数理解析研究所講究録
1073巻 1998年 106-113

Lecture II : Finite order automorphisms of a p-adic open disc

by Michel Matignon

Notations: Same as in Lecture I.

0. Introduction

We would like to understand when the local lifting problem has a positive answer, and moreover for a given group as automorphism group of $k[[z]]$ we would like to classify the possible liftings via geometric datas suppress, the inverse Galois type conjecture as settled in Lecture I says that we expect a lot of solutions.

The first important case to handle is that of p-cyclic groups.

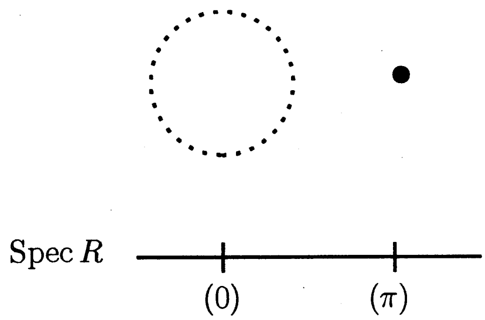
I. Generalities

a. Open disc over R.

Definition. *Let R be as above, let D^o be the R-scheme* $\mathrm{Spec}R[[Z]]$, *it's geometric generic fiber* $D^o_{(K^{\mathrm{alg}})} = \mathrm{Spec}(R[[Z]] \otimes_R K^{\mathrm{alg}})$ *can be easily described. The closed points are given by the ideals $(Z - Z_0)$ where $Z_0 \in K^{\mathrm{alg}}$ is in the open disc $v(Z_0) > 0$. Then*

$$D^o_{(K)} \simeq D^o_{(K^{\mathrm{alg}})}/\mathrm{Gal}(K^{\mathrm{alg}}/K),$$

this is the open disc over K (of ray 1) and we will call its minimal smooth model over R, D^o the open disc over R.



b. Automorphisms of open discs.

The R-automorphisms of $R[[Z]]$ are continuous for the (π, Z)-adic topology, we denote by $\mathrm{Aut}_R R[[Z]]$ their set.

Such $\sigma \in \mathrm{Aut}_R R[[Z]]$ is determined by $\sigma(Z) := a_0 + a_1 Z + \cdots$ such that $a_0 \in \pi Z$ and $a_1 \in R^\times$.

As usual σ acts on the scheme D^o; namely for $Z_0 \in \pi R$, the action on the ideal $(Z - Z_0)$ is the ideal $\sigma^{-1}(Z - Z_0) = (Z - Z_0')$ where Z_0' is the series $\sigma(Z)$ evaluated in Z_0. We will do the following abuse, we will denote $Z_0 \to \sigma(Z_0)$ this action on closed points in $D^o_{(K^{\mathrm{alg}})}$.

Definiton. *Let $\sigma \in \mathrm{Aut}_R R[[Z]]$ be a finite order automorphism; we denote by F_σ the set of geometric points in $D^o_{(K^{\mathrm{alg}})}$ which are fixed by the action of σ, i.e. the roots of the series $\sigma(Z) - Z$.*

In the sequel unless mentionned we focus our attention on finite order σ's for which $F_\sigma \neq \emptyset$.

Write $\sigma(Z) - Z = b_0 + b_1 Z + \cdots = f_{m+1}(Z)U(Z)$ by Weierstrass Preparation Theorem, where $f_{m+1}(Z)$ is a degree $m+1$ distinguished polynomial and $U(Z)$ a unit in $R[[Z]]$.

One can show that $f_{m+1}(Z)$ has $m+1$ distinct roots in K^{alg} (with value $|\;| < 1$), then

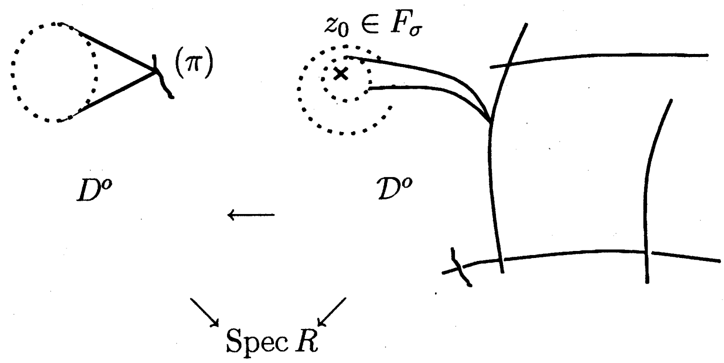
$$|F_\sigma| = m + 1 = \inf\{\, i \,|\, v(b_i) \le v(b_j), \forall j\}.$$

Say order $\sigma = p$ and $F_\sigma \neq \emptyset$. To each point $Z_0 \in F_\sigma$ we attached a primitive n-th root of unity namely $\frac{\sigma(Z - Z_0)}{Z - Z_0} \bmod (Z - Z_0)$.

Fixing a primitive m-th root of 1 say ζ this defines for $F_\sigma = \{Z_0, \cdots, Z_m\}$ a set $\{h_0, \cdots, h_m\} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^m$, we call this set the Hurwitz data $H(\sigma)$ of the automorphism σ.

c. Let σ as above. After a finite extension of R we can assume that $F_\sigma \subset D^o(R)$. We denote by $\mathcal{D}^o$, the minimal semi-stable model of $D^o_{(K)}$ in which the points in F_σ specialize in distinct smooth points (this can be achieved by successive blowing up centered in (π, Z)), moreover by the minimality condition this model is unique and so σ acts on $\mathcal{D}^o$. This model gives a picture of the geometry of points in F_σ.

The special fibre is an oriented tree like of projective lines attached to the original generic point $(\pi) \in D^o$ (as origin); each projective line gets in this way a natural ∞ point.



Main problem: Describe the possible trees and the relative positions of crossing points as well of specializations of points in F_σ.

d. Some examples.

0. Finite order automorphisms σ such that $F_\sigma = \emptyset$ naturally occur when considering Lubin-Tate formal groups. Namely let $F(Z_1, Z_2)$ be a formal group law over R, R^s(*resp.* $\mathfrak{m}^s$) $:= \{z \in K^{\mathrm{alg}} | v(z) \geq 0$ (*resp.* > 0)$\}$ and denote by $F(\mathfrak{m}^s)$ the group whose underlying space is $\mathfrak{m}^s$ and the group law is given by $z_1 +_F z_2 = F(z_1, z_2)$.

Let $\Lambda(\mathfrak{m}^s) \subset F(\mathfrak{m}^s)$ be the torsion subgroup. The map $\Phi : \Lambda(\mathfrak{m}^s) \to \mathrm{Aut}_{R^s} R^s[[Z]]$ defined by $\Phi(z)(Z) = F(Z, z)$ is an injective homomorphism ([Ha] 35.2.6). It is easy to see that $\Phi(z)$ induces the identity automorphism at the special fiber and that it has no fix point. Moreover when $\Lambda(\mathfrak{m}^s) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^h$ where h is the height of $F(Z_1, Z_2)$ (see [H] 35.1.6). Now consider G a finite abelian p-group of p rank h, let $F(Z_1, Z_2)$ be a Lubin-Tate formal group of height h then $G \subset \Lambda(\mathfrak{m}^s)$ occurs as a subgroup of $\mathrm{Aut}_R R[[Z]]$.

1. Let $o(\sigma) = n$ and $(n, p) = 1$, then σ has a unique fix point which is rational, moreover it is linearizable *i.e.* there is a new parameter Z' such that $\sigma(Z') = \zeta^h Z'$ for ζ^h a primitive n-th root of unity. This classifies such automorphism up to conjugation.

2. More generally (see [G-M2] Prop.6.2.1) if σ is a finite order automorphism with only one fix point then it is linearizable.

3. Let $(m, p) = 1$ and consider the order p-automorphism build in the previous lecture $\sigma(Z) = \zeta Z(1 + Z^m)^{-1/m}$, then

$$F_\sigma = \{0, \theta^i(\zeta^m - 1)^{1/m} \,|\, 0 \leq i < m\}$$

where θ is a primitive m-th root of 1. The Hurwitz datas are $(1, -1/m, ..., -1/m)$ and the tree as considered in **c.** has only one projective line (*i.e.* the fix points are equidistant).

4. In [M] we build an example of order p-automorphism with equidistant fix points in order to lift some $(\mathbb{Z}/p\mathbb{Z})^n$-realization as an automorphism group of $k[[z]]$. (See end of previous lecture.)

We prove

Theorem([M]). *Let $a_1, a_2, \cdots, a_n \in \mathbb{Z}_p^{\mathrm{ur}}$ and*

$$P(X) = \prod_{(\varepsilon_1, \cdots, \varepsilon_n) \in \{0, \cdots, p-1\}^n} \left[1 + \left(\sum_{1 \leq i \leq n} \varepsilon_i a_i\right)^p X\right]^{\varepsilon_1}$$

then there exists $u \in \mathbb{Z}_p^{\mathrm{ur}}$; $Q(X), R(X), S(X), T(X) \in \mathbb{Z}_p^{\mathrm{ur}}[X]$ *and* $m_n = p^{n-1}(p-1)-1$ *such that*

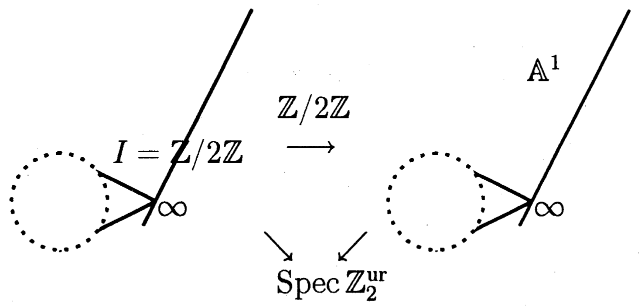
$$P(X) = (1 + XQ(X))^p + u^p X^{m_n}(1 + XR(X)) + pX^{(m_n+1)/p}S(X) + p^2T(X).$$

Moreover there are infinitely many choices of a_i *such that the p-cyclic cover of* $\mathbb{P}^1$ *defined by the equation* $Y^p = P(X)$ *has potentially good reduction at p relatively to the S-Gauss valuation for* $S := \lambda^{-p/m_n}X$ *and mod* π *induces an étale cover of* $\mathbb{P}^1$ *with conductor* $m_n + 1$ *at* ∞*. In particular the morphism at the level of formal fibre at* ∞ *induces an order p-automorphism of the open disc with* $m_n + 1$ *fix points. Hurwitz datas are* $\{1\ (p^n\ times), 2\ (p^n\ times), ..., p-1\ (p^n\ times)\}$ *and the tree as considered in* c. *has only one projective line (i.e. the fix points are equidistant).*

5. An example with more than 1 component. Let $p = 2$ and consider the elliptic curve $Y^2 = X(X-1)(X-\rho)$. For $|2|^4 < |\rho| < 1$,

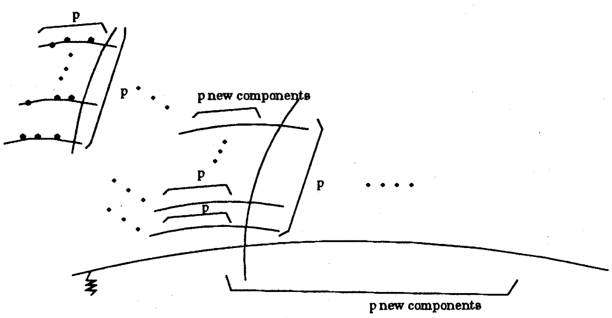
$$|j(\rho)| = \left|\frac{2^8(\rho^2 - \rho + 1)^3}{\rho^2(\rho - 1)^2}\right| < 1,$$

so the curve has potentially good reduction which is supersingular *i.e.* a 2-étale cover of $\mathbb{A}^1$.



So it induces an order 2-automorphism of the open disc.

6. Order p automorphism witout inertia at π naturally also occur when considering endomorphisms of the so called Lubin-Tate formal groups (see [G-M 2] II.3.3.3). The number of fix points is a power of p and the Hurwitz datas are $(1, 1, ..., 1)$. The geometry of tree is that of a tree of valence p.



Oriented tree $\mathcal{D}_s^0$

Along the same line one can give order p^n automorphism without inertia at π and in this way we prove the cyclic p-groups have the Inverse Galois type property (see lecture I).

II. Order p-automorphisms

Let σ be an order p-automorphism with $F_\sigma \neq \emptyset$. Consider the morphism $f : \mathcal{D}^o \longrightarrow \mathcal{D}^o/\langle\sigma\rangle$. From the unicity of $\mathcal{D}^o$ it follows that σ is the identity on each irreducible component of $\mathcal{D}^o_s$ and so $f_s : \mathcal{D}^o_s \longrightarrow (\mathcal{D}^o/\langle\sigma\rangle)_s$ is an homeomorphism.

The first qualitative result is

Theorem([G-M2]). *The fix points in F_σ specialize in the terminal components.*

Proof. Say $Z_i = 0 \in F_\sigma$ is a fix point. Let $D^c(0,\rho)$ be the closed disc inside $D^o_{(K)}$ centered in 0 and ray $v(\rho)$. Let v_ρ be the Gauss-valuation relative to $\frac{Z}{\rho}$, it defines a p-cyclic valued field extension $\mathrm{Fr}R[[Z]]/\mathrm{Fr}R[[Z]]^{\langle\sigma\rangle}$ which is residually purely inseparable, moreover the valuation ring is monogenic generated by $\frac{Z}{\rho}$. Let $d(v(\rho))$ be the degree of the different in this valued extension. Then

$$d(v(\rho)) = (p-1)v_\rho(\frac{\sigma(Z)}{Z} - 1)$$

if $\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots)$; then

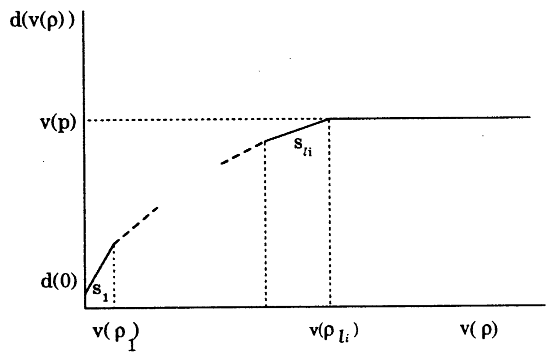
$$d(v(\rho)) = (p-1)\inf_{n\geq 0}\{v(\zeta - 1), v(a_n) + nv(\rho)\} \leq v(p)$$

and

$$\frac{\sigma(Z)}{Z} - 1 = \prod_{\substack{Z_j \neq 0 \\ Z_j \in F_\sigma}} (Z - Z_j)U(Z)$$

where $U(Z)$ is an unit.

We get the graph of $d(v(\rho))$.



$s_1 = \text{gradient} = (p-1)m$
$\rho_{\ell_i} = \inf_{Z_j \in F_\sigma} v(Z_i - Z_j)$

Now consider an other fixed point Z_j. We remark that for $v(\rho) \le v(Z_i - Z_j)$ one has

$$v_\rho(\frac{\sigma(Z) - Z}{Z}) = v_\rho(\frac{\sigma(Z - Z_j) - (Z - Z_j)}{Z - Z_j}),$$

so the graphs of different centered in Z_i on Z_j coincide for $v(\rho) \le v(Z_i - Z_j)$.

As the value of the different in ρ_{l_i} is $v(p)$, it follows that $\rho_{l_i} = \rho_{l_j}$ for Z_j in the first neighborhood of Z_i, *i.e.* the points in the first neighborhood of Z_i are equidistant.

Now in order to get information the trick is to look at equations induced by σ and to compare formulas for the different with the previous one.

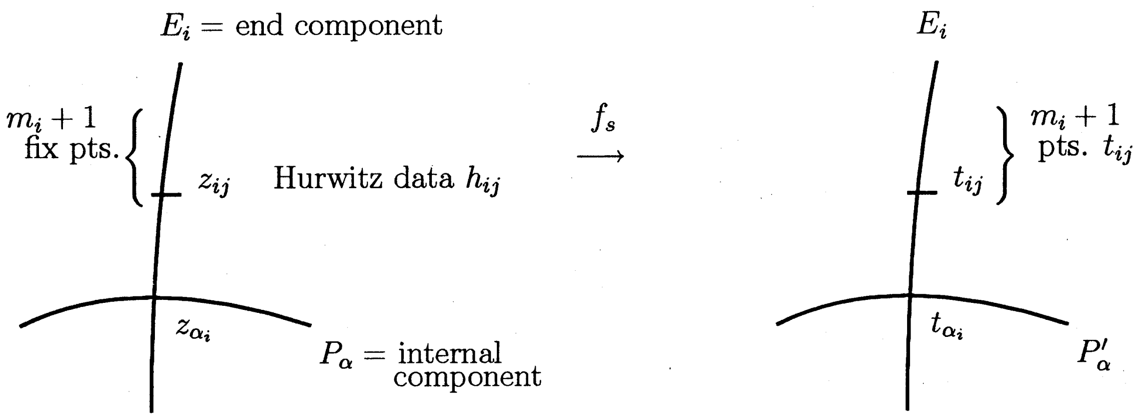
Theorem[G-M2]). *Let $X^p = \prod_{i,j}(T - T_{ij})^{n_{ij}}u$ (where u is a unit, $(n_{ij}, p) = 1$) be a μ_p-torsor of the punctured closed disc $D^c - \{T_{ij}\}$. We assume that $V(\pi) \subset$ (Branch locus). Two cases can occur.*

1-st case. *$\bar{u}$ is not a p-power then it is defined up to multiplication by a p-power. Moreover the equation gives an étale equation outside the branch locus which mod π gives the equation of the reduction component which is smooth outside the specialization of branch points. Moreover v(different) $= v(\rho)$ and $\omega = d\bar{u}$ is defined up to multiplication by p-powers.*

2-nd case. *$\bar{u}$ is a p-power then after a transformation one gets a new equation $X^p = 1 + \pi^{p^t}u$ where $\bar{u}$ is not a p-power; the irreducible polynomial of $\frac{X-1}{\pi^t}$ gives the integral model and in reduction this model gives the equation of the reduction component which is smooth outside the specialization of branch points and the different $v(diff) = v(\rho) - (p-1)t < v(p)$ and $\omega = d\bar{u}$ is uniquely defined.*

We then apply the Theorem to the closed discs which correspond to the irreducible components in $\mathcal{D}_s^o$.

The result is as follows: For simplification sake we assume that P_α is an internal component meeting only one other internal component.



End components E_i correspond to the first case above (μ_p-type degeneration), there is $\overline{u_i}$ such that $X^p = \overline{u_i}$ defines a smooth curve outside Z_{ij} and ∞ so $support(d\bar{u}_i) \subset \{t_{ij}, \infty\}$, moreover

$$\mathrm{ord}_{t_{ij}}\omega_i \equiv h_{ij} - 1 \bmod p$$

and

$$\mathrm{ord}_{\infty_i = t_{\alpha_i}}\omega_i = m_i - 1.$$

Internal component correspond to the second case (α_p-type degeneration). Let $\omega_\alpha = d\bar{u_\alpha}$ be the corresponding differential then $ord_{t_{\alpha_i}}\omega_\alpha = -(m_i + 1)$ (this is a crucial part, the trick consists in comparing the gradient of the different obtained on one side from the graph $d(v(\rho))$ and on the other side by deforming the ray of the closed disc in second part of the theorem above).

It follows that

$$\mathrm{ord}_\infty \omega_\alpha = -2 + \sum_i m_i + 1.$$

A first noticeable application is

Theorem([G-M2]). *Let σ an order p-automorphism and assume $|F_\sigma| = m + 1 \geq 2$ and $m < p$, then the points in F_σ are equidistant i.e. D_s^o has only one irreducible component.*

Proof. If we had more than one component then concider a path of maximal length in the tree it ends as in the example above. Now we remark that the function $\bar{u_\alpha}$ defines a finite cover $\mathbb{P}^1 \longrightarrow \mathbb{P}^1$ which is étale outside ∞ and 0 (it is ramified above ∞ in t_{α_i} with order $m_i < p$ so tamely ramified and above 0 in ∞ with order $-1 + \sum(m_i + 1) \leq -1 + m + 1 < p$), so we get a tame cover of $\mathbb{P}^1 - \{0, \infty\}$ so it is as in characteristic 0 totally ramified and cyclic so $\bar{u_\alpha}$ has only one pole; this contradicts the minimality of D^o.

Moreover the coordinates of the specialization of the points in F_σ satisfy the following equations;

$$\begin{cases} h_0 + \cdots + h_m = 0 \\ h_0 t_0 + \cdots + h_m t_m = 0 \\ \cdots\cdots \\ h_0 t_0^{m-1} + \cdots + h_m t_m^{m-1} = 0 \end{cases}$$

and

$$\prod (t_i - t_j) \neq 0.$$

In particular for fixed t_0,t_1 there are only a finite number of solutions; this is the first step to prove:

Theorem([G-M2]). *Assume* $1 \leq m+1 \leq p$ *then there are only a finite number of conjugacy classes of order p-automorphism without inertia at* π *with* $m+1$ *fix points.*

A representative system occurs when considering the p-cyclic cover of $\mathbb{P}^1$ (which has potentially good reduction an *é*tale cover of $\mathbb{A}^1$ with conductor $m+1$ at ∞)

$$Y^n = \prod (1 - T_i X)^{h_i}$$

where T_i are solutions in $\mathbb{Z}_p^{\mathrm{ur}}$ of the system of equations

$$\begin{cases} h_0 T_0 + \cdots + h_m T_m = 0 \\ \cdots\cdots \\ h_0 T_0^{m-1} + \cdots + h_m T_m^{m-1} = 0. \end{cases}$$

IV. References

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

[G-M 2] B. Green, M. Matignon, *Order p automorphisms of the open disc of a p-adic field*, Journal of AMS, to appear.

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

[M] M. Matignon,*p-groupes abéliens de type* $(p, ..., p)$ *et disques ouverts p-adiques*, Prépublication 83 (1998), Laboratoire de Mathématiques pures de Bordeaux.