p-adic dynamical systems of finite order

Michel Matignon

Institut of Mathematics, University Bordeaux 1

ANR Berko

Abstract

In this lecture we intend to study the finite subgroups of the group $\mathrm{Aut}_R\, R[[Z]]$ of R-automorphisms of the formal power series ring $R[[Z]]$.

Notations

(K, v) is a discretely valued complete field of inequal characteristic $(0, p)$. Typically a finite extension of $\mathbb{Q}_p^{unr}$.

R denotes its valuation ring.

π is a uniformizing element and $v(\pi) = 1$.

$k := R/\pi R$,the residue field, is algebraically closed of char. $p > 0$

(K^{alg}, v) is a fixed algebraic closure endowed with the unique prolongation of the valuation v.

ζ_p is a primitive p-th root of 1 and $\lambda = \zeta_p - 1$ is a uniformizing element of $\mathbb{Q}_p(\zeta_p)$.

Introduction

Let us cite J. Lubin (Non archimedean dynamical sytems. Compositio 94).

” Some of the standard and well-established techniques of local arithmetic geometry can also be seen as involving dynamical systems.

Introduction

Let us cite J. Lubin (Non archimedean dynamical sytems. Compositio 94).

” Some of the standard and well-established techniques of local arithmetic geometry can also be seen as involving dynamical systems.
Let $K/\mathbb{Q}_p$ be a finite extension. For a particular formal group F (the so called Lubin-Tate formal groups) we get a representation of $\mathrm{Gal}(K^{alg}/K)$ from the torsion points of a particular formal group F over R the valuation ring of K.

Introduction

Let us cite J. Lubin (Non archimedean dynamical sytems. Compositio 94).

" Some of the standard and well-established techniques of local arithmetic geometry can also be seen as involving dynamical systems.
Let $K/\mathbb{Q}_p$ be a finite extension. For a particular formal group F (the so called Lubin-Tate formal groups) we get a representation of $\mathrm{Gal}(K^{alg}/K)$ from the torsion points of a particular formal group F over R the valuation ring of K.
They occur as the roots of the iterates of $[p]_F(X) = pX + ...$, the endomorphism of multiplication by p.

Introduction

Let us cite J. Lubin (Non archimedean dynamical sytems. Compositio 94).

” Some of the standard and well-established techniques of local arithmetic geometry can also be seen as involving dynamical systems.
Let $K/\mathbb{Q}_p$ be a finite extension. For a particular formal group F (the so called Lubin-Tate formal groups) we get a representation of $\mathrm{Gal}(K^{alg}/K)$ from the torsion points of a particular formal group F over R the valuation ring of K.
They occur as the roots of the iterates of $[p]_F(X) = pX + ...$, the endomorphism of multiplication by p.
They occur aswell as the fix points of the automorphism (of formal group) given by $[1+p]_F(X) = F(X, [p]_F(X)) = (1+p)X + ...$”

Introduction

Let us cite J. Lubin (Non archimedean dynamical sytems. Compositio 94).

" Some of the standard and well-established techniques of local arithmetic geometry can also be seen as involving dynamical systems.
Let $K/\mathbb{Q}_p$ be a finite extension. For a particular formal group F (the so called Lubin-Tate formal groups) we get a representation of $\mathrm{Gal}(K^{alg}/K)$ from the torsion points of a particular formal group F over R the valuation ring of K.
They occur as the roots of the iterates of $[p]_F(X) = pX + ...$, the endomorphism of multiplication by p.
They occur aswell as the fix points of the automorphism (of formal group) given by $[1+p]_F(X) = F(X,[p]_F(X)) = (1+p)X + ...$"
In these lectures we focuss our attention on power series $f(Z) \in R[[Z]]$ such that $f(0) \in \pi R$ and $f^{\circ n}(Z) = Z$ for some $n > 0$.

Introduction

Let us cite J. Lubin (Non archimedean dynamical sytems. Compositio 94).

" Some of the standard and well-established techniques of local arithmetic geometry can also be seen as involving dynamical systems.
Let $K/\mathbb{Q}_p$ be a finite extension. For a particular formal group F (the so called Lubin-Tate formal groups) we get a representation of $\mathrm{Gal}(K^{alg}/K)$ from the torsion points of a particular formal group F over R the valuation ring of K.
They occur as the roots of the iterates of $[p]_F(X) = pX + ...$, the endomorphism of multiplication by p.
They occur aswell as the fix points of the automorphism (of formal group) given by $[1+p]_F(X) = F(X, [p]_F(X)) = (1+p)X + ...$"
In these lectures we focuss our attention on power series $f(Z) \in R[[Z]]$ such that $f(0) \in \pi R$ and $f^{\circ n}(Z) = Z$ for some $n > 0$. This is the same as considering cyclic subgroups of $\mathrm{Aut}_R R[[Z]]$.

Introduction

Let us cite J. Lubin (Non archimedean dynamical sytems. Compositio 94).

” Some of the standard and well-established techniques of local arithmetic geometry can also be seen as involving dynamical systems.
Let $K/\mathbb{Q}_p$ be a finite extension. For a particular formal group F (the so called Lubin-Tate formal groups) we get a representation of $\mathrm{Gal}(K^{alg}/K)$ from the torsion points of a particular formal group F over R the valuation ring of K.
They occur as the roots of the iterates of $[p]_F(X) = pX + \ldots$, the endomorphism of multiplication by p.
They occur aswell as the fix points of the automorphism (of formal group) given by $[1+p]_F(X) = F(X, [p]_F(X)) = (1+p)X + \ldots$.”
In these lectures we focuss our attention on power series $f(Z) \in R[[Z]]$ such that $f(0) \in \pi R$ and $f^{\circ n}(Z) = Z$ for some $n > 0$. This is the same as considering cyclic subgroups of $\mathrm{Aut}_R R[[Z]]$. More generally we study finite order subgroups of the group $\mathrm{Aut}_R R[[Z]]$ throughout their occurence in ”arithmetic geometry”.

Generalities

The ring $R[[Z]]$

Generalities

The ring $R[[Z]]$

Definition

Distinguished polynomials. $P(Z) \in R[Z]$ is said to be distinguished if $P(Z) = Z^n + a_{n-1}Z^{n-1} + \ldots + a_0$, $a_i \in \pi R$

Generalities

The ring $R[[Z]]$

Definition

Distinguished polynomials. $P(Z) \in R[Z]$ is said to be distinguished if $P(Z) = Z^n + a_{n-1}Z^{n-1} + \ldots + a_0$, $a_i \in \pi R$

Theorem

Weierstrass preparation theorem. Let $f(Z) = \sum_{i\geq 0} a_i Z^i \in R[[Z]]$ $a_i \in \pi R$ *for* $0 \leq i \leq n-1$. $a_n \in R^\times$. *The integer* n *is the Weierstrass degree for* f.

Generalities

The ring $R[[Z]]$

Definition

Distinguished polynomials. $P(Z) \in R[Z]$ is said to be distinguished if $P(Z) = Z^n + a_{n-1}Z^{n-1} + \ldots + a_0$, $a_i \in \pi R$

Theorem

Weierstrass preparation theorem. Let $f(Z) = \sum_{i \geq 0} a_i Z^i \in R[[Z]]$ $a_i \in \pi R$ *for* $0 \leq i \leq n-1$. $a_n \in R^\times$. *The integer n is the Weierstrass degree for f.* *Then* $f(Z) = P(Z)U(Z)$ *where* $U(Z) \in R[[Z]]^\times$ *and* $P(Z)$ *is distinguished of degree n are uniquely defined.*

Generalities

The ring $R[[Z]]$

Definition

Distinguished polynomials. $P(Z) \in R[Z]$ is said to be distinguished if $P(Z) = Z^n + a_{n-1}Z^{n-1} + \ldots + a_0$, $a_i \in \pi R$

Theorem

Weierstrass preparation theorem. Let $f(Z) = \sum_{i\geq 0} a_i Z^i \in R[[Z]]$ $a_i \in \pi R$ *for* $0 \leq i \leq n-1$. $a_n \in R^\times$. *The integer n is the Weierstrass degree for f.* *Then* $f(Z) = P(Z)U(Z)$ *where* $U(Z) \in R[[Z]]^\times$ *and* $P(Z)$ *is distinguished of degree n are uniquely defined.*

Lemma

Division lemma. $f, g \in R[[Z]]$ $f(Z) = \sum_{i\geq 0} a_i Z^i \in R[[Z]]$ $a_i \in \pi R$ *for* $0 \leq i \leq n-1$. $a_n \in R^\times$ *There is a unique* $(q, r) \in R[[Z]] \times R[Z]$ *with* $g = qf + r$

Open disc

Let $X := \operatorname{Spec} R[[Z]]$.

Open disc

Let $X := \operatorname{Spec} R[[Z]]$.

Closed fiber $X_s := X \times_R k = \operatorname{Spec} k[[Z]]$: two points generic point (π) and closed point (π, Z)

Open disc

Let $X := \operatorname{Spec} R[[Z]]$.

Closed fiber $X_s := X \times_R k = \operatorname{Spec} k[[Z]]$: two points generic point (π) and closed point (π, Z)

Generic fiber $X_K := X \times_R K = \operatorname{Spec} R[[Z]] \otimes_R K$.
Note that $R[[Z]] \otimes_R K = \{\sum_i a_i Z^i \in K[[Z]] \mid \inf_i v(a_i) > -\infty\}$.

Open disc

Let $X := \operatorname{Spec} R[[Z]]$.

Closed fiber $X_s := X \times_R k = \operatorname{Spec} k[[Z]]$: two points generic point (π) and closed point (π, Z)

Generic fiber $X_K := X \times_R K = \operatorname{Spec} R[[Z]] \otimes_R K$.
Note that $R[[Z]] \otimes_R K = \{\sum_i a_i Z^i \in K[[Z]] \mid \inf_i v(a_i) > -\infty\}$.

generic point (0) and closed points $(P(Z))$ where $P(Z)$ is an irreducible distinguished polynomial.

Open disc

Let $X := \operatorname{Spec} R[[Z]]$.

Closed fiber $X_s := X \times_R k = \operatorname{Spec} k[[Z]]$: two points generic point (π) and closed point (π, Z)

Generic fiber $X_K := X \times_R K = \operatorname{Spec} R[[Z]] \otimes_R K$.
Note that $R[[Z]] \otimes_R K = \{\sum_i a_i Z^i \in K[[Z]] \mid \inf_i v(a_i) > -\infty\}$.

generic point (0) and closed points $(P(Z))$ where $P(Z)$ is an irreducible distinguished polynomial.

$X_{(K^{alg})} \simeq \{z \in K^{alg} \mid v(z) > 0\}$ is the open disc in K^{alg} so that we can identify $X_K = R[[Z]] \otimes_R K$ with $\frac{X_{(K^{alg})}}{\operatorname{Gal}(K^{alg}/K)}$.

Open disc

Let $X := \operatorname{Spec} R[[Z]]$.

Closed fiber $X_s := X \times_R k = \operatorname{Spec} k[[Z]]$: two points generic point (π) and closed point (π, Z)

Generic fiber $X_K := X \times_R K = \operatorname{Spec} R[[Z]] \otimes_R K$.
Note that $R[[Z]] \otimes_R K = \{\sum_i a_i Z^i \in K[[Z]] \mid \inf_i v(a_i) > -\infty\}$.

generic point (0) and closed points $(P(Z))$ where $P(Z)$ is an irreducible distinguished polynomial.

$X_{(K^{alg})} \simeq \{z \in K^{alg} \mid v(z) > 0\}$ is the open disc in K^{alg} so that we can identify $X_K = R[[Z]] \otimes_R K$ with $\frac{X_{(K^{alg})}}{\operatorname{Gal}(K^{alg}/K)}$.

Although $X = \operatorname{Spec} R[[Z]]$ is a minimal regular model for X_K we call it the open disc over K.

$\mathrm{Aut}_R R[[Z]]$

Let $\sigma \in \mathrm{Aut}_R R[[Z]]$ then

- σ is continuous for the (π, Z) topology.
- $(\pi, Z) = (\pi, \sigma(Z))$
- $R[[Z]] = R[[\sigma(Z)]]$
- Reciprocally if $Z' \in R[[Z]]$ and $(\pi, Z) = (\pi, Z')$ i.e. $Z' \in \pi R + ZR[[Z]]^{\times}$, then $\sigma(Z) = Z'$ defines an element $\sigma \in \mathrm{Aut}_R R[[Z]]$
- σ induces a bijection $\tilde{\sigma} : \pi R \to \pi R$ where $\tilde{\sigma}(z) := (\sigma(Z))_{Z=z}$
- $\tilde{\tau\sigma}(z) = \tilde{\sigma}(\tilde{\tau}(z))$.

Structure theorem

Let $r: R[[Z]] \to R/(\pi)[[z]]$, be the canonical homomorphism induced by the reduction mod π.
It induces a surjective homomorphism $r : \mathrm{Aut}_R R[[Z]] \to \mathrm{Aut}_k k[[Z]]$.
$N := \ker r = \{\sigma \in \mathrm{Aut}_R R[[Z]] \mid \sigma(Z) = Z \mod \pi\}$.

Proposition

Let $G \subset \mathrm{Aut}_R R[[Z]]$ be a subgroup with $|G| < \infty$, then G contains a unique p-Sylow subgroup G_p and C a cyclic subgroup of order e prime to p with $G = G_p \rtimes C$. Moreover there is a parameter Z' of the open disc such that $C =< \sigma >$ where $\sigma(Z') = \zeta_e Z'$.

The proof uses several elementary lemmas

Lemma

- *Let* $e \in \mathbb{N}^{\times}$ *and* $f(Z) \in \mathrm{Aut}_R R[[Z]]$ *of order* e *and* $f(Z) = Z \mod Z^2$ *and then* $e = 1$.

The proof uses several elementary lemmas

Lemma

- *Let* $e \in \mathbb{N}^{\times}$ *and* $f(Z) \in \mathrm{Aut}_R R[[Z]]$ *of order* e *and* $f(Z) = Z \mod Z^2$ *and then* $e = 1$.
- *Let* $f(Z) = a_0 + a_1 Z + \dots \in R[[Z]]$ *with* $a_0 \in \pi R$ *and for some* $e \in \mathbb{N}*$ *let* $f^{\circ e}(Z) = b_0 + b_1 Z + \dots$*, then* $b_0 = a_0(1 + a_1 + \dots . + a_1^{e-1}) \mod a_0^2 R$ *and* $b_1 = a_1^e \mod a_0 R$.

The proof uses several elementary lemmas

Lemma

- *Let* $e \in \mathbb{N}^{\times}$ *and* $f(Z) \in \mathrm{Aut}_R R[[Z]]$ *of order* e *and* $f(Z) = Z \mod Z^2$ *and then* $e = 1$.
- *Let* $f(Z) = a_0 + a_1 Z + \ldots \in R[[Z]]$ *with* $a_0 \in \pi R$ *and for some* $e \in \mathbb{N}*$ *let* $f^{\circ e}(Z) = b_0 + b_1 Z + \ldots$, *then* $b_0 = a_0(1 + a_1 + \ldots. + a_1^{e-1}) \mod a_0^2 R$ *and* $b_1 = a_1^e \mod a_0 R$.
- *Let* $\sigma \in \mathrm{Aut}_R R[[Z]]$ *with* $\sigma^e = Id$ *and* $(e,p) = 1$ *then* σ *has a rational fix point.*

The proof uses several elementary lemmas

Lemma

- *Let* $e \in \mathbb{N}^{\times}$ *and* $f(Z) \in \mathrm{Aut}_R R[[Z]]$ *of order* e *and* $f(Z) = Z \mod Z^2$ *and then* $e = 1$.
- *Let* $f(Z) = a_0 + a_1 Z + \ldots \in R[[Z]]$ *with* $a_0 \in \pi R$ *and for some* $e \in \mathbb{N}*$ *let* $f^{\circ e}(Z) = b_0 + b_1 Z + \ldots$, *then* $b_0 = a_0(1 + a_1 + \ldots. + a_1^{e-1}) \mod a_0^2 R$ *and* $b_1 = a_1^e \mod a_0 R$.
- *Let* $\sigma \in \mathrm{Aut}_R R[[Z]]$ *with* $\sigma^e = Id$ *and* $(e, p) = 1$ *then* σ *has a rational fix point.*
- *Let* σ *as above then* σ *is linearizable.*

Proof

The case $|G| = e$ is prime to p.

Proof

The case $|G| = e$ is prime to p.

Claim. $G =< \sigma >$ and there is Z' a parameter of the open disc such that $\sigma(Z') = \theta Z'$ for θ a primitive e-th root of 1.In other words σ is linearizable.

Proof

The case $|G| = e$ is prime to p.

Claim. $G =< \sigma >$ and there is Z' a parameter of the open disc such that $\sigma(Z') = \theta Z'$ for θ a primitive e-th root of 1.In other words σ is linearizable.

$N \cap G = \{1\}$. By item 4, $\sigma \in G$ is linearisable and so for some parameter Z' one can write $\sigma(Z') = \theta Z'$ and if $\sigma \in N$ we have $\sigma(Z) = Z \mod \pi R$, and as $(e,p) = 1$ it follows that $\sigma = Id$.

Proof

The case $|G| = e$ is prime to p.

Claim. $G =< \sigma >$ and there is Z' a parameter of the open disc such that $\sigma(Z') = \theta Z'$ for θ a primitive e-th root of 1.In other words σ is linearizable.

$N \cap G = \{1\}$. By item 4, $\sigma \in G$ is linearisable and so for some parameter Z' one can write $\sigma(Z') = \theta Z'$ and if $\sigma \in N$ we have $\sigma(Z) = Z \mod \pi R$, and as $(e,p) = 1$ it follows that $\sigma = Id$.

The homomorphism $\varphi : G \to k^\times$ with $\varphi(\sigma) = \frac{r(\sigma)(z)}{z}$ is injective (apply item 1 to the ring $R = k$).
The result follows.

General case.

General case.

From the first part it follows that $N \cap G$ is a p-group.

General case.

From the first part it follows that $N \cap G$ is a p-group.

Let $\overline{G} := r(G)$. This is a finite group in $\mathrm{Aut}_k\, k[[z]]$.

General case.

From the first part it follows that $N \cap G$ is a p-group.

Let $\overline{G} := r(G)$. This is a finite group in $\mathrm{Aut}_k\, k[[z]]$.

Let $\overline{G}_1 := \ker(\varphi : \overline{G} \to k^{\times})$ given by $\varphi(\sigma) = \frac{\sigma(z)}{z}$

General case.

From the first part it follows that $N \cap G$ is a p-group.

Let $\overline{G} := r(G)$. This is a finite group in $\mathrm{Aut}_k\, k[[z]]$.

Let $\overline{G}_1 := \ker(\varphi : \overline{G} \to k^\times)$ given by $\varphi(\sigma) = \frac{\sigma(z)}{z}$

this is the p-Sylow subgroup of $\overline{G}$.

General case.

From the first part it follows that $N \cap G$ is a p-group.

Let $\overline{G} := r(G)$. This is a finite group in $\mathrm{Aut}_k\, k[[z]]$.

Let $\overline{G}_1 := \ker(\varphi : \overline{G} \to k^{\times})$ given by $\varphi(\sigma) = \frac{\sigma(z)}{z}$

this is the p-Sylow subgroup of $\overline{G}$.

In particular $\frac{\overline{G}}{\overline{G}_1}$ is cyclic of order e prime to p.

General case.

From the first part it follows that $N \cap G$ is a p-group.

Let $\overline{G} := r(G)$. This is a finite group in $\mathrm{Aut}_k\, k[[z]]$.

Let $\overline{G}_1 := \ker(\varphi : \overline{G} \to k^\times)$ given by $\varphi(\sigma) = \frac{\sigma(z)}{z}$

this is the p-Sylow subgroup of $\overline{G}$.

In particular $\frac{\overline{G}}{\overline{G}_1}$ is cyclic of order e prime to p.

Let $G_p := r^{-1}(\overline{G}_1)$, this is the unique p-Sylow subgroup of G as $N \cap G$ is a p-group.

General case.

From the first part it follows that $N \cap G$ is a p-group.

Let $\overline{G} := r(G)$. This is a finite group in $\mathrm{Aut}_k\, k[[z]]$.

Let $\overline{G}_1 := \ker(\varphi : \overline{G} \to k^\times)$ given by $\varphi(\sigma) = \frac{\sigma(z)}{z}$

this is the p-Sylow subgroup of $\overline{G}$.

In particular $\frac{\overline{G}}{\overline{G}_1}$ is cyclic of order e prime to p.

Let $G_p := r^{-1}(\overline{G}_1)$, this is the unique p-Sylow subgroup of G as $N \cap G$ is a p-group.

Now we have an exact sequence $1 \to G_p \to G \to \frac{\overline{G}}{\overline{G}_1} \simeq \mathbb{Z}/e\mathbb{Z} \to 1$. The result follows by Hall's theorem.

Remark.

Let G be any finite p-group.

Remark.

Let G be any finite p-group.

There is a dvr, R which is finite over $\mathbb{Z}_p$ and an injective morphism $G \to \mathrm{Aut}_R R[[Z]]$ which induces a free action of G on $\mathrm{Spec}\, R[[Z]] \times K$ and which is the identity modulo π.

Remark.

Let G be any finite p-group.

There is a dvr, R which is finite over $\mathbb{Z}_p$ and an injective morphism $G \to \mathrm{Aut}_R R[[Z]]$ which induces a free action of G on $\mathrm{Spec}\, R[[Z]] \times K$ and which is the identity modulo π.

In particular the extension of dvr
$R[[Z]]_{(\pi)}/R[[Z]]^G_{(\pi)}$
is fiercely ramified.

The local lifting problem

Let G be a finite p-group. The group G occurs as an automorphism group of $k[[z]]$ in many ways.

The local lifting problem

Let G be a finite p-group. The group G occurs as an automorphism group of $k[[z]]$ in many ways.

This is a consequence of the Witt-Shafarevich theorem on the structure of the Galois group of a field K of characteristic $p > 0$.

The local lifting problem

Let G be a finite p-group. The group G occurs as an automorphism group of $k[[z]]$ in many ways.

This is a consequence of the Witt-Shafarevich theorem on the structure of the Galois group of a field K of characteristic $p > 0$.

This theorem asserts that the Galois group $I_p(K)$ of its maximal p-extension is pro-p free on $|K/\wp(K)|$ elements (as usual $\wp$ is the operator Frobenius minus identity).

The local lifting problem

Let G be a finite p-group. The group G occurs as an automorphism group of $k[[z]]$ in many ways.

This is a consequence of the Witt-Shafarevich theorem on the structure of the Galois group of a field K of characteristic $p > 0$.

This theorem asserts that the Galois group $I_p(K)$ of its maximal p-extension is pro-p free on $|K/\wp(K)|$ elements (as usual $\wp$ is the operator Frobenius minus identity).

We apply this theorem to the power series field $K = k((t))$. Then $K/\wp(K)$ is infinite so we can realize G in infinitely many ways as a quotient of I_p and so as Galois group of a Galois extension L/K.

The local lifting problem

Let G be a finite p-group. The group G occurs as an automorphism group of $k[[z]]$ in many ways.

This is a consequence of the Witt-Shafarevich theorem on the structure of the Galois group of a field K of characteristic $p > 0$.

This theorem asserts that the Galois group $I_p(K)$ of its maximal p-extension is pro-p free on $|K/\wp(K)|$ elements (as usual $\wp$ is the operator Frobenius minus identity).

We apply this theorem to the power series field $K = k((t))$. Then $K/\wp(K)$ is infinite so we can realize G in infinitely many ways as a quotient of I_p and so as Galois group of a Galois extension L/K.

The local field L can be uniformized: namely $L = k((z))$. If $\sigma \in G = \mathrm{Gal}(L/K)$, then σ is an isometry of (L, v) and so G is a group of k-automorphisms of $k[[z]]$ with fixed ring $k[[z]]^G = k[[t]]$.

Definition

The local lifting problem for a finite p-group action $G \subset \mathrm{Aut}_k\, k[[z]]$ is to find a dvr, R finite over $W(k)$ and a commutative diagram

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

A p-group G has the local lifting property if the local lifting problem for all actions $G \subset \mathrm{Aut}_k\, k[[z]]$ has a positive answer.

Inverse Galois local lifting problem for p-groups

Let G be a finite p-group, we have seen that G occurs as a group of k-automorphism of $k[[z]]$ in many ways,

Inverse Galois local lifting problem for p-groups

Let G be a finite p-group, we have seen that G occurs as a group of k-automorphism of $k[[z]]$ in many ways,

so we can consider a weaker problem than the local lifting problem.

Inverse Galois local lifting problem for p-groups

Let G be a finite p-group, we have seen that G occurs as a group of k-automorphism of $k[[z]]$ in many ways,

so we can consider a weaker problem than the local lifting problem.

Definition

For a finite p-group G we say that G has the inverse Galois local lifting property if there exists a dvr, R finite over $W(k)$, a faithful action $i : G \to \mathrm{Aut}_k\, k[[z]]$ and a commutative diagram

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

Sen's theorem

Let $G_1(k) := zk[[z]]$ endowed with composition law. We write v for v_z. The following theorem was conjectured by Grothendieck.

Sen's theorem

Let $G_1(k) := zk[[z]]$ endowed with composition law. We write v for v_z.
The following theorem was conjectured by Grothendieck.

Theorem

Sen (1969). Let $f \in G_1(k)$ such that $f^{\circ p^n} \neq Id$. Let $i(n) := v(f^{\circ p^n}(z) - z)$, then $i(n) = i(n-1) \mod p^n$.

Sen's theorem

Let $G_1(k) := zk[[z]]$ endowed with composition law. We write v for v_z.
The following theorem was conjectured by Grothendieck.

Theorem

Sen (1969). Let $f \in G_1(k)$ such that $f^{\circ p^n} \neq Id$. Let $i(n) := v(f^{\circ p^n}(z) - z)$, then $i(n) = i(n-1) \mod p^n$.

Sketch proof (Lubin 95). The proof is interesting for us because it counts the fix points for the iterates of a power series which lifts f.

Sen's theorem

Let $G_1(k) := zk[[z]]$ endowed with composition law. We write v for v_z.
The following theorem was conjectured by Grothendieck.

Theorem

Sen (1969). Let $f \in G_1(k)$ such that $f^{\circ p^n} \neq Id$. Let $i(n) := v(f^{\circ p^n}(z) - z)$, then $i(n) = i(n-1) \mod p^n$.

Sketch proof (Lubin 95). The proof is interesting for us because it counts the fix points for the iterates of a power series which lifts f.

Let $X^{alg} := \{z \in K^{alg} \mid v(z) > 0\}$

Sen's theorem

Let $G_1(k) := zk[[z]]$ endowed with composition law. We write v for v_z.
The following theorem was conjectured by Grothendieck.

Theorem

Sen (1969). Let $f \in G_1(k)$ such that $f^{\circ p^n} \neq Id$. Let $i(n) := v(f^{\circ p^n}(z) - z)$, then $i(n) = i(n-1) \mod p^n$.

Sketch proof (Lubin 95). The proof is interesting for us because it counts the fix points for the iterates of a power series which lifts f.

Let $X^{alg} := \{z \in K^{alg} \mid v(z) > 0\}$

Let $F(Z) \in R[[Z]]$ such that

- $F(0) = 0$ and $F^{\circ p^n}(Z) \neq Z \mod \pi R$
- The roots of $F^{\circ p^n}(Z) - Z$ in X^{alg} are simple.

Then $\forall m$ such that $0 < m \leq n$ one has $i(m) = i(m-1) \mod p^m$ where $i(n) := v(\tilde{F}^{\circ p^n}(z) - z)$ is the Weierstrass degree of $F^{\circ p^n}(Z) - Z$.

Proof:

Claim: let $Q_m(Z) := \frac{F^{\circ p^n}(Z)-Z}{F^{\circ p^{n-1}}(Z)-Z} \in R[[Z]]$

Proof:

Claim: let $Q_m(Z) := \frac{F^{\circ p^n}(Z)-Z}{F^{\circ p^{n-1}}(Z)-Z} \in R[[Z]]$

For this we remark that if $F^{\circ p^{m-1}}(Z) - Z = (Z - z_0)^a V(Z)$ with $a > 1$ and $z_0 \in X^{alg}$, then $F^{\circ p^m}(Z) - Z = (Z - z_0)^a W(Z)$ i.e. the multiplicity of fix points increases in particular the roots of $F^{\circ p^{m-1}}(Z) - Z$ are simple as those of $F^{\circ p^n}(Z) - Z$.

Proof:

Claim: let $Q_m(Z) := \frac{F^{\circ p^n}(Z)-Z}{F^{\circ p^{n-1}}(Z)-Z} \in R[[Z]]$

For this we remark that if $F^{\circ p^{m-1}}(Z) - Z = (Z - z_0)^a V(Z)$ with $a > 1$ and $z_0 \in X^{alg}$, then $F^{\circ p^m}(Z) - Z = (Z - z_0)^a W(Z)$ i.e. the multiplicity of fix points increases in particular the roots of $F^{\circ p^{m-1}}(Z) - Z$ are simple as those of $F^{\circ p^n}(Z) - Z$.

It follows that the series $Q_i(Z)$ for $1 \leq i \leq n$ have distinct roots.

Proof:

Claim: let $Q_m(Z) := \frac{F^{\circ p^n}(Z)-Z}{F^{\circ p^{n-1}}(Z)-Z} \in R[[Z]]$

For this we remark that if $F^{\circ p^{m-1}}(Z) - Z = (Z - z_0)^a V(Z)$ with $a > 1$ and $z_0 \in X^{alg}$, then $F^{\circ p^m}(Z) - Z = (Z - z_0)^a W(Z)$ i.e. the multiplicity of fix points increases in particular the roots of $F^{\circ p^{m-1}}(Z) - Z$ are simple as those of $F^{\circ p^n}(Z) - Z$.

It follows that the series $Q_i(Z)$ for $1 \leq i \leq n$ have distinct roots.

Let z_0 with $Q_m(z_0) = 0$ then $z_0, F(z_0), \ldots, F^{\circ p^m - 1}(z_0)$ are distinct roots of $Q_m(Z)$.

Reversely if $|\{z_0, F(z_0), \dots, F^{\circ p^m - 1}(z_0)\}| = p^m$ and if $F^{\circ p^m}(z_0) = z_0$, then z_0 is a root of $Q_m(Z)$.

Reversely if $|\{z_0, F(z_0), \ldots, F^{\circ p^m - 1}(z_0)\}| = p^m$ and if $F^{\circ p^m}(z_0) = z_0$, then z_0 is a root of $Q_m(Z)$.

In other words z_0 is a root of $Q_m(Z)$ iff $|\operatorname{Orb} z_0| = p^m$.

Reversely if $|\{z_0, F(z_0), \dots, F^{\circ p^m - 1}(z_0)\}| = p^m$ and if $F^{\circ p^m}(z_0) = z_0$, then z_0 is a root of $Q_m(Z)$.

In other words z_0 is a root of $Q_m(Z)$ iff $|\operatorname{Orb} z_0| = p^m$.

It follows that the Weierstrass degree $i(m) - i(m-1)$ of $Q_m(Z)$ is $0 \mod p^m$. Now Sen's theorem follows from the following

Lemma

k be an algebraically closed field of char. $p > 0$

Reversely if $|\{z_0, F(z_0), \ldots, F^{\circ p^m - 1}(z_0)\}| = p^m$ and if $F^{\circ p^m}(z_0) = z_0$, then z_0 is a root of $Q_m(Z)$.

In other words z_0 is a root of $Q_m(Z)$ iff $|\operatorname{Orb} z_0| = p^m$.

It follows that the Weierstrass degree $i(m) - i(m-1)$ of $Q_m(Z)$ is $0 \mod p^m$. Now Sen's theorem follows from the following

Lemma

k be an algebraically closed field of char. $p > 0$
$f \in k[[z]]$ with $f(z) = z \mod (z^2)$, and $n > 0$ such that $f^{\circ p^n}(z) \neq z$.

Reversely if $|\{z_0, F(z_0), \dots, F^{\circ p^m - 1}(z_0)\}| = p^m$ and if $F^{\circ p^m}(z_0) = z_0$, then z_0 is a root of $Q_m(Z)$.

In other words z_0 is a root of $Q_m(Z)$ iff $|\mathrm{Orb}\, z_0| = p^m$.

It follows that the Weierstrass degree $i(m) - i(m-1)$ of $Q_m(Z)$ is $0 \mod p^m$. Now Sen's theorem follows from the following

Lemma

k be an algebraically closed field of char. $p > 0$
$f \in k[[z]]$ with $f(z) = z \mod (z^2)$, and $n > 0$ such that $f^{\circ p^n}(z) \neq z$.
There is a complete dvr R with

Reversely if $|\{z_0, F(z_0), \ldots, F^{\circ p^m - 1}(z_0)\}| = p^m$ and if $F^{\circ p^m}(z_0) = z_0$, then z_0 is a root of $Q_m(Z)$.

In other words z_0 is a root of $Q_m(Z)$ iff $|\operatorname{Orb} z_0| = p^m$.

It follows that the Weierstrass degree $i(m) - i(m-1)$ of $Q_m(Z)$ is $0 \mod p^m$. Now Sen's theorem follows from the following

Lemma

k be an algebraically closed field of char. $p > 0$
$f \in k[[z]]$ with $f(z) = z \mod (z^2)$, and $n > 0$ such that $f^{\circ p^n}(z) \neq z$.
There is a complete dvr R with
$\operatorname{char.} R > 0$ *and* $R/(\pi) = k$ *and*

Reversely if $|\{z_0, F(z_0), \dots, F^{\circ p^m - 1}(z_0)\}| = p^m$ and if $F^{\circ p^m}(z_0) = z_0$, then z_0 is a root of $Q_m(Z)$.

In other words z_0 is a root of $Q_m(Z)$ iff $|\operatorname{Orb} z_0| = p^m$.

It follows that the Weierstrass degree $i(m) - i(m-1)$ of $Q_m(Z)$ is $0 \mod p^m$. Now Sen's theorem follows from the following

Lemma

k be an algebraically closed field of char. $p > 0$
$f \in k[[z]]$ *with* $f(z) = z \mod (z^2)$, *and* $n > 0$ *such that* $f^{\circ p^n}(z) \neq z$.
There is a complete dvr R with
char. $R > 0$ *and* $R/(\pi) = k$ *and*
$F(Z) \in R[[Z]]$ *with* $r(F) = f$ *such that* $F^{\circ p^n}(Z) - Z$ *has simple roots in* X^{alg}.

Hasse-Arf theorem

Notations.

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.
There is a filtration $(G_i)_{i \geq -1}$ with $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.
There is a filtration $(G_i)_{i \geq -1}$ with $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$
$G = G_{-1} \supset G_0 \supset G_1 \ldots$

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.
There is a filtration $(G_i)_{i \geq -1}$ with $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$
$G = G_{-1} \supset G_0 \supset G_1 \ldots$
$G_i \lhd G$

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.
There is a filtration $(G_i)_{i\geq -1}$ with $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$
$G = G_{-1} \supset G_0 \supset G_1 \ldots$
$G_i \lhd G$
$G/G_0 \simeq \mathrm{Gal}(k_L/k_K)$

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.
There is a filtration $(G_i)_{i \geq -1}$ with $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$
$G = G_{-1} \supset G_0 \supset G_1 \dots$
$G_i \lhd G$
$G/G_0 \simeq \mathrm{Gal}(k_L/k_K)$
G/G_1 is cyclic with order prime to char. k_K

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.
There is a filtration $(G_i)_{i\geq -1}$ with $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$
$G = G_{-1} \supset G_0 \supset G_1 \ldots$
$G_i \lhd G$
$G/G_0 \simeq \mathrm{Gal}(k_L/k_K)$
G/G_1 is cyclic with order prime to char. k_K
If char. $k_K = 0$ the group G_1 is trivial

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.
There is a filtration $(G_i)_{i\geq -1}$ with $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$
$G = G_{-1} \supset G_0 \supset G_1 \ldots$
$G_i \lhd G$
$G/G_0 \simeq \mathrm{Gal}(k_L/k_K)$
G/G_1 is cyclic with order prime to char. k_K
If char. $k_K = 0$ the group G_1 is trivial
If char. $k_K = p$ the group G_1 is a p-group.

Hasse-Arf theorem

Notations.

O_K is a complete dvr with $K = \mathrm{Fr}\, O_K$.
L/K is a finite Galois extension with group G.
O_L is the integral closure of O_K.
π_K, π_L uniformizing elements, k_K, k_L the residue fields
The residual extension k_L/k_K is assumed to be separable.
There is a filtration $(G_i)_{i\geq -1}$ with $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$
$G = G_{-1} \supset G_0 \supset G_1 \dots$
$G_i \lhd G$
$G/G_0 \simeq \mathrm{Gal}(k_L/k_K)$
G/G_1 is cyclic with order prime to char. k_K
If char. $k_K = 0$ the group G_1 is trivial
If char. $k_K = p$ the group G_1 is a p-group.
G_i/G_{i+1} is a p elementary abelian group.

The different ideal $\mathscr{D}_{L/K} \subset O_L$.

The different ideal $\mathscr{D}_{L/K} \subset O_L$.

Under our hypothesis there is $z \in O_L$ such that $O_L = O_K[z]$, then $\mathscr{D}_{L/K} = (P'(z))$ where P is the irreducible polynomial of z over K.

The different ideal $\mathscr{D}_{L/K} \subset O_L$.
Under our hypothesis there is $z \in O_L$ such that $O_L = O_K[z]$, then $\mathscr{D}_{L/K} = (P'(z))$ where P is the irreducible polynomial of z over K.
It follows that $v_L(\mathscr{D}_{L/K}) = \sum_{i\geq 0}(|G_i| - 1)$

The different ideal $\mathscr{D}_{L/K} \subset O_L$.

Under our hypothesis there is $z \in O_L$ such that $O_L = O_K[z]$, then $\mathscr{D}_{L/K} = (P'(z))$ where P is the irreducible polynomial of z over K.

It follows that $v_L(\mathscr{D}_{L/K}) = \sum_{i \geq 0}(|G_i| - 1)$

Ramification jumps

The different ideal $\mathscr{D}_{L/K} \subset O_L$.
Under our hypothesis there is $z \in O_L$ such that $O_L = O_K[z]$, then $\mathscr{D}_{L/K} = (P'(z))$ where P is the irreducible polynomial of z over K.
It follows that $v_L(\mathscr{D}_{L/K}) = \sum_{i \geq 0}(|G_i| - 1)$

Ramification jumps
An integer $i \geq 1$ such that $G_i \neq G_{i+1}$ is a jump.

The different ideal $\mathscr{D}_{L/K} \subset O_L$.
Under our hypothesis there is $z \in O_L$ such that $O_L = O_K[z]$, then $\mathscr{D}_{L/K} = (P'(z))$ where P is the irreducible polynomial of z over K.
It follows that $v_L(\mathscr{D}_{L/K}) = \sum_{i \geq 0}(|G_i| - 1)$

Ramification jumps
An integer $i \geq 1$ such that $G_i \neq G_{i+1}$ is a jump.
Moreover if $G_t \neq G_{t+1} = 1$ then $i = t \mod p$.

The different ideal $\mathscr{D}_{L/K} \subset O_L$.
Under our hypothesis there is $z \in O_L$ such that $O_L = O_K[z]$, then $\mathscr{D}_{L/K} = (P'(z))$ where P is the irreducible polynomial of z over K.
It follows that $v_L(\mathscr{D}_{L/K}) = \sum_{i \geq 0}(|G_i| - 1)$
Ramification jumps
An integer $i \geq 1$ such that $G_i \neq G_{i+1}$ is a jump.
Moreover if $G_t \neq G_{t+1} = 1$ then $i = t \mod p$.

Sen's theorem implies Hasse-Arf theorem for power series.

Theorem

Hasse-Arf. Let $i \geq 1$ such that $G_i \neq G_{i+1}$ then $\varphi(i) := \frac{1}{|G_0|}(\sum_{0 \leq j \leq i} |G_j|)$ is an integer.

The different ideal $\mathscr{D}_{L/K} \subset O_L$.
Under our hypothesis there is $z \in O_L$ such that $O_L = O_K[z]$, then $\mathscr{D}_{L/K} = (P'(z))$ where P is the irreducible polynomial of z over K.
It follows that $v_L(\mathscr{D}_{L/K}) = \sum_{i \geq 0}(|G_i| - 1)$

Ramification jumps
An integer $i \geq 1$ such that $G_i \neq G_{i+1}$ is a jump.
Moreover if $G_t \neq G_{t+1} = 1$ then $i = t \mod p$.

Sen's theorem implies Hasse-Arf theorem for power series.

Theorem

Hasse-Arf. Let $i \geq 1$ such that $G_i \neq G_{i+1}$ then $\varphi(i) := \frac{1}{|G_0|}(\sum_{0 \leq j \leq i} |G_j|)$ is an integer.

Corollary

When G is a p-group which is abelian then for $s < t$ are two consecutive jumps $G_s \neq G_{s+1} = \ldots = G_t \neq G_{t+1}$ one has $s = t \mod (G : G_t)$.

Proposition

Let $G \subset \mathrm{Aut}_k\, k[[z]]$ *a finite group. Then* $k[[z]]^G = k[[t]]$ *and* $k((z))/k((t))$ *is Galois with group* G*.*

Proposition

Let $G \subset \mathrm{Aut}_k\, k[[z]]$ a finite group. Then $k[[z]]^G = k[[t]]$ and $k((z))/k((t))$ is Galois with group G.

Proof. This is a special case of the following theorem.

Theorem

Let A be an integral ring and $G \subset \mathrm{Aut}_A\, Z[[Z]]$ a finite subgroup then $A[[Z]]^G = A[[T]]$. Moreover $T := \prod_{g \in G} g(Z)$ works.

When A is a noetherian complete integral local ring the result is due to Samuel.

The local lifting problem for $G \simeq \mathbb{Z}/p\mathbb{Z}$

Proposition

Let k be an algebraically closed of char. $p > 0$. *Let* $\sigma \in \mathrm{Aut}_k\, k[[z]]$ *with order* p. *Then there is* $m \in \mathbb{N}^\times$ *prime to* p *such that* $\sigma(z) = z(1+z^m)^{-1/m}$.

The local lifting problem for $G \simeq \mathbb{Z}/p\mathbb{Z}$

Proposition

Let k be an algebraically closed of char. $p > 0$. Let $\sigma \in \mathrm{Aut}_k\, k[[z]]$ with order p. Then there is $m \in \mathbb{N}^\times$ prime to p such that $\sigma(z) = z(1+z^m)^{-1/m}$.

Proof: Artin-Schreier theory gives a parametrization for p-cyclic extensions in char. $p > 0$. There $f \in k((z))$ such that $\mathrm{Tr}_{k((z))/k((t))} f = 1$.

The local lifting problem for $G \simeq \mathbb{Z}/p\mathbb{Z}$

Proposition

Let k be an algebraically closed of char. $p > 0$. Let $\sigma \in \mathrm{Aut}_k\, k[[z]]$ with order p. Then there is $m \in \mathbb{N}^\times$ prime to p such that $\sigma(z) = z(1+z^m)^{-1/m}$.

Proof: Artin-Schreier theory gives a parametrization for p-cyclic extensions in char. $p > 0$. There $f \in k((z))$ such that $\mathrm{Tr}_{k((z))/k((t))} f = 1$.
Let $x := -\sum_{1\leq i\leq p} i\sigma^i(f)$, then $\sigma(x) = x+1$ and so $y := x^p - x \in k((t))$ and so $k((z)) = k((t))[z]$ and $X^p - X - y$ is the irreducible polynomial of x over $k((t))$.

The local lifting problem for $G \simeq \mathbb{Z}/p\mathbb{Z}$

Proposition

Let k be an algebraically closed of char. $p > 0$. Let $\sigma \in \mathrm{Aut}_k\, k[[z]]$ with order p. Then there is $m \in \mathbb{N}^{\times}$ prime to p such that $\sigma(z) = z(1+z^m)^{-1/m}$.

Proof: Artin-Schreier theory gives a parametrization for p-cyclic extensions in char. $p > 0$. There $f \in k((z))$ such that $\mathrm{Tr}_{k((z))/k((t))} f = 1$.
Let $x := -\sum_{1 \le i \le p} i\sigma^i(f)$, then $\sigma(x) = x+1$ and so $y := x^p - x \in k((t))$ and so $k((z)) = k((t))[z]$ and $X^p - X - y$ is the irreducible polynomial of x over $k((t))$.
We write $y = \sum_{i \ge i_0} a_i t^i$. By Hensel's lemma we can assume that $a_i = 0$ for $i \ge 0$. Now we remark that for $i = pj$ we can write $a_i = b_j^p$ and that $a_{pj}/t^{pj} = b/t^j + (b/t^j)^p - b/t^j$ and finally we can assume that $y = (b/t^m)(1 + tP(t))$ for some $b \in k^*$ and $P(t) \in k[t]$ and $(m,p) = 1$.

The local lifting problem for $G \simeq \mathbb{Z}/p\mathbb{Z}$

Proposition

Let k be an algebraically closed of char. $p > 0$. *Let* $\sigma \in \mathrm{Aut}_k\, k[[z]]$ *with order* p. *Then there is* $m \in \mathbb{N}^\times$ *prime to* p *such that* $\sigma(z) = z(1+z^m)^{-1/m}$.

Proof: Artin-Schreier theory gives a parametrization for p-cyclic extensions in char. $p > 0$. There $f \in k((z))$ such that $\mathrm{Tr}_{k((z))/k((t))} f = 1$.
Let $x := -\sum_{1\leq i \leq p} i\sigma^i(f)$, then $\sigma(x) = x+1$ and so $y := x^p - x \in k((t))$ and so $k((z)) = k((t))[z]$ and $X^p - X - y$ is the irreducible polynomial of x over $k((t))$.
We write $y = \sum_{i \geq i_0} a_i t^i$. By Hensel's lemma we can assume that $a_i = 0$ for $i \geq 0$. Now we remark that for $i = pj$ we can write $a_i = b_j^p$ and that $a_{pj}/t^{pj} = b/t^j + (b/t^j)^p - b/t^j$ and finally we can assume that $y = (b/t^m)(1+tP(t))$ for some $b \in k^*$ and $P(t) \in k[t]$ and $(m,p) = 1$.
Then changing t by $t/(b(1+tP(t))^{1/m}$ we can assume that $f = 1/t^m$.

The local lifting problem for $G \simeq \mathbb{Z}/p\mathbb{Z}$

Proposition

Let k be an algebraically closed of char. $p > 0$. Let $\sigma \in \mathrm{Aut}_k k[[z]]$ with order p. Then there is $m \in \mathbb{N}^\times$ prime to p such that $\sigma(z) = z(1+z^m)^{-1/m}$.

Proof: Artin-Schreier theory gives a parametrization for p-cyclic extensions in char. $p > 0$. There $f \in k((z))$ such that $\mathrm{Tr}_{k((z))/k((t))} f = 1$.
Let $x := -\sum_{1 \le i \le p} i\sigma^i(f)$, then $\sigma(x) = x + 1$ and so $y := x^p - x \in k((t))$ and so $k((z)) = k((t))[z]$ and $X^p - X - y$ is the irreducible polynomial of x over $k((t))$.
We write $y = \sum_{i \ge i_0} a_i t^i$. By Hensel's lemma we can assume that $a_i = 0$ for $i \ge 0$. Now we remark that for $i = pj$ we can write $a_i = b_j^p$ and that $a_{pj}/t^{pj} = b/t^j + (b/t^j)^p - b/t^j$ and finally we can assume that $y = (b/t^m)(1 + tP(t))$ for some $b \in k^*$ and $P(t) \in k[t]$ and $(m,p) = 1$.
Then changing t by $t/(b(1+tP(t)))^{1/m}$ we can assume that $f = 1/t^m$.
An exercise shows that $z' := x^{-1/m} \in k((z))$ is a uniformizing parameter. As $\sigma(z') = (x+1)^{-1/m}$, the result follows.

Proposition

Let ζ_p be a primitive p-th root of 1 *in* K^{alg} *and* $m > 0$ *and prime to p.*

Proposition

Let ζ_p be a primitive p-th root of 1 in K^{alg} and $m > 0$ and prime to p. Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$, it defines an order p automorphism $\Sigma \in \mathrm{Aut}_R R[[Z]]$ for $R = W(k)[\zeta_p]$ and $r(\Sigma(Z)) = \sigma(z)$.

Proposition

Let ζ_p be a primitive p-th root of 1 in K^{alg} and $m > 0$ and prime to p.
Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$, it defines an order p automorphism $\Sigma \in \mathrm{Aut}_R R[[Z]]$ for $R = W(k)[\zeta_p]$ and $r(\Sigma(Z)) = \sigma(z)$.
In other words Σ is a lifting of σ.

Proposition

Let ζ_p be a primitive p-th root of 1 *in* K^{alg} *and* $m > 0$ *and prime to p.*
Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$, *it defines an order p automorphism* $\Sigma \in \mathrm{Aut}_R R[[Z]]$ *for* $R = W(k)[\zeta_p]$ *and* $r(\Sigma(Z)) = \sigma(z)$.
In other words Σ *is a lifting of* σ.

Proof: $\Sigma(Z^m) = \zeta_p^m \frac{Z^m}{1+Z^m}$ is an homographical transformation on Z^m of order p.

Proposition

Let ζ_p be a primitive p-th root of 1 *in* K^{alg} *and* $m>0$ *and prime to p.*
Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$*, it defines an order p automorphism* $\Sigma \in \mathrm{Aut}_R R[[Z]]$ *for* $R = W(k)[\zeta_p]$ *and* $r(\Sigma(Z)) = \sigma(z)$.
In other words Σ *is a lifting of* σ.

Proof: $\Sigma(Z^m) = \zeta_p^m \frac{Z^m}{1+Z^m}$ is an homographical transformation on Z^m of order p.
So $\Sigma^p(Z) = \theta Z$ with $\theta^m = 1$.

Proposition

Let ζ_p be a primitive p-th root of 1 in K^{alg} and $m > 0$ and prime to p.
Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$, it defines an order p automorphism $\Sigma \in \mathrm{Aut}_R R[[Z]]$ for $R = W(k)[\zeta_p]$ and $r(\Sigma(Z)) = \sigma(z)$.
In other words Σ is a lifting of σ.

Proof: $\Sigma(Z^m) = \zeta_p^m \frac{Z^m}{1+Z^m}$ is an homographical transformation on Z^m of order p.
So $\Sigma^p(Z) = \theta Z$ with $\theta^m = 1$.
Now we remark that $\Sigma(Z) = \zeta_p(Z) \mod Z^2$ and so $\Sigma^p(Z) = Z \mod Z^2$. ///

Proposition

Let ζ_p be a primitive p-th root of 1 in K^{alg} and $m > 0$ and prime to p.
Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$, it defines an order p automorphism $\Sigma \in \mathrm{Aut}_R R[[Z]]$ for $R = W(k)[\zeta_p]$ and $r(\Sigma(Z)) = \sigma(z)$.
In other words Σ is a lifting of σ.

Proof: $\Sigma(Z^m) = \zeta_p^m \frac{Z^m}{1+Z^m}$ is an homographical transformation on Z^m of order p.
So $\Sigma^p(Z) = \theta Z$ with $\theta^m = 1$.
Now we remark that $\Sigma(Z) = \zeta_p(Z) \mod Z^2$ and so $\Sigma^p(Z) = Z \mod Z^2$. ///

The geometry of fix points.

Proposition

Let ζ_p be a primitive p-th root of 1 in K^{alg} and $m > 0$ and prime to p.
Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$, it defines an order p automorphism $\Sigma \in \mathrm{Aut}_R R[[Z]]$ for $R = W(k)[\zeta_p]$ and $r(\Sigma(Z)) = \sigma(z)$.
In other words Σ is a lifting of σ.

Proof: $\Sigma(Z^m) = \zeta_p^m \frac{Z^m}{1+Z^m}$ is an homographical transformation on Z^m of order p.
So $\Sigma^p(Z) = \theta Z$ with $\theta^m = 1$.
Now we remark that $\Sigma(Z) = \zeta_p(Z) \mod Z^2$ and so $\Sigma^p(Z) = Z \mod Z^2$. ///

The geometry of fix points.

$\mathrm{Fix}\,\Sigma = \{z \in X^{alg} \mid z = \zeta_p z(1+z^m)^{-1/m}\}$ then

Proposition

Let ζ_p be a primitive p-th root of 1 in K^{alg} and $m > 0$ and prime to p.
Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$, it defines an order p automorphism $\Sigma \in \mathrm{Aut}_R R[[Z]]$ for $R = W(k)[\zeta_p]$ and $r(\Sigma(Z)) = \sigma(z)$.
In other words Σ is a lifting of σ.

Proof: $\Sigma(Z^m) = \zeta_p^m \frac{Z^m}{1+Z^m}$ is an homographical transformation on Z^m of order p.
So $\Sigma^p(Z) = \theta Z$ with $\theta^m = 1$.
Now we remark that $\Sigma(Z) = \zeta_p(Z) \mod Z^2$ and so $\Sigma^p(Z) = Z \mod Z^2$. ///

The geometry of fix points.

$\mathrm{Fix}\,\Sigma = \{z \in X^{alg} \mid z = \zeta_p z(1+z^m)^{-1/m}\}$ then

$\mathrm{Fix}\,\Sigma = \{0\} \cup \{\theta_m^i(\zeta_p^m - 1)^{1/m}\},\ 1 \leq i \leq m$, θ_m is a primitive m-th root of 1.

Proposition

Let ζ_p be a primitive p-th root of 1 in K^{alg} and $m > 0$ and prime to p.
Let $F(Z) := \zeta_p Z(1+Z^m)^{-1/m}$, it defines an order p automorphism $\Sigma \in \mathrm{Aut}_R R[[Z]]$ for $R = W(k)[\zeta_p]$ and $r(\Sigma(Z)) = \sigma(z)$.
In other words Σ is a lifting of σ.

Proof: $\Sigma(Z^m) = \zeta_p^m \frac{Z^m}{1+Z^m}$ is an homographical transformation on Z^m of order p.
So $\Sigma^p(Z) = \theta Z$ with $\theta^m = 1$.
Now we remark that $\Sigma(Z) = \zeta_p(Z) \mod Z^2$ and so $\Sigma^p(Z) = Z \mod Z^2$. ///

The geometry of fix points.

$\mathrm{Fix}\,\Sigma = \{z \in X^{alg} \mid z = \zeta_p z(1+z^m)^{-1/m}\}$ then

$\mathrm{Fix}\,\Sigma = \{0\} \cup \{\theta_m^i(\zeta_p^m - 1)^{1/m}\},\ 1 \le i \le m$, θ_m is a primitive m-th root of 1.

The mutual distances are all equal ; this is the equidistant geometry.

Geometric method.

Geometric method.

We can mimic at the level of R-algebras what we have done for k-algebras. Namely one can deform the isogeny $x \to x^p - x$ in $X \to \frac{(\lambda X+1)^p - 1}{\lambda^p}$.

Geometric method.

We can mimic at the level of R-algebras what we have done for k-algebras. Namely one can deform the isogeny $x \to x^p - x$ in $X \to \frac{(\lambda X+1)^p-1}{\lambda^p}$.

So we can lift over R any dvr finite over $W(k)[\zeta_p]$ at the level of fields $x^p - x = 1/t^m$ in

$(*) \quad \frac{(\lambda X+1)^p-1}{\lambda^p} = \frac{1}{\prod_{1\leq i\leq m}(T-t_i)}$ with $t_i \in X^{alg}$

Geometric method.

We can mimic at the level of R-algebras what we have done for k-algebras. Namely one can deform the isogeny $x \to x^p - x$ in $X \to \frac{(\lambda X+1)^p - 1}{\lambda^p}$.

So we can lift over R any dvr finite over $W(k)[\zeta_p]$ at the level of fields $x^p - x = 1/t^m$ in

$(*) \quad \frac{(\lambda X+1)^p - 1}{\lambda^p} = \frac{1}{\prod_{1\le i\le m}(T-t_i)}$ with $t_i \in X^{alg}$

(*) defines a p-cyclic cover of $\mathbb{P}^1_K$ which is highly singular.

Geometric method.

We can mimic at the level of R-algebras what we have done for k-algebras. Namely one can deform the isogeny $x \to x^p - x$ in $X \to \frac{(\lambda X+1)^p-1}{\lambda^p}$.

So we can lift over R any dvr finite over $W(k)[\zeta_p]$ at the level of fields $x^p - x = 1/t^m$ in

$(*) \quad \frac{(\lambda X+1)^p-1}{\lambda^p} = \frac{1}{\prod_{1\le i\le m}(T-t_i)}$ with $t_i \in X^{alg}$

(*) defines a p-cyclic cover of $\mathbb{P}^1_K$ which is highly singular.

Take the normalisation of $\mathbb{P}^1_R$, we get generically a p-cyclic cover C_η of $\mathbb{P}^1_K$ whose branch locus Br is given by the roots of $(\prod_{1\le i\le m}(T-t_i))(\lambda^p + \prod_{1\le i\le m}(T-t_i))$ with prime to p multiplicity.

We would like a smooth R-curve.

We would like a smooth R-curve.

We calculate the genus.

We would like a smooth R-curve.

We calculate the genus.

$$2(g(C_\eta)-1) = 2p(0-1) + |Br|(p-1) + m(p-1)$$

We would like a smooth R-curve.

We calculate the genus.

$2(g(C_\eta)-1) = 2p(0-1) + |Br|(p-1) + m(p-1)$

The special fiber C_s is reduced and geometric genus
$2(g(C_s)-1) = 2p(0-1) + (m+1)(p-1)$

We would like a smooth R-curve.

We calculate the genus.

$2(g(C_\eta)-1) = 2p(0-1)+|Br|(p-1)+m(p-1)$

The special fiber C_s is reduced and geometric genus
$2(g(C_s)-1) = 2p(0-1)+(m+1)(p-1)$

and it is smooth iff $|Br|(p-1)+m(p-1) = (m+1)(p-1)$.

We would like a smooth R-curve.

We calculate the genus.

$2(g(C_\eta)-1)=2p(0-1)+|Br|(p-1)+m(p-1)$

The special fiber C_s is reduced and geometric genus
$2(g(C_s)-1)=2p(0-1)+(m+1)(p-1)$

and it is smooth iff $|Br|(p-1)+m(p-1)=(m+1)(p-1)$.

This is the case when the t_i are all equal. For example for
$(**) \quad \frac{(\lambda X+1)^p-1}{\lambda^p}=\frac{1}{T^m}$

We would like a smooth R-curve.

We calculate the genus.

$2(g(C_\eta)-1) = 2p(0-1) + |Br|(p-1) + m(p-1)$

The special fiber C_s is reduced and geometric genus
$2(g(C_s)-1) = 2p(0-1) + (m+1)(p-1)$

and it is smooth iff $|Br|(p-1) + m(p-1) = (m+1)(p-1)$.

This is the case when the t_i are all equal. For example for
$(**) \quad \frac{(\lambda X+1)^p-1}{\lambda^p} = \frac{1}{T^m}$

When we consider the cover between the completion of the local rings at the closed point (π, T) we recover the order p automorphism $\in \mathrm{Aut}_R R[[Z]]$ considered above.

p^n-cyclic groups

Oort conjecture.

p^n-cyclic groups

Oort conjecture.

There is a conjecture named in the litterature ”Oort conjecture” which states that the local lifting problem for the group $\mathbb{Z}/p^n\mathbb{Z}$ as a positive answer.

p^n-cyclic groups

Oort conjecture.

There is a conjecture named in the litterature "Oort conjecture" which states that the local lifting problem for the group $\mathbb{Z}/p^n\mathbb{Z}$ as a positive answer.

The conjecture was set after global considerations relative to the case $n = 1$ which we have seen is elementary in the local case and so works in the global case due to a local-global principle.

p^n-cyclic groups

Oort conjecture.

There is a conjecture named in the litterature "Oort conjecture" which states that the local lifting problem for the group $\mathbb{Z}/p^n\mathbb{Z}$ as a positive answer.

The conjecture was set after global considerations relative to the case $n = 1$ which we have seen is elementary in the local case and so works in the global case due to a local-global principle.

It became serious when a proof along the lines of the geometric method described above was given in the case $n = 2$.

p^n-cyclic groups

Oort conjecture.

There is a conjecture named in the litterature ”Oort conjecture” which states that the local lifting problem for the group $\mathbb{Z}/p^n\mathbb{Z}$ as a positive answer.

The conjecture was set after global considerations relative to the case $n = 1$ which we have seen is elementary in the local case and so works in the global case due to a local-global principle.

It became serious when a proof along the lines of the geometric method described above was given in the case $n = 2$.

Recently a proof was announced by Obus and Wewers for the case $n = 3$ and for $n > 3$ under an extra condition (see the recent survey A. Obus: The (local) lifting problem for curves, arXiv 8 May 2011).

p^n-cyclic groups

Oort conjecture.

There is a conjecture named in the litterature "Oort conjecture" which states that the local lifting problem for the group $\mathbb{Z}/p^n\mathbb{Z}$ as a positive answer.

The conjecture was set after global considerations relative to the case $n = 1$ which we have seen is elementary in the local case and so works in the global case due to a local-global principle.

It became serious when a proof along the lines of the geometric method described above was given in the case $n = 2$.

Recently a proof was announced by Obus and Wewers for the case $n = 3$ and for $n > 3$ under an extra condition (see the recent survey A. Obus: The (local) lifting problem for curves, arXiv 8 May 2011).

In the next paragraph we give a method using formal groups which gives a positive answer to the inverse Galois problem for cyclic p-groups.

p^n-cyclic groups

Oort conjecture.

There is a conjecture named in the litterature "Oort conjecture" which states that the local lifting problem for the group $\mathbb{Z}/p^n\mathbb{Z}$ as a positive answer.

The conjecture was set after global considerations relative to the case $n = 1$ which we have seen is elementary in the local case and so works in the global case due to a local-global principle.

It became serious when a proof along the lines of the geometric method described above was given in the case $n = 2$.

Recently a proof was announced by Obus and Wewers for the case $n = 3$ and for $n > 3$ under an extra condition (see the recent survey A. Obus: The (local) lifting problem for curves, arXiv 8 May 2011).

In the next paragraph we give a method using formal groups which gives a positive answer to the inverse Galois problem for cyclic p-groups.

We illustrate this method in the case $n = 1$.

p^n-cyclic groups and formal groups

Notations

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$
(the series $exp(f(Z)$ is the so-called Artin-Hasse exponential)

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$
(the series $exp(f(Z)$ is the so-called Artin-Hasse exponential)
$F(Z_1, Z_2) := f^{\circ -1}(f(Z_1) + f(Z_2)) \in K[[Z_1, Z_2]]$

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$
(the series $exp(f(Z)$ is the so-called Artin-Hasse exponential)
$F(Z_1,Z_2) := f^{\circ -1}(f(Z_1)+f(Z_2)) \in K[[Z_1,Z_2]]$
$[\pi]_F(Z) := f^{\circ -1}(\pi f(Z)) \in K[[Z]]$.

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$
(the series $exp(f(Z)$ is the so-called Artin-Hasse exponential)
$F(Z_1, Z_2) := f^{\circ -1}(f(Z_1) + f(Z_2)) \in K[[Z_1, Z_2]]$
$[\pi]_F(Z) := f^{\circ -1}(\pi f(Z)) \in K[[Z]]$.
The main result is that $F(Z_1, Z_2) \in R[[Z_1, Z_2]]$ and $[\pi]_F(Z) \in R[[Z]]$.

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$
(the series $exp(f(Z)$ is the so-called Artin-Hasse exponential)
$F(Z_1, Z_2) := f^{\circ -1}(f(Z_1) + f(Z_2)) \in K[[Z_1, Z_2]]$
$[\pi]_F(Z) := f^{\circ -1}(\pi f(Z)) \in K[[Z]]$.
The main result is that $F(Z_1, Z_2) \in R[[Z_1, Z_2]]$ and $[\pi]_F(Z) \in R[[Z]]$.
Moreover $[\pi]_F(Z) = \pi Z \mod Z^2$ and $[\pi]_F(Z) = Z^p \mod \pi$

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$
(the series $exp(f(Z)$ is the so-called Artin-Hasse exponential)
$F(Z_1,Z_2) := f^{\circ -1}(f(Z_1)+f(Z_2)) \in K[[Z_1,Z_2]]$
$[\pi]_F(Z) := f^{\circ -1}(\pi f(Z)) \in K[[Z]]$.
The main result is that $F(Z_1,Z_2) \in R[[Z_1,Z_2]]$ and $[\pi]_F(Z) \in R[[Z]]$.
Moreover $[\pi]_F(Z) = \pi Z \mod Z^2$ and $[\pi]_F(Z) = Z^p \mod \pi$
It follows that for all $a \in R$ there is $[a]_F(Z) \in R[[Z]]$ such that
$[a]_F(F(Z_1,Z_2)) = F([a]_F(Z_1),[a]_F(Z_2))$ and $[a]_F(Z) = aZ \mod Z^2$.

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$
(the series $exp(f(Z)$ is the so-called Artin-Hasse exponential)
$F(Z_1,Z_2) := f^{\circ -1}(f(Z_1)+f(Z_2)) \in K[[Z_1,Z_2]]$
$[\pi]_F(Z) := f^{\circ -1}(\pi f(Z)) \in K[[Z]]$.
The main result is that $F(Z_1,Z_2) \in R[[Z_1,Z_2]]$ and $[\pi]_F(Z) \in R[[Z]]$.
Moreover $[\pi]_F(Z) = \pi Z \mod Z^2$ and $[\pi]_F(Z) = Z^p \mod \pi$
It follows that for all $a \in R$ there is $[a]_F(Z) \in R[[Z]]$ such that
$[a]_F(F(Z_1,Z_2)) = F([a]_F(Z_1),[a]_F(Z_2))$ and $[a]_F(Z) = aZ \mod Z^2$.
Then $a \in R \to [a]_F(Z)$ is an injective homomorphism of R into End_F.

p^n-cyclic groups and formal groups

Notations

K is a finite totally ramified extension of $\mathbb{Q}_p[\zeta_p]$ of degree n.
$R := O_K$ and π a uniformising parameter.
$f(Z) := \sum_{i\geq 0} \frac{Z^{p^k}}{\pi^k} \in K[[Z]]$
(the series $exp(f(Z)$ is the so-called Artin-Hasse exponential)
$F(Z_1,Z_2) := f^{\circ -1}(f(Z_1)+f(Z_2)) \in K[[Z_1,Z_2]]$
$[\pi]_F(Z) := f^{\circ -1}(\pi f(Z)) \in K[[Z]]$.
The main result is that $F(Z_1,Z_2) \in R[[Z_1,Z_2]]$ and $[\pi]_F(Z) \in R[[Z]]$.
Moreover $[\pi]_F(Z) = \pi Z \mod Z^2$ and $[\pi]_F(Z) = Z^p \mod \pi$
It follows that for all $a \in R$ there is $[a]_F(Z) \in R[[Z]]$ such that
$[a]_F(F(Z_1,Z_2)) = F([a]_F(Z_1),[a]_F(Z_2))$ and $[a]_F(Z) = aZ \mod Z^2$.
Then $a \in R \to [a]_F(Z)$ is an injective homomorphism of R into End_F.
For example $\sigma(Z) := [\zeta_p]_F(Z) = f^{\circ -1}(\zeta_p f(Z))$ is an order p-automorphism of $R[[Z]]$ which is not trivial $\mod \pi$ and with p^n fix points whose geometry is well understood.

Obstructions to the local lifting problem

There is a local version of the criterium of good reduction which involves degrees of differents.

Obstructions to the local lifting problem

There is a local version of the criterium of good reduction which involves degrees of differents.

Proposition

Let $A = R[[T])$ *and B be a finite A-module and a normal integral local ring.*

Obstructions to the local lifting problem

There is a local version of the criterium of good reduction which involves degrees of differents.

Proposition

Let $A = R[[T])$ *and* B *be a finite* A*-module and a normal integral local ring. Set* $A_K := A \otimes_R K$ *and* $B_K := B \otimes_R K$*,*

Obstructions to the local lifting problem

There is a local version of the criterium of good reduction which involves degrees of differents.

Proposition

Let $A = R[[T]])$ and B be a finite A-module and a normal integral local ring. Set $A_K := A \otimes_R K$ and $B_K := B \otimes_R K$, $A_0 := A/\pi A$ and $B_0 := B/\pi B$.

Obstructions to the local lifting problem

There is a local version of the criterium of good reduction which involves degrees of differents.

Proposition

Let $A = R[[T])$ *and* B *be a finite* A*-module and a normal integral local ring.*
Set $A_K := A \otimes_R K$ *and* $B_K := B \otimes_R K$*,*
$A_0 := A/\pi A$ *and* $B_0 := B/\pi B$*.*
We assume that B_0 *is reduced and that* B_0/A_0 *is generically étale.*

Obstructions to the local lifting problem

There is a local version of the criterium of good reduction which involves degrees of differents.

Proposition

Let $A = R[[T])$ and B be a finite A-module and a normal integral local ring.
Set $A_K := A \otimes_R K$ and $B_K := B \otimes_R K$,
$A_0 := A/\pi A$ and $B_0 := B/\pi B$.
We assume that B_0 is reduced and that B_0/A_0 is generically étale.
Let B_0^{alg} the B_0 integral closure and $\delta_k(B) := \dim_k B_0^{alg}/B_0$.

Obstructions to the local lifting problem

There is a local version of the criterium of good reduction which involves degrees of differents.

Proposition

Let $A = R[[T])$ and B be a finite A-module and a normal integral local ring.
Set $A_K := A \otimes_R K$ and $B_K := B \otimes_R K$,
$A_0 := A/\pi A$ and $B_0 := B/\pi B$.
We assume that B_0 is reduced and that B_0/A_0 is generically étale.
Let B_0^{alg} the B_0 integral closure and $\delta_k(B) := \dim_k B_0^{alg}/B_0$.
Let d_η resp. d_s the degree of the generic resp. special different.

Obstructions to the local lifting problem

There is a local version of the criterium of good reduction which involves degrees of differents.

Proposition

Let $A = R[[T])$ and B be a finite A-module and a normal integral local ring.
Set $A_K := A \otimes_R K$ and $B_K := B \otimes_R K$,
$A_0 := A/\pi A$ and $B_0 := B/\pi B$.
We assume that B_0 is reduced and that B_0/A_0 is generically étale.
Let B_0^{alg} the B_0 integral closure and $\delta_k(B) := \dim_k B_0^{alg}/B_0$.
Let d_η resp. d_s the degree of the generic resp. special different.
Then $d_\eta = d_s + 2\delta_k(B)$ and $d_\eta = d_s$ iff $B = R[[Z]]$.

Application: the local lifting problem for $G = (\mathbb{Z}/p\mathbb{Z})^2$

The ramification filtration.

Application: the local lifting problem for $G = (\mathbb{Z}/p\mathbb{Z})^2$

The ramification filtration.

$G = G_0 = G_1 = \ldots = G_{m_1} \supsetneq G_{m_1+1} \supset \ldots \supset G_{m_2} \supsetneq G_{m_2+1} = 0$

Application: the local lifting problem for $G = (\mathbb{Z}/p\mathbb{Z})^2$

The ramification filtration.

$G = G_0 = G_1 = \ldots = G_{m_1} \supsetneq G_{m_1+1} \supset \ldots \supset G_{m_2} \supsetneq G_{m_2+1} = 0$

The extension is birationnaly defined by $k((z)) = k((t))[x_1, x_2]$ where

Application: the local lifting problem for $G = (\mathbb{Z}/p\mathbb{Z})^2$

The ramification filtration.

$G = G_0 = G_1 = ... = G_{m_1} \supsetneq G_{m_1+1} \supset ... \supset G_{m_2} \supsetneq G_{m_2+1} = 0$

The extension is birationnaly defined by $k((z)) = k((t))[x_1, x_2]$ where $x_1^p - x_1 = 1/t^{m'_1}$, $x_2^p - x_2 = a_{m'_2}/t^{m'_2} + ... + a_1/t$

Application: the local lifting problem for $G = (\mathbb{Z}/p\mathbb{Z})^2$

The ramification filtration.

$G = G_0 = G_1 = ... = G_{m_1} \supsetneq G_{m_1+1} \supset ... \supset G_{m_2} \supsetneq G_{m_2+1} = 0$

The extension is birationnaly defined by $k((z)) = k((t))[x_1, x_2]$ where

$x_1^p - x_1 = 1/t^{m_1'}$, $x_2^p - x_2 = a_{m_2'}/t^{m_2'} + ... + a_1/t$

where $m_1' \leq m_2'$ are prime to p, $a_{m_2'} \in k^\times$ and $a_{m_2'} \notin \mathbb{F}_p$ if $m_1' = m_2'$.

Application: the local lifting problem for $G = (\mathbb{Z}/p\mathbb{Z})^2$

The ramification filtration.
$G = G_0 = G_1 = \ldots = G_{m_1} \supsetneq G_{m_1+1} \supset \ldots \supset G_{m_2} \supsetneq G_{m_2+1} = 0$
The extension is birationnaly defined by $k((z)) = k((t))[x_1, x_2]$ where
$x_1^p - x_1 = 1/t^{m'_1}$, $x_2^p - x_2 = a_{m'_2}/t^{m'_2} + \ldots . + a_1/t$
where $m'_1 \leq m'_2$ are prime to p, $a_{m'_2} \in k^\times$ and $a_{m'_2} \notin \mathbb{F}_p$ if $m'_1 = m'_2$.
One can show that $m_1 = m'_1$ and $m_2 = m'_2 p - m'_1(p-1)$. Then
$d_s = (m_1+1)(p^2-1) + (m_2 - m_1)(p-1)$.

Application: the local lifting problem for $G = (\mathbb{Z}/p\mathbb{Z})^2$

The ramification filtration.

$G = G_0 = G_1 = ... = G_{m_1} \supsetneq G_{m_1+1} \supset ... \supset G_{m_2} \supsetneq G_{m_2+1} = 0$

The extension is birationnaly defined by $k((z)) = k((t))[x_1, x_2]$ where

$x_1^p - x_1 = 1/t^{m'_1}$, $x_2^p - x_2 = a_{m'_2}/t^{m'_2} + ... + a_1/t$

where $m'_1 \leq m'_2$ are prime to p, $a_{m'_2} \in k^\times$ and $a_{m'_2} \notin \mathbb{F}_p$ if $m'_1 = m'_2$.

One can show that $m_1 = m'_1$ and $m_2 = m'_2 p - m'_1(p-1)$. Then

$d_s = (m_1+1)(p^2-1) + (m_2 - m_1)(p-1)$.

Let $R[[Z]]/R[[T]]$ be a lifting then

$d_\eta = (m'_1 + 1 - d)p(p-1) + (m'_2 + 1 - d)p(p-1) + dp(p-1)$, where d is the number of branch points in common in the lifting of the two basis covers.

Application: the local lifting problem for $G = (\mathbb{Z}/p\mathbb{Z})^2$

The ramification filtration.

$G = G_0 = G_1 = \ldots = G_{m_1} \supsetneq G_{m_1+1} \supset \ldots \supset G_{m_2} \supsetneq G_{m_2+1} = 0$

The extension is birationnaly defined by $k((z)) = k((t))[x_1, x_2]$ where

$x_1^p - x_1 = 1/t^{m'_1}$, $x_2^p - x_2 = a_{m'_2}/t^{m'_2} + \ldots . + a_1/t$

where $m'_1 \leq m'_2$ are prime to p, $a_{m'_2} \in k^\times$ and $a_{m'_2} \notin \mathbb{F}_p$ if $m'_1 = m'_2$.

One can show that $m_1 = m'_1$ and $m_2 = m'_2 p - m'_1(p-1)$. Then

$d_s = (m_1+1)(p^2-1) + (m_2 - m_1)(p-1)$.

Let $R[[Z]]/R[[T]]$ be a lifting then

$d_\eta = (m'_1 + 1 - d)p(p-1) + (m'_2 + 1 - d)p(p-1) + dp(p-1)$, where d is the number of branch points in common in the lifting of the two basis covers.

A necessary and sufficient condition is that $d_s = d_\eta$ i.e. $dp = (m_1+1)(p-1)$.

In particular $m_1 = -1 \mod p$, this is an obstruction to the local lifting problem when $p > 2$.

The inverse local lifting problem for $G = (Z/pZ)^n,\ n > 1$

The condition $dp = (m_1 + 1)(p - 1)$ is not easy to realize because the geometry of branch points is rigid as we will see in the last lecture.

The inverse local lifting problem for $G = (Z/pZ)^n$, $n > 1$

The condition $dp = (m_1 + 1)(p - 1)$ is not easy to realize because the geometry of branch points is rigid as we will see in the last lecture. Nevertheless one can show that the inverse Galois problem for $G = (Z/pZ)^n$ has a positive answer.

The inverse local lifting problem for $G = (Z/pZ)^n,\ n > 1$

The condition $dp = (m_1 + 1)(p - 1)$ is not easy to realize because the geometry of branch points is rigid as we will see in the last lecture.
Nevertheless one can show that the inverse Galois problem for $G = (Z/pZ)^n$ has a positive answer.
Here is a proof in the case $p = 2$ and $n = 3$. It depends on the following lemma

Lemma

$p = 2$, and let

The inverse local lifting problem for $G = (Z/pZ)^n$, $n > 1$

The condition $dp = (m_1 + 1)(p - 1)$ is not easy to realize because the geometry of branch points is rigid as we will see in the last lecture.
Nevertheless one can show that the inverse Galois problem for $G = (Z/pZ)^n$ has a positive answer.
Here is a proof in the case $p = 2$ and $n = 3$. It depends on the following lemma

Lemma

$p = 2$, and let
$Y^2 = f(X) = (1 + \alpha_1 X)(1 + \alpha_2 X)(1 + (\alpha_1^{1/2} + \alpha_2^{1/2})^2 X)$

The inverse local lifting problem for $G = (Z/pZ)^n$, $n > 1$

The condition $dp = (m_1 + 1)(p - 1)$ is not easy to realize because the geometry of branch points is rigid as we will see in the last lecture.
Nevertheless one can show that the inverse Galois problem for $G = (Z/pZ)^n$ has a positive answer.
Here is a proof in the case $p = 2$ and $n = 3$. It depends on the following lemma

Lemma

$p = 2$, and let
$Y^2 = f(X) = (1 + \alpha_1 X)(1 + \alpha_2 X)(1 + (\alpha_1^{1/2} + \alpha_2^{1/2})^2 X)$
with $\alpha_i \in W(k)^{alg}$ and let $a_i \in k$ the reduction of α_i mod π. We assume that $a_1 a_2 (a_1 + a_2)(a_1^2 + a_2^2 + a_1 a_2) \neq 0$.

The inverse local lifting problem for $G = (Z/pZ)^n$, $n > 1$

The condition $dp = (m_1 + 1)(p - 1)$ is not easy to realize because the geometry of branch points is rigid as we will see in the last lecture.
Nevertheless one can show that the inverse Galois problem for $G = (Z/pZ)^n$ has a positive answer.
Here is a proof in the case $p = 2$ and $n = 3$. It depends on the following lemma

Lemma

$p = 2$, and let
$Y^2 = f(X) = (1 + \alpha_1 X)(1 + \alpha_2 X)(1 + (\alpha_1^{1/2} + \alpha_2^{1/2})^2 X)$
with $\alpha_i \in W(k)^{alg}$ and let $a_i \in k$ the reduction of α_i mod π. We assume that
$a_1 a_2 (a_1 + a_2)(a_1^2 + a_2^2 + a_1 a_2) \neq 0$.
Then $f(X) = (1 + \beta X)^2 + \alpha_1 \alpha_2 (\alpha_1^{1/2} + \alpha_2^{1/2})^2 X^3$.

The inverse local lifting problem for $G=(Z/pZ)^n$, $n>1$

The condition $dp=(m_1+1)(p-1)$ is not easy to realize because the geometry of branch points is rigid as we will see in the last lecture.
Nevertheless one can show that the inverse Galois problem for $G=(Z/pZ)^n$ has a positive answer.
Here is a proof in the case $p=2$ and $n=3$. It depends on the following lemma

Lemma

$p=2$, and let
$Y^2=f(X)=(1+\alpha_1X)(1+\alpha_2X)(1+(\alpha_1^{1/2}+\alpha_2^{1/2})^2X)$
with $\alpha_i\in W(k)^{alg}$ and let $a_i\in k$ the reduction of α_i mod π. We assume that
$a_1a_2(a_1+a_2)(a_1^2+a_2^2+a_1a_2)\neq 0.$
Then $f(X)=(1+\beta X)^2+\alpha_1\alpha_2(\alpha_1^{1/2}+\alpha_2^{1/2})^2X^3.$
Set $R:=W(k)[2^{1/3}]$ *and* $X=2^{2/3}T^{-1}$, *and* $Y=1+\beta X+2Z$

The inverse local lifting problem for $G = (Z/pZ)^n$, $n > 1$

The condition $dp = (m_1+1)(p-1)$ is not easy to realize because the geometry of branch points is rigid as we will see in the last lecture.
Nevertheless one can show that the inverse Galois problem for $G = (Z/pZ)^n$ has a positive answer.
Here is a proof in the case $p = 2$ and $n = 3$. It depends on the following lemma

Lemma

$p = 2$, and let
$Y^2 = f(X) = (1+\alpha_1 X)(1+\alpha_2 X)(1+(\alpha_1^{1/2}+\alpha_2^{1/2})^2 X)$
with $\alpha_i \in W(k)^{alg}$ and let $a_i \in k$ the reduction of α_i mod π. We assume that
$a_1 a_2 (a_1+a_2)(a_1^2+a_2^2+a_1 a_2) \neq 0$.
Then $f(X) = (1+\beta X)^2 + \alpha_1\alpha_2(\alpha_1^{1/2}+\alpha_2^{1/2})^2 X^3$.
Set $R := W(k)[2^{1/3}]$ *and* $X = 2^{2/3}T^{-1}$, *and* $Y = 1+\beta X + 2Z$
then $Z^2 + (1+2^{2/3}\beta T)Z = \alpha_1\alpha_2(\alpha_1^{1/2}+\alpha_2^{1/2})^2 T^{-3}$ *which gives* $\mod \pi$
$z^2 + z = a_1 a_2 (a_1+a_2)^2 t^{-3}$.

The idea is to consider the compositum of three 2-cyclic covers of $\mathbb{P}^1_K$ given by

The idea is to consider the compositum of three 2-cyclic covers of $\mathbb{P}^1_K$ given by

$Y_1^2 = (1+\alpha_1 X)(1+\alpha_2 X)(1+(\alpha_1^{1/2}+\alpha_2^{1/2})^2 X)$

The idea is to consider the compositum of three 2-cyclic covers of $\mathbb{P}^1_K$ given by

$$Y_1^2 = (1+\alpha_1 X)(1+\alpha_2 X)(1+(\alpha_1^{1/2}+\alpha_2^{1/2})^2 X)$$

$$Y_1^2 = (1+\alpha_2 X)(1+\alpha_3 X)(1+(\alpha_2^{1/2}+\alpha_3^{1/2})^2 X)$$

The idea is to consider the compositum of three 2-cyclic covers of $\mathbb{P}^1_K$ given by

$$Y_1^2 = (1+\alpha_1 X)(1+\alpha_2 X)(1+(\alpha_1^{1/2}+\alpha_2^{1/2})^2 X)$$

$$Y_1^2 = (1+\alpha_2 X)(1+\alpha_3 X)(1+(\alpha_2^{1/2}+\alpha_3^{1/2})^2 X)$$

$$Y_1^2 = (1+\alpha_3 X)(1+\alpha_1 X)(1+(\alpha_3^{1/2}+\alpha_1^{1/2})^2 X)$$

The idea is to consider the compositum of three 2-cyclic covers of $\mathbb{P}^1_K$ given by

$Y_1^2 = (1+\alpha_1 X)(1+\alpha_2 X)(1+(\alpha_1^{1/2}+\alpha_2^{1/2})^2 X)$

$Y_1^2 = (1+\alpha_2 X)(1+\alpha_3 X)(1+(\alpha_2^{1/2}+\alpha_3^{1/2})^2 X)$

$Y_1^2 = (1+\alpha_3 X)(1+\alpha_1 X)(1+(\alpha_3^{1/2}+\alpha_1^{1/2})^2 X)$

with $a_1+a_2+a_3 \neq 0$, $1+(a_1+a_2+a_3)(a_1^{-1}+a_2^{-1}+a_3^{-1}) \neq 0$ and analoguous conditions as in the lemma.

The idea is to consider the compositum of three 2-cyclic covers of $\mathbb{P}^1_K$ given by

$Y_1^2 = (1+\alpha_1 X)(1+\alpha_2 X)(1+(\alpha_1^{1/2}+\alpha_2^{1/2})^2 X)$

$Y_1^2 = (1+\alpha_2 X)(1+\alpha_3 X)(1+(\alpha_2^{1/2}+\alpha_3^{1/2})^2 X)$

$Y_1^2 = (1+\alpha_3 X)(1+\alpha_1 X)(1+(\alpha_3^{1/2}+\alpha_1^{1/2})^2 X)$

with $a_1+a_2+a_3 \neq 0$, $1+(a_1+a_2+a_3)(a_1^{-1}+a_2^{-1}+a_3^{-1}) \neq 0$ and analoguous conditions as in the lemma.

Then any pair of 2-covers have in common 2 branch points and any triple of 2-covers have in common 1 branch point. This insure that $d_\eta = d_s$

Minimal stable model for the pointed disc

From now we shall assume that σ is an order p-automorphism and the its fix points are rational over K.

Proposition

Order p-automorphisms with one fix point are linearizable.

Minimal stable model for the pointed disc

From now we shall assume that σ is an order p-automorphism and the its fix points are rational over K.

Proposition

Order p-automorphisms with one fix point are linearizable.

Now we assume that $|\operatorname{Fix}\sigma| = m+1 > 1$ and $\operatorname{Fix}\sigma = \{z_0, z_1, ..., z_m\}$

Minimal stable model for the pointed disc

From now we shall assume that σ is an order p-automorphism and the its fix points are rational over K.

Proposition

Order p-automorphisms with one fix point are linearizable.

Now we assume that $|\operatorname{Fix}\sigma| = m+1 > 1$ and $\operatorname{Fix}\sigma = \{z_0, z_1, \ldots, z_m\}$

Minimal stable model for the pointed disc $(X, \operatorname{Fix}\sigma)$

Minimal stable model for the pointed disc

From now we shall assume that σ is an order p-automorphism and the its fix points are rational over K.

Proposition

Order p-automorphisms with one fix point are linearizable.

Now we assume that $|\mathrm{Fix}\,\sigma| = m+1 > 1$ and $\mathrm{Fix}\,\sigma = \{z_0, z_1, \ldots, z_m\}$

Minimal stable model for the pointed disc $(X, \mathrm{Fix}\,\sigma)$

The method:

Minimal stable model for the pointed disc

From now we shall assume that σ is an order p-automorphism and the its fix points are rational over K.

Proposition

Order p-automorphisms with one fix point are linearizable.

Now we assume that $|\mathrm{Fix}\,\sigma| = m+1 > 1$ and $\mathrm{Fix}\,\sigma = \{z_0, z_1, \ldots, z_m\}$

Minimal stable model for the pointed disc $(X, \mathrm{Fix}\,\sigma)$

The method:

Let $v(\rho) = inf_{i\neq j}\{v(z_i - z_j)\} = v(z_{i_0} - z_{i_1})$

Minimal stable model for the pointed disc

From now we shall assume that σ is an order p-automorphism and the its fix points are rational over K.

Proposition

Order p-automorphisms with one fix point are linearizable.

Now we assume that $|\mathrm{Fix}\,\sigma| = m+1 > 1$ and $\mathrm{Fix}\,\sigma = \{z_0, z_1, \ldots, z_m\}$

Minimal stable model for the pointed disc $(X, \mathrm{Fix}\,\sigma)$

The method:

Let $v(\rho) = inf_{i\neq j}\{v(z_i - z_j)\} = v(z_{i_0} - z_{i_1})$

A blowing up along the ideal $(Z - z_{i_0}, \rho)$ induces a new model in which the specialization map induces a non trivial partition on $\mathrm{Fix}\,\sigma$.

Minimal stable model for the pointed disc

From now we shall assume that σ is an order p-automorphism and the its fix points are rational over K.

Proposition

Order p-automorphisms with one fix point are linearizable.

Now we assume that $|\mathrm{Fix}\,\sigma| = m+1 > 1$ and $\mathrm{Fix}\,\sigma = \{z_0, z_1, \ldots, z_m\}$

Minimal stable model for the pointed disc $(X, \mathrm{Fix}\,\sigma)$

The method:

Let $v(\rho) = inf_{i\neq j}\{v(z_i - z_j)\} = v(z_{i_0} - z_{i_1})$

A blowing up along the ideal $(Z - z_{i_0}, \rho)$ induces a new model in which the specialization map induces a non trivial partition on $\mathrm{Fix}\,\sigma$.

An induction argument will produce a minimal stable model $\mathscr{X}_\sigma$ for the pointed disc $(X, \mathrm{Fix}\,\sigma)$.

Geometry of order p-automorphisms of the disc

Proposition

The fix points specialize in $\mathscr{X}_\sigma$ in the terminal components.

Geometry of order p-automorphisms of the disc

Proposition

The fix points specialize in $\mathscr{X}_\sigma$ in the terminal components.

Theorem

Let $\sigma \in \mathrm{Aut}_R R[[Z]]$ be an automorphism of order p such that

Geometry of order p-automorphisms of the disc

Proposition

The fix points specialize in $\mathscr{X}_\sigma$ in the terminal components.

Theorem

Let $\sigma \in \mathrm{Aut}_R R[[Z]]$ be an automorphism of order p such that $1 < |\mathrm{Fix}\,\sigma| = m+1 < p$,

Geometry of order p-automorphisms of the disc

Proposition

The fix points specialize in $\mathscr{X}_\sigma$ in the terminal components.

Theorem

Let $\sigma \in \mathrm{Aut}_R R[[Z]]$ be an automorphism of order p such that
$1 < |\mathrm{Fix}\,\sigma| = m+1 < p$,
$r(\sigma) \neq Id$.

Geometry of order p-automorphisms of the disc

Proposition

The fix points specialize in $\mathscr{X}_\sigma$ in the terminal components.

Theorem

Let $\sigma \in \mathrm{Aut}_R R[[Z]]$ *be an automorphism of order* p *such that*
$1 < |\mathrm{Fix}\,\sigma| = m+1 < p$,
$r(\sigma) \neq Id$.
Then the minimal stable model for the pointed disc $(X, \mathrm{Fix}\,\sigma)$ *has only one component.*

Geometry of order p-automorphisms of the disc

Proposition

The fix points specialize in $\mathscr{X}_\sigma$ in the terminal components.

Theorem

Let $\sigma \in \mathrm{Aut}_R R[[Z]]$ be an automorphism of order p such that
$1 < |\mathrm{Fix}\,\sigma| = m+1 < p$,
$r(\sigma) \neq Id$.
Then the minimal stable model for the pointed disc $(X, \mathrm{Fix}\,\sigma)$ has only one component.
There is a finite number of conjugacy classes of such automorphisms.