq j \leq t-1} \binom{t}{j} c^{t-j} x^j) = g(x) \mod (F - \mathrm{Id})k[x]$$

where $g(x) = \sum_{(t,p)=1} b_t x^t$ is the unique polynomial in $k[x]$ with these properties.

So $b_t(c) = 0$ for all t with $(t,p) = 1$ and the only contributing terms in $f(x+c) - f(x)$ for the coefficient of $x^{(q-1)p^k+1}$ in $g(x)$ are $a_t \binom{t}{j_0} c^{t-j_0} x^{j_0}$ with $j_0 < t \leq m$ and $(t,p) = 1$, $j_0 = ((q-1)p^k+1)p^l < m = qp^k+1$. So $l = 0$ and $g(x) = (\sum_{j_0 < t \leq m, \ (t,p)=1} a_t \binom{t}{j_0} c^{t-j_0}) x^{j_0}$+lower degree terms.

As $\binom{m}{j_0} \equiv q \mod p$ it follows that $\deg b_{j_0} = m - j_0 = p^k$ so $\operatorname{card}\{c\} \leq \deg b_{j_0} = p^k$ and so $\operatorname{card} G_{\infty,1} \leq p.p^k = p^{k+1}$. If $p = 2$ the condition $j_0 < t \leq m,\ (t,2) = 1$ implies $j_0 + 1 < t$, so $c = 0$ is a multiple root and as we search for an additive polynomial its degree is bounded by a power of 2 which is $< 2^k$; the bound follows.

In order to see that the bound is optimal we remark that for any prime p if $f = x^{1+p+p^3} - x^{1+p^2+p^3}$; then $\operatorname{card} G_{\infty,1} = p^2$; in particular for $p = 2$ this gives the bound. Now for $p > 2$ let us consider $f = x^{1+p^k} * (x^{p^k} - x)$; then $m = 1 + 2 * p^k$ and $\operatorname{card} G_{\infty,1} = p^{k+1}$; one can check that the group is abelian with exponent p^2 if $p = 3$ and exponent p otherwise.

Note that from the discussion above that for any f, $G_{1,\infty}$ has exponent p or p^2; this last case is possible for special f.

3 Application to potentially good reduction

We keep the same notations as in the end of section 1.

Our problem was to find Y_0, a potential center for a blowing up as in part 2 of the criterium. Assume that $m = 1 + qp^k$, with $(q,p) = 1$, $q > 1$ and $k \geq 0$. We know by section 2 that $(\operatorname{Aut} C_s)_{\infty,1}$ has order $\leq p^{k+1}$ so we need a polynomial over K of degree $\leq p^k$ whose one zero is a center Y_0 for the blowing up which induces the potential good reduction when it exists. We have the following

Théorème 3.1 (Le-Ma) *Let $N(X) := \frac{F'}{gcd(F,F')}$ which we choose to be monic. If $m = 1 + qp^k$, with $(q,p) = 1$, $q > 1$ and $k \geq 0$ then $\frac{N^{m-1-p^k}}{(m-1-p^k)!} \in O_K[X]$; moreover the leading term is $\binom{m-1}{p^k} X^{p^k}$ is a unit mod p and there is a root which is congruent to $Y_0 \mod \lambda^{p/m}$.*

Sketch proof. Case $k = 0$ is proved in [Le]. Let $Y_0 \in O_{K^{alg}}$, then (see [Ma])

$$F(X + Y_0) = E(X)^p + \sum_{t \leq m, (t,p)=1} A_t X^t \mod (p^{c_n} X, X^{m+1})$$

where $E(X) \in O_{K^{alg}}$, $c_n = 1 + \frac{1}{p} + ... + \frac{1}{p^n}$ with $p^n \leq m < p^{n+1}$.

If the cover C has potentially good reduction and Y_0 is a center for the blowing up, then (cf. [Ma]),

i) $v(A_m) = 0$

ii) For $t < m$ with $(t,p) = 1$ one has $v(A_t) \geq (m-t) v(\lambda^{p/m})$

Set $j_0 := m - p^k$, then

$N(X + Y_0) = \frac{j_0}{m} A_{j_0} X^{j_0 - 1} \mod (\lambda^{p^{k+1}/m}, X^{j_0})$ and so $\frac{N^{m-1-p^k}}{(m-1-p^k)!}(Y_0) = 0 \mod \lambda^{p^{k+1}/m}$.

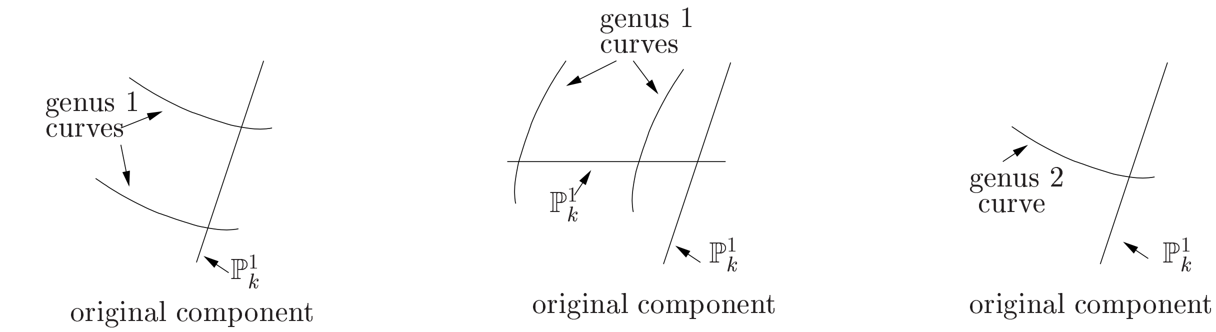
Remarque 3.2 In the difficult case i.e. $m = 1 + p^k$, consider the following exemple:

$$F(X) := 1 + cX^{p^k} + X^{p^{k+1}}$$

and $K = \mathbb{Q}_p^{nr}(c)$; and $v(c) \geq 0$.

For $v(c) \geq 0$, $Z^p = F(X)$ has potentially good reduction and for suitable c one can show ([Le-Ma]) that the wild monodromy can be as big as possible i.e. $\operatorname{card} G_{1,\infty} = p^{2k+1}$ (compare with section 2).

Remarque 3.3 In [Le-Ma], we consider the following question: for a given conductor m there are several types of degeneration and each type has an upper bound for the cardinality of the wild automorphism group $(\operatorname{Aut}_k C_s)_w$ at the special fiber. Now for a p-cyclic cover of the projective line which gets this upper bound we ask for a lifting with cardinality of the wild monodromy group $\operatorname{Gal}(L/K)_w$ equals this upper bound. For example let us consider the case where $p = 2$ and $m = 5$ i.e. genus 2 curves.



Type 1 $|\mathrm{Gal}(L/K)_w| \leq 2^6$

Type 2 $|\mathrm{Gal}(L/K)_w| \leq 2^7$

Type 3 $|\mathrm{Gal}(L/K)_w| \leq 2^5$

Fig. 6

We have then 3 degeneration types (see figure 6 below), where the genus 1 curves are isomorphic to the unique supersingular elliptic curve in characteristic 2: $(E)\ \ y^2 - y = x^3$ whose wild automorphism group is H_8. In the same inspiration as theorem 1.3. we show that $\mathrm{Gal}(L/K)_w \hookrightarrow ({\mathrm{Aut}}_{\,k} C_s)_w{}^O$ where $({\mathrm{Aut}}_{\,k} C_s)_w{}^O$ is the subgroup of automorphism fixing the original projective line. In the first type $\mathrm{card}\,({\mathrm{Aut}}_{\,k} C_s)_w{}^O \leq \mathrm{card}\, H_8 \times H_8 = 2^6$, in the second type $\mathrm{card}\,({\mathrm{Aut}}_{\,k} C_s)_w{}^O \leq \mathrm{card}\,(H_8 \times H_8) \rtimes \mathbb{Z}/2\mathbb{Z} = 2^7$ and for the last type $\mathrm{card}\,(({\mathrm{Aut}}_{\,k} C_s)_w{}^O) \leq 2^5$. The action of $\mathbb{Z}/2\mathbb{Z}$ on $H_8 \times H_8$ in $(H_8 \times H_8) \rtimes \mathbb{Z}/2\mathbb{Z}$ corresponds to the automorphism which exchanges the two isomorphic elliptic curves. In [Le-Ma] one shows that the curve $Z^2 = F(X) = 1 + a * X^2 + a^2 * X^3 + X^5$ over $K = Q_2^{unr}(a = 2^{1/3})$ gets semi-stable reduction of type 2 after the finite extension $L = K(y_i, F(y_i)^{1/2}, i = 1, ..8)$ where y_i are the roots of the polynomial $T(Y) := 15 * Y^8 + 22 * Y^6 * a^2 + 24 * Y^5 * a + 6 * Y^4 * a + 48 * Y^3 + 12 * Y * a^2 + 4 * a$ and we show with the help of MAGMA and the geometric action on the special fiber that $\mathrm{Gal}(L/K)_w \simeq (H_8 \times H_8) \rtimes \mathbb{Z}/2\mathbb{Z}$.

References

[Leo] H-W. Leopoldt, *Über die Automorphismengruppe des Fermat körpers* J. Number Theory 56 (1996), no. 2, 256–282.

[Le-Ma] C. Lehr, M. Matignon, *Wild monodromy and automorphisms of curves*, in preparation.

[Le 1] C. Lehr, *Reduction of p-cyclic Covers of the Projective Line*, Manuscripta Math. 106 (2001) 2, 151-175.

[Le 2] C. Lehr, *Effective methods for vanishing cycles of p-cyclic covers of the p-adic line*, Préprint Univ. Lille, (2002).

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

[Ma] M. Matignon, *Vers un algorithme pour la réduction stable des revêtements p-cycliques de la droite projective sur un corps p-adique*, Mathematische Annalen, Vol. 325 Issue 2 (2003) pp 323-354

[St 1] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe.* Arch. Math. (Basel) 24 (1973) 527–544.

[St 2] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern.* Arch. Math. (Basel) 24 (1973), 615–631.

Claus LEHR
UFR de Mathématiques Pures et Appliquées, Cité Scientifique- Bât. M2, F-59655
Villeneuve d'Ascq Cedex
e-mail : `lehr@agat.univ-lille1.fr`

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`