Automorphisms and monodromy *

M. Matignon

June 28, 2006

1 Introduction

1.1 Monodromy and automorphism groups

- R is a strictly henselian DVR of inequal characteristic $(0, p)$.

  $K := \mathrm{Fr}R$; for example $K/\mathbb{Q}_p^{ur}$ finite.

  π a uniformizing parameter.

  $k := R_K/\pi R_K$.

  C/K smooth projective curve, $g(C) \geq 1$.

- C has potentially good reduction over K if there is L/K (finite) such that $C \times_K L$ has a smooth model over R_L. Then:

- There is a minimal extension L/K with this property; it is Galois and called the **monodromy** extension.

- $\mathrm{Gal}(L/K)$ is the **monodromy group**.

- Its p-Sylow subgroup is the **wild monodromy group** .

- The base change $C \times_K K^{alg}$ induces an homomorphism $\varphi : \mathrm{Gal}(K^{alg}/K) \to \mathrm{Aut}_k C_s$, where C_s is the special fiber of the smooth model over R_L and $L = (K^{alg})^{\ker \varphi}$.

- Let ℓ be a prime number, then, $n_\ell := v_\ell(|\mathrm{Gal}(L/K)|) \leq v_\ell(|\mathrm{Aut}_k C_s|)$.

- If $\ell \notin \{2, p\}$, then ℓ^{n_ℓ} is bounded by the maximal order of an ℓ-cyclic subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ i.e. $\ell^{n_\ell} \leq O(g)$.

- If $p > 2$, then $n_p \leq \inf_{\ell \neq 2,p} v_p(|\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|) = a + [a/p] + ...$, where $a = [\frac{2g}{p-1}]$.

  This gives an exponential type bound in g for $|\mathrm{Aut}_k C_s|$. This justifies our interest in looking at Stichtenoth ([St,73]) and Singh ([Si,73]).

Theorem 1.1. *([Ra, 90]). Let $Y_K \to X_K$ be a Galois cover with group G. Let us assume that:*

---

*This paper is a report on common work with Claus Lehr. This is a pdf style version of lectures given at Chuo University April 2006. A slide version using beamer is available at http://www.math.u-bordeaux.fr/˜matignon/

- *G is nilpotent.*
- *X_K has a smooth model X.*
- *The Zariski closure B of the branch locus B_K in X is étale over R_K.*

Then, the special fiber of the stable model Y_K is tree-like, i.e. the Jacobian of Y_K has potentially good reduction.

Raynaud's proof is qualitative and it seems difficult to give a constructive one in the simplest cases.

We have given in [Le-Ma1] such a proof in the case of p-cyclic covers of the projective line.

Thanks. The author would like to use this opportunity to thank T. Sekiguchi, N. Suwa and B. Green for the pleasant and working atmosphere during his visit to Tokyo.

2 Automorphism groups of curves in char.$p > 0$

2.1 p -cyclic covers of the affine line

k is an algebraically closed of char. $p > 0$.

- $f(X) \in Xk[X]$ monic,deg $f = m > 1$ prime to p.
- $C_f : W^p - W = f(X)$. Let ∞ be the point of C_f above $X = \infty$ and z a local parameter. Then, $g := g(C_f) = \frac{p-1}{2}(m-1) > 0$.
- $G_\infty(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid \sigma(\infty) = \infty\}$.
- $G_{\infty,1}(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid v_\infty(\sigma(z) - z) \geq 2\}$, the p-Sylow.
- ([St,73]) Let $g(C_f) \geq 2$, then $G_{\infty,1}(f)$ is a p-Sylow of $\mathrm{Aut}_k C_f$.
- It is normal except for $f(X) = X^m$ where $m|1+p$.

2.2 Structure of $G_{\infty,1}(f)$

- Let $\rho(X) = X$, $\rho(W) = W + 1$, then $< \rho >= G_{\infty,2} \subset Z(G_{\infty,1})$
- $0 \to < \rho > \to G_{\infty,1} \to V \to 0, \quad V := \{\tau_y | \ \tau_y(X) = X + y, \ y \in k\}$.
  $f(X+y) = f(X) + f(y) + (F - \mathrm{Id})(P(X,y))$, $P(X,y) \in Xk[X]$.
  $V \simeq (\mathbb{Z}/p\mathbb{Z})^v$ as a subgroup of k.
- Let $\tau_y(W) := W + a_y + P(X,y)$, $a_y \in \mathbb{F}_p$, then $[\tau_y, \tau_z] = \rho^{\epsilon(y,z)}$, where $\epsilon : V \times V \to \mathbb{F}_p$ is an alternating form.
- ϵ is non degenerated iff $< \rho >= Z(G_{\infty,1})$.

2.3 Bounds for $|G_{\infty,1}(f)|$

Lemma 2.1. *If $f(X)=\sum_{1\leq i\leq m} t_i X^i \in k[X]$ is monic, then:*

- $\Delta(f)(X,Y) := f(X+Y)-f(X)-f(Y) = R(X,Y)+(F-\mathrm{Id})(P_f(X,Y))$, *where* $R \in \bigoplus_{\lfloor \frac{m}{p} \rfloor \leq ip^{n(i)}<m,\ (i,p)=1} k[Y]X^{ip^{n(i)}}$ *and* $P_f \in Xk[X,Y]$.
- $P_f = (\mathrm{Id}+F+...+F^{n-1})(\Delta(f)) \mod X^{[\frac{m-1}{p}]+1}$.

Let us denote by $\mathrm{Ad}_f(Y)$ *the content of* $R(X,Y)\in k[Y][X]$*, then*

- $\mathrm{Ad}_f(Y)$ *is an additive and separable polynomial.*
- $Z(\mathrm{Ad}_f(Y)) \simeq V$.

Let $m-1=\ell p^s$ with $(\ell,p)=1$.

- ([St 73]) $|G_{\infty,1}| = p\deg \mathrm{Ad}_f \leq p(m-1)^2$, i.e. $\frac{|G_{\infty,1}|}{g^2} \leq \frac{4p}{(p-1)^2}$.
- ([St 73]) $s=0$ i.e. $(m-1,p)=1$, then $|G_{\infty,1}|=p$.
- If $s>0$,
  - $\ell>1$, $p=2$, then $\frac{|G_{\infty,1}|}{g} \leq \frac{2}{3}$.
  - $\ell>1$, $p>2$, then $\frac{|G_{\infty,1}|}{g} \leq \frac{p}{p-1}$.
  - ([St 73]) $\ell>1$, $m=1+p^s$, then $\frac{|G_{\infty,1}|}{g} \leq 2p^s\frac{p}{p-1}$ (with equality for $f(X)=X^{1+p^s}$).

2.4 Characterization of $G_{\infty,1}(f)$

- We consider the extensions $0\to N\simeq Z/p\mathbb{Z}\to G\to(\mathbb{Z}/p\mathbb{Z})^n\to 0$ (note that $G_{\infty,1}(f)$ is an extension of this type). Then $G'\subset N\subset Z(G)$.
- If $G'=Z(G)$, G is called extraspecial.
  - Then, $|G|=p^{2s+1}$ and there are 2 isomorphism classes for a given s.
  - If $p>2$, we denote by $E(p^3)$ (resp. $M(p^3)$) the non abelian group of order p^3 and exponent p (resp. p^2). Then, $G\simeq E(p^3)*E(p^3)*...*E(p^3)$ or $M(p^3)*E(p^3)*...*E(p^3)$, according as the exponent is p or p^2.
  - If $p=2$, then $G\simeq D_8*D_8*...*D_8$ or $Q_8*D_8*...*D_8$ (in both cases, the exponent is 2^2).
- If $G'\subset Z(G)$, G is a subgroup of an extraspecial group E with $Z(E)\subset G$.

Theorem 2.2. *([Le-Ma 1]). Let* $f(X)=X\Sigma(F)(X)\in Xk[X]$, $\Sigma(F)=\sum_{0\leq i\leq s} a_iF^i \in k\{F\}$ *an additive polynomial with* $\deg f = 1+p^s$*. Then,*

- $\mathrm{Ad}_f(Y)=F^s(\sum_{0\leq i\leq s}(a_iF^i+F^{-i}a_i)(Y))$*, a palyndromic polynomial.*
- $G_{\infty,1}(f)$ *is an extraspecial group with cardinal* p^{2s+1} *and exponent* p *for* $p>2$*, and of type* $Q_8*D_8*...*D_8$ *for* $p=2$.

Theorem 2.3. *([Le-Ma 1]). If G is an extension of type* $0 \to \mathbb{Z}/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$*, there is* $f \in Xk[X]$ *with* $G \simeq G_{\infty,1}(f)$.

- Sketch proof: Extraspecial groups with exponent p^2 are realized by a modification by a Witt cocycle of the polynomial f in the previous theorem.
- We can see G as a subgroup of an extraspecial group E, then we realize E with f_E and a suitable modification of f_E will limit $G_{\infty,1}(f_E)$ to G.

3 Actions of p-groups over a curve C with $g(C) \geq 2$

3.1 Big actions (I)

Theorem 3.1. *([Le-Ma 1]). Let* $f(X) \in Xk[X]$ *with* $(\deg f, p) = 1$*. If* $\frac{|G_{\infty,1}|}{g} > \frac{p}{p-1}$ *(*$\frac{2}{3}$ *for* $p = 2$*), then* $f(X) = cX + X\Sigma(F)(X) \in k[X]$.

- Sketch proof: One shows that monomials in f with a degree $\notin 1 + p^{\mathbb{N}}$ will limit the degree of Ad_f.
- Let (C, G) with $G \subset \mathrm{Aut}_k C$, a p-group. We say that (C, G) is a **big action** if:
  (N) $g_C > 0$ and $\frac{|G|}{g_C} > \frac{2p}{p-1}$.
  It follows from ([Na 87]) that there is $\infty \in C$, with
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ is étale and $G = G_{\infty,1}$.
  - $G_{\infty,2} \neq G_{\infty,1}$ and $C/G_{\infty,2} \simeq \mathbb{P}^1_k$
  - Then, $G_{\infty,1}/G_{\infty,2}$ acts as a group of translations of the affine line $C/G_{\infty,2} - \{\infty\}$.
- **Transfert of condition (N) to quotients.** Let (C, G) a big action, if $H \lhd G$ and if $g(C/H) > 0$, then $(C/H, G/H)$ is a big action.

3.2 Condition (N) and G_2

In this section (C, G) **is a big action.** Let G_i be the lower ramification groups.

- Let $H \lhd G$ and H with index p in G_2 (H exists!), then $(C/H, G/H)$ satisfies (N).
- $(G/H)_2 = G_2/H \simeq \mathbb{Z}/p\mathbb{Z}$.
- There is $S(F) \in k\{F\}$, $f_1 = cX + X\Sigma(F)(X) \in k[X]$ with $C/H \simeq C_{f_1}$.
- If $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^t$, then $k(C) = k(X, W_1, ..., W_t)$ and $\wp(W_1, ..., W_t) = (f_1(X), f_2(X), ..., f_t(X)) \in (k[X])^t$
- $f_1(X), .., f_t(X)$ are $\mathbb{F}_p$-free $\mod \wp(k[X])$.
- The group extension $0 \to G_2 \to G_1 \to V = (\mathbb{Z}/p\mathbb{Z})^v \to 0$ induces a representation $\rho : V \to \mathrm{Gl}_t(\mathbb{F}_p)$
- dual to the one given by V acting via translation: $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to \to (f_1(X+v), f_2(X+v), ..., f_t(X+v)) \mod \wp(k[X])^t$

- Imρ is a unipotent subgroup of $\mathrm{Gl}_t(\mathbb{F}_p)$ which is the identity iff $G_2 \subset Z(G)$. In this case $f_i(X) = c_iX + X\Sigma_i(F)(X)$ where $\Sigma_i(F) \in k\{F\}$ and $v \in V$ is a commun zero to the palyndromic polynomials $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- Let $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ with $\alpha^p + \alpha = 0$; then $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
- Let $f_2 := X^{1+2p} - X^{2+p}$, then
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p \mod \wp(k[X,Y])$
- If $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ one has

  $f_2(X+y) = \frac{2(y^p-y)}{\alpha} f_1(X) + f_2(X) + \wp(P_2)$.
- $y \longrightarrow \frac{2(y^p-y)}{\alpha}$ is a non zero linear form over $\mathbb{F}_{p^2}$ with value in $\mathbb{F}_p$.
- $|G| = p^2p^2$ and $g = \frac{p-1}{2}(p + p(2p))$.
- $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

Theorem 3.2. *([Le-Ma 4]) Let (C, G) be a big action then $G_2 = G'$.*

- Sketch proof: If $G' \neq G_2$, there is $H \lhd G$ with $G' \subset H \subset G_2$ and $[G_2 : H] = p$. $(C/H, G/H)$ satisfies condition (N);
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^s$.
- $(\mathrm{Aut}C/H)_{\infty,1} := E$, is extraspecial with order p^{2s+1}.
- G/H is abelian and normal in E.
- ([Hu 67] Satz 13.7 p. 353) $|G/H| \leq p^{s+1}$ and so $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$, a contradiction.

  We deduce the following corollary from ([Su 86] 4.21 p.75).

Corollary 3.3. *If $|G_2| = p^3$, then G_2 is abelian.*

3.3 Riemann surfaces

- In characteristic 0, an analogue of big actions is given by the actions of a finite group G on a compact Riemann surface C with $g_C \geq 2$ such that $|G| = 84(g_C - 1)$ (we say that C is an **Hurwitz curve**) ([Co 90]).
- Let us mention Klein's quartic ($G \simeq PSL_2(\mathbb{F}_7)$) ([El 99]).
- The Fricke-Macbeath curves with genus 7 ($G \simeq PSL_2(\mathbb{F}_8)$) ([Mc],65).
- Let C be an Hurwitz curve with genus g_C. Let $n > 1$ and C_n the maximal unramified Galois cover whose group is abelian with exponent n. The Galois group of C_n/C is $(\mathbb{Z}/n\mathbb{Z})^{2g_C}$. It follows from the unicity of C_n that the k-automorphisms of C have n^{2g} prolongations to C_n. Therefore $g_{C_n} - 1 = n^{2g}(g_C - 1)$ and $n^{2g}|\mathrm{Aut}_kC| \leq |\mathrm{Aut}_kC_n|$, where $|\mathrm{Aut}_kC_n| \geq 84(g_{C_n} - 1)$; C_n is an Hurwitz curve ([Mc],61).

3.4 Ray class fields

- If (C, G) is a big action in char.$p > 0)$, then $C \to C/G$ is an tale cover of the affine line whose group is a p-group; it follows that the Hasse-Witt invariant of C is zero; therefore, in order to adapt the previous proof to char. $p > 0$, one needs to accept ramification. This is done with the so called ray class fields of function fields over finite fields.

- Let $K := \mathbb{F}_q(X)$ where $q = p^e$, S the set of finite rational places $(X - v)$, $v \in \mathbb{F}_q$ and $m \in \mathbb{N}$. Let K^{alg} be an algebraic closure. Let $K_S^m \subset K^{alg}$ be the biggest abelian extension L of K with conductor $\leq m\infty$ and such that the places in S are completely decomposed.

- ([La 99], [Au 00]) The constant field of K_S^m is $\mathbb{F}_q$ and $G_S(m) := \mathrm{Gal}(K_S^m/K) \simeq (1 + T\mathbb{F}_q[[T]])/ < 1 + T^m\mathbb{F}_q[[T]], 1 - vT, v \in \mathbb{F}_q >$, is a p-group.

- ([Ma-Le 4]) Let $C_m/\mathbb{F}_q$ be the smooth projective curve with function field K_S^m. The translations $X \to X + v$, $v \in \mathbb{F}_q$ stabilize S and ∞; they can be extended to $\mathbb{F}_q$-automorphisms of K_S^m. In this way, we get an action of a p-group $G(m)$ on C_m with $0 \to G_S(m) \to G(m) \to \mathbb{F}_q \to 0$

- ([Au 00] If $n_m := |G_S(m)|$, then $g_{C_m} = 1 + n_m(-1 + m/2) - (1/2)\sum_{0\leq j\leq m-1} n_j \leq n_m(-1 + m/2)$

- $\frac{|G(m)|}{g_{C_m}} \geq \frac{n_m q}{n_m(-1+m/2)} = \frac{q}{-1+m/2}$. This is a "big action" as soon as $\frac{q}{-1+m/2} > \frac{2p}{p-1}$ (we have $G_2 = G_S(m)$)

- Let $N_q := |C_m(\mathbb{F}_q)|$. Then, $N_q = 1 + |G(m)|$, and the quotient $\frac{|G(m)|}{g_{C_m}} \sim \frac{N_q}{g_{C_m}}$.

- ([La 99]) If $q = p^e$,$m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$ is the smallest conductor m such that the exponent of G_S^m is $> p$.

- If $e > 2$, $(C_{m_2}, G(m_2))$ is a big action and G_2 is abelian with exponent p^2.

3.5 Big actions (II)

From now on, k is any algebraically closed field and (C, G) is a big action.

- If $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$, then $n = 1$ ([Le-Ma 4]).
  - Sketch proof: Let $H = G_2^{p^{n-2}}$ then $(C/H, G/H)$ is a big action, it follows that one can assume that $n = 2$. Then $C \to C/G_2$ is given by $\wp(W_0, W_1) = (f_0, f_1)$ with $f_0 = X\Sigma(F)(X)$, $\deg f_0 = 1 + p^s$.
  - Let $v \in V := Z(\mathrm{Ad}_{f_0})$ and $P \in k[X]$ with $f_0(X + v) = f_0(X) + \wp(P)$ then $f_1(X + v) - f_1(X) = \ell(v)f_0(X) + \frac{1}{p}(f_0(X)^p + P(X)^p - P(X)^{p^2} - (f_0(X) + P(X))^p - f_0(X + v)^p + (f_0(X + v) + P(X)^p)^p)$
  - $= \ell(v)f_0(X) + \sum_{1\leq i\leq p-1} \frac{(-1)^{i-1}}{i} v^i X^{p-i+p^{s+1}} \mod X^{p^{s+1}}$ where $\ell : V \to \mathbb{F}_p$ is a linear form.

- More generally for G_2 abelian with exponent p^e, $e \geq 2$, one can expect a lower bound in $O(log(g_C))$ for the p-rank of G_2. This is the case in the preceding situation i.e. $(C, G) = (C_{m_2}, G(m_2))$ ([M. Rocher, thesis in preparation]).

3.6 Maximal curves

Let us assume that (C,G) is a big action.

- Let i_0 with $G_2 = G_3 = ... = G_{i_0} \supsetneqq G_{i_0+1}$. Then $g_{(C/G_{i_0+1})} = \frac{1}{2}(|G_2/G_{i_0+1}| - 1)(i_0 - 1)$.
- If $0 < M \leq \frac{|G|}{g_C^2}$, then
  $|G_{i_0+1}| \leq \frac{1}{M}\frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.

Theorem 3.4. *([Le-Ma 1]) If $\frac{|G|}{g_C^2} \geq \frac{4}{(p-1)^2}$, then there is $\Sigma(F) \in k\{F\}$ and $f = cX + X\Sigma(F)(X) \in k[X]$ with $C \simeq C_f$.*

Moreover there are two possibilities for G:

- $\frac{|G|}{g_C^2} = \frac{4p}{(p-1)^2}$ *and* $G = G_{\infty,1}(f)$ *or*
- $\frac{|G|}{g_C^2} = \frac{4}{(p-1)^2}$ *and* $G \subset G_{\infty,1}(f)$ *has index* p.

- Note that the sequence $\frac{p^n}{(p^n-1)^2}$ is decreasing and that $|G_{i_0+1}| \in p^{\mathbb{N}}$.
- We deduce bounds for $|G_2/G_{i_0+1}|$, $|G_{i_0+1}|$ and so for $|G_2|$.

We still assume that (C,G) is a big action.

- One can push the "classification " of big actions up to the condition $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$. Namely
- One first show that $|G_2|$ divides p^3.
- G_2 is abelian by corollary 7.
- Applying ([Mr 71]) to the case of abelian extensions with group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$, one shows that G_2 has exponent p (we have seen in 3.5 that G_2 is cyclic iff $G_2 = \mathbb{Z}/p\mathbb{Z}$).

Theorem 3.5. *([Le-Ma 4]) For all $M > 0$, the set $\frac{|G|}{g_C^2} > M$, for (C,G) a big action with G_2 abelian with exponent p, is finite.*

Sketch proof: We saw that $|G_2|$ and so t are bounded above. We use the notations introduce in 3.2. moreover we can choose the f_i and the $m_i := \deg f_i$ with $m_1 \leq m_2 \leq ... \leq m_t$ and in such a way that $\deg(\sum_{1\leq i\leq t} \lambda_i f_i) \in \{m_i,\ 1 \leq i \leq t\}$ for $[\lambda_i] \in \mathbb{P}^{t-1}(\mathbb{F}_p)$.

We distinguish two cases:

- If $\mathrm{Im}\rho$ is trivial.
  - Then $m_i - 1 = p^{\nu_i}$ and $\nu_1 \leq ... \leq \nu_t$
  - $|G| = p^t|V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ is bounded above.

- $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ and so $\{\frac{p^{2\nu_1}}{|V|}\}$ is finite.
- $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ is finite.

- If Imρ isn't trivial.
  - There is a smallest i_0 such that $f_{i_0+1}(X) \neq cX + X\Sigma(F)(X)$ (exercise).
  - For $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v)f_i(X) \mod \wp(k[X])$
  - ℓ_i is a non zero linear form on the $\mathbb{F}_p$-space V.
  - Let $W := \cap_{1\leq i\leq i_0} \ker \ell_i$, then $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i-1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1}-1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2}p^{i_0}(m_{i_0+1}-1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ is bounded above and $g_C^2 \leq \frac{p^t|V|}{M}$ is also bounded above .
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ is finite. ///

4 Monodromy polynomial

- Let $C \longrightarrow \mathbb{P}^1_K$ birationally given by the equation: $Z_0^p = f(X_0) = \prod_{1\leq i\leq m}(X_0 - x_i)^{n_i} \in R[X_0]$, $(n_i, p) = 1$ and $(\deg f, p) = 1$, $v(x_i - x_j) = v(x_i) = 0$ for $i \neq j$.

- $f'(Y)/f(Y) = S_1(Y)/S_0(Y)$, $(S_0(Y), S_1(Y)) = 1$; then $\deg(S_1(Y)) = m-1$ and $\deg(S_0(Y)) = m$.

- $f(X+Y) = f(Y)((1 + a_1(Y)X + ... + a_r(Y)X^r)^p - \sum_{r+1\leq i\leq n} A_i(Y)X^i)$, where $r+1 = [n/p]$, $a_i(Y), A_i(Y) \in K(Y)$.

- There is a unique α such that $r < p^\alpha < n < p^{\alpha+1}$

- There is $T(Y) \in R[Y]$ with $A_{p^\alpha}(Y) = -\binom{\frac{1}{p}}{p^{\alpha-1}}^p \frac{S_1(Y)^{p^\alpha} + pT(Y)}{S_0(Y)^{p^\alpha}}$.

- $\mathcal{L}(Y) := S_1(Y)^{p^\alpha} + pT(Y)$. This is a polynomial of degree $p^\alpha(m-1)$ which is called the **monodromy polynomial** of $f(Y)$.

4.1 Marked stable model

We mean the R-model $\mathcal{C}_R$ defined by $Z_0^p = f(X_0) = \prod_{1\leq i\leq m}(X_0 - x_i)^{n_i} \in R[X_0]$ (cf. fig 1).

Theorem 4.1. *([Le-Ma 3])*

- *The components with genus > 0 of the marked stable model of C correspond bijectively to the Gauss valuations v_{X_j} with $\rho_j X_j = X_0 - y_j$, where y_j is a zero of the monodromy polynomial $\mathcal{L}(Y)$*

- $\rho_j \in R^{\mathrm{alg}}$ *satisfies* $v(\rho_j) = \max\{\frac{1}{i}v\left(\frac{\lambda^p}{A_i(y_j)}\right)$ *for* $r+1 \leq i \leq n\}$.

- *The dual graph of the special fiber of the marked stable model of C is an oriented tree whose ends are in bijection with the components of genus > 0.*

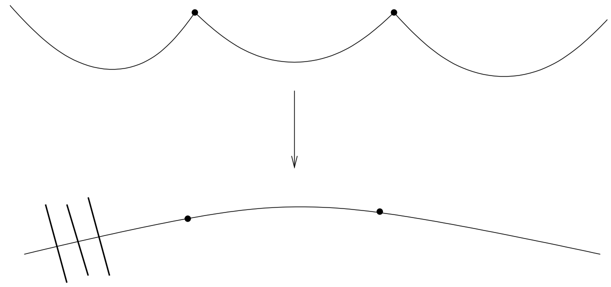


Figure 1: $\mathcal{C}_R \otimes_R k \longrightarrow \mathbb{P}^1_k$ with singularities and branch locus

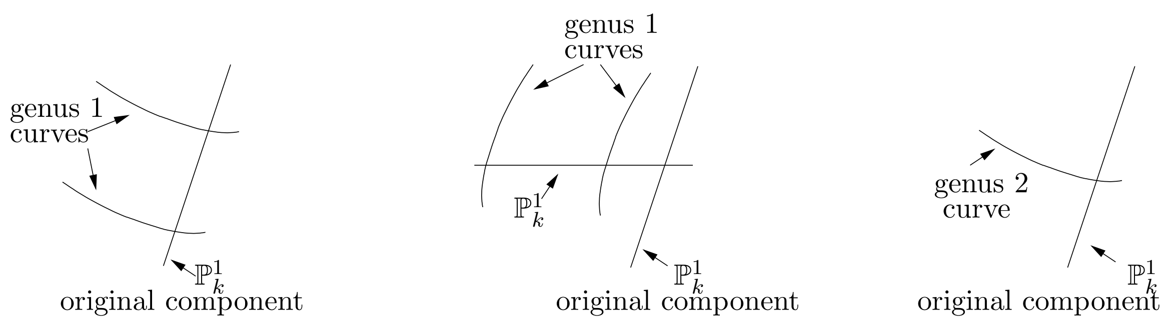
4.2 Potentially good reduction

Theorem 4.2. *([Le-Ma 3])*

- $p > 2$, $q = p^n$, $n \geq 1$, $K = \mathbb{Q}_p^{\mathrm{ur}}(p^{p/(q+1)})$ *and* $C \longrightarrow \mathbb{P}^1_K$ *is birationally defined by the equation* $Z_0^p = f(X_0) = 1 + p^{p/(q+1)} X_0^q + X_0^{q+1}$.
- *Then,* C *has potentially good reduction and* $\mathcal{L}(Y)$ *is irreducible over* K*.*
- *The monodromy* L/K *is the extension of the decomposition field of* $\mathcal{L}(Y)$ *obtained by adjoining the* p*-roots* $f(y)^{1/p}$*, for* y *describing the zeroes of* $\mathcal{L}(Y)$*.*
- *The monodromy group is the extraspecial group with exponent* p^2 *and order* pq^2 *(which is maximal for this conductor).*

4.3 Genus 2

- Case $p = 2$ and $m = 5$ (i.e. curves with genus 2 over a 2-adic field $\subset \mathbb{Q}_2^{\mathrm{tame}}$).
- There are 3 types of degeneration for the marked stable model.



- Type 1: $\mathrm{Gal}(K'/K)_w \hookrightarrow Q_8 \times Q_8$ — Type 2: $\mathrm{Gal}(K'/K)_w \hookrightarrow (Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$ — Type 3: $\mathrm{Gal}(K'/K)_w \hookrightarrow Q_8 * D_8$

- $C \longrightarrow \mathbb{P}^1_K$ is birationally defined by the equation $Z_0^p = f(X_0)$ with $f(X_0) = 1 + b_2 X_0^2 + b_3 X_0^3 + b_4 X_0^4 + X_0^5 \in R[X_0]$.

Now, we see that the monodromy can be maximal for the 3 types of degeneration.
a) $f(X_0) = 1 + 2^{3/5} X_0^2 + X_0^3 + 2^{2/5} X_0^4 + X_0^5$ and $K = \mathbb{Q}_2^{\mathrm{ur}}(2^{1/15})$;

- C has a marked stable model of type 1.

- The maximal monodromy group is $\simeq Q_8 \times Q_8$.

b) Let $K = \mathbb{Q}_2^{\mathrm{ur}}(a)$ with $a^9 = 2$ and $f(X_0) = 1 + a^3 X_0^2 + a^6 X_0^3 + X_0^5$.

- C has a marked stable model of type 2.
- The maximal monodromy group is $\simeq (Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Z}/2\mathbb{Z}$ exchanges the 2 factors.

c) $K = \mathbb{Q}_2^{\mathrm{ur}}$ and $f(X_0) = 1 + X_0^4 + X_0^5$.

- C has potentially good reduction (i.e. is of type 3)
- The maximal monodromy group is $\simeq Q_8 * D_8$.

References

[Au 00] R. Auer, *Ray class fields of global function fields with many rational places*, Acta Arith. 95 (2000), no. 2, 97–122.

[Co 90] M. Conder, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. (N.S.) 23 (1990), no. 2, 359–370.

[El 99] N. Elkies, *The Klein quartic in number theory*, The eightfold way, 51–101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, 1999.

[La 99] K. Lauter, *A formula for constructing curves over finite fields with many rational points*, J. Number Theory 74 (1999), no. 1, 56–72.

[Le-Ma 1] C. Lehr, M. Matignon, *Automorphism groups for p-cyclic covers of the affine line*, Compos. Math. 141 (2005), no. 5, 1213–1237.

[Le-Ma 2] C. Lehr, M. Matignon,*Automorphisms of curves and stable reduction*, in Problems from the workshop on "Automorphisms of Curves" (Leiden, August, 2004), edited by G. Cornelissen and F.Oort, Rend. Sem. Math. Univ. Padova. Vol. 113 (2005), 151-158.

[Le-Ma 3] C. Lehr, M. Matignon, *Wild monodromy and automorphisms of curves* , Duke math. J. à paraître.

[Le-Ma 4] C. Lehr, M. Matignon, *Curves with a big p-group action*, En préparation.

[Mc 61] A. M. Macbeath, *On a theorem of Hurwitz*, Proc. Glasgow Math. Assoc. 5 1961 90–96 (1961).

[Mc 65] A. M. Macbeath, *On a curve of genus* 7, Proc. London Math. Soc. (3) 15 1965 527–542.

[Mr 71] M. Marshall, *Ramification groups of abelian local field extensions*, Canad. J. Math. 23 (1971) 271–281.

[Na 87] S. Nakajima, *p-ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc. 303, 595-607 (1987).

[Ra 90] M. Raynaud, *p-groupes et réduction semi-stable des courbes*, The Grothendieck Festschrift, Vol.3, Basel-Boston-Berlin: Birkhäuser (1990).

[Si 74] B. Singh, *On the group of automorphisms of function field of genus at least two*, J. Pure Appl. Algebra 4 (1974), 205–229.

[St 73] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I, II.* Arch. Math. 24 (1973) 527–544 , 615–631.

[Su 86] M. Suzuki, *Group theory II*, Grundlehren der Mathematischen Wissenschaften 248. Springer-Verlag, New York, 1986.

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-bordeaux1.fr