Order p automorphisms of the open disc of a p-adic field

By

Barry Green and Michel Matignon

Abstract: Let k be an algebraically closed field of characteristic $p > 0$, $W(k)$ the ring of Witt vectors and R be a complete discrete valuation ring dominating $W(k)$ and containing ζ, a primitive p-th root of unity. Let π denote a uniformizing parameter for R.

We study order p automorphisms of the formal power series ring $R[[Z]]$, which are defined by a series

$$\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots + a_i Z^i + \cdots) \in R[[Z]].$$

The set of fixed points of σ is denoted by F_σ and we suppose that they are K-rational and that $|F_\sigma| = m + 1$ for $m \geq 0$.

Let $\mathcal{D}^o$ be the minimal semi-stable model of the p-adic open disc over R in which F_σ specializes to distinct smooth points. We study the differential data that can be associated to each irreducible component of the special fibre of $\mathcal{D}^o$. Using this data we show that if $m < p$ the fixed points are equidistant, and that there are only a finite number of conjugacy classes of order p automorphisms in $\mathrm{Aut}_R(R[[Z]])$ which are not the identity $\bmod (\pi)$.

1991 AMS Subject Classification. Primary 14G20, 14L27; Secondary 14D15, 14E22.

Key Words: Order p automorphisms of open p-adic discs; fixed points, Hurwitz data, Lubin-Tate formal groups, semi-stable models, degeneration of μ_p-torsors, automorphism conjugacy classes.

Contents

0. **Introduction**

I. **Notation and the geometry of p-adic discs**

II. **Order p automorphisms of p-adic discs**

III. **Geometry of the fixed points of order p automorphisms**

IV. **Local obstructions to the lifting**

V. **Moduli of order p automorphisms**

VI. **References**

0. Introduction

Let k be an algebraically closed field of characteristic $p > 0$ and R be a complete discrete valuation ring dominating the ring of Witt vectors $W(k)$. Let π denote a uniformizing parameter of R and R^{alg} be the integral closure in a fixed algebraic closure of $K := \mathrm{Fr}(R)$. Throughout the paper we shall assume that R contains a prescribed primitive p-th root of unity, which we denote by ζ.

In our previous paper [G-M], we were concerned with liftings of G-Galois covers of proper smooth curves over k to G-Galois covers of curves over R. There we have shown that this problem is of local nature and so the crucial study is that of G-covers $R[\![Z]\!]/R[\![Z]\!]^G$ which induce G-covers $k[\![z]\!]/k[\![z]\!]^G \mod \pi$, i.e. determination of the automorphism groups G of $k[\![z]\!]$ which can be lifted to automorphism groups of $R[\![Z]\!]$. Another weaker question is to ask what the finite groups which occur as subgroups of $\mathrm{Aut}_R R[\![Z]\!]$ with no inertia at (π) are.

We were able to show that the local lifting for p^2-cyclic covers is always possible; the key point was to produce enough automorphisms of order p of $R[\![Z]\!]$ which are p-powers. This confirmed our conviction that the objects to be studied are automorphisms of order p, which is the aim of this paper.

Now we describe the content of the paper. In chapter II we explain that this study is that of R-automorphisms $\sigma \in \mathrm{Aut}_R R[\![Z]\!]$ with series representation

$$\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots + a_m Z^m + \cdots) \in R[\![Z]\!],$$

such that the p-th iterate $\sigma^p(Z) = Z$. Our programme is to classify such automorphisms up to a change of parameter.

Such an automorphism σ acts naturally on $D^o := \mathrm{Spec}\, R[\![Z]\!]$ giving the following geometric data: let F_σ be the set of points fixed by σ, i.e. the roots in the maximal ideal of R^{alg} of the series $\sigma(Z) - Z$. It is shown that they are simple roots and in the sequel we shall only consider those σ for which $F_\sigma = \{Z_0, ..., Z_m\}$ is non-empty and for convenience the Z_i are R-rational. We can attach *Hurwitz data,* $H_\sigma = (h_0, ..., h_m) \in (\mathbb{Z}/p\mathbb{Z})^{m+1}$, to the fixed points of an order p automorphism, which gives the list of exponents of ζ which occur in the series representation of the action of σ on the tangent space of the fixed points.

We then consider the minimal semi-stable model $f : (\mathcal{D}^o, F_\sigma) \to D^o$ of the p-adic open disc D^o_K for which the points in F_σ specialize to distinct smooth points. The morphism f is a composition of blowing-ups at closed points. We intend to describe the morphism:

$$\varphi : (\mathcal{D}^o, F_\sigma) \to (\mathcal{D}^o, F_\sigma)/\langle\sigma\rangle := \mathcal{D}'^o.$$

Let $\mathcal{D}^o_s$ (resp. $\mathcal{D}'^o_s$) denote the special fibre, which is a tree of projective lines that will be oriented positively with respect to the original generic point (π) of D^o_s in D^o by the blowing up process. Each successive blowing up enlarges the tree representing the special fibre by a copy of $\mathbb{P}^1_k$ attached to the previous tree at a double crossing point. In this way we have a canonical infinite point, ∞, on each irreducible component of $\mathcal{D}^o_s$ (resp. $\mathcal{D}'^o_s$), namely the first closed point we meet in an injective path from the root (π). On the special fibres $\varphi_s : \mathcal{D}^o_s \to \mathcal{D}'^o_s$ is a homeomorphism. Let E_i, E'_i (resp. P_α, P'_α) be the terminal (resp. the internal) components of $\mathcal{D}^o_s$ and $\mathcal{D}'^o_s$. The canonical infinite points on these components are denoted by ∞_i (resp. ∞_α).

Fixing notation in order to explain the main results of the paper, let $\{Z_{i,j},\ 0 \leq j \leq m_i\}$ be the set of fixed points of σ whose specialization $z_{i,j}$ lies in E_i with image $t_{i,j} := \varphi_s(z_{i,j}) \in E'_i$ and let

$h_{i,j}$ be the Hurwitz data at $Z_{i,j}$. By studying the variation of the different along paths of the special fibre, we show (Prop. II.1.2) that the points fixed by σ specialize to the terminal components.

Following this we study the differential data that can be associated to each irreducible component of the special fibre $\mathcal{D}'^o_s$. The result proved here (Th. II.2.1) is the main theorem of the paper; using it we show that if $0 < m < p$, then $\mathcal{D}^o_s$ has only one component and consequently the fixed points are all equidistant. More precisely, given an internal component P'_α let $t_{\alpha,n} \in P'_\alpha$, $1 \leq n \leq n_\alpha$, be its crossing points. To each point $t_{\alpha,n}$ we associate the terminal components E'_i, indexed by $i \in I_n$, which are connected to $t_{\alpha,n}$ by a positive path. We set $m_{\alpha,n} + 1 := \sum_{i \in I_n}(m_i + 1)$. Then:

Theorem II.2.1. *There exist functions $\bar{u}_i \in k(E'_i)$ with $\mathrm{ord}_{\infty_i}\bar{u}_i = 0$, such that the differentials $\omega_i = d\bar{u}_i$ have divisor support in $\{t_{i,j}\}_j \cup \{\infty_i\}$ and satisfy $\mathrm{ord}_{t_{i,j}}\omega_i \equiv h_{i,j} - 1 \bmod p$ and $\mathrm{ord}_{\infty_i}\omega_i = m_i - 1$. Moreover, $(m_i, p) = 1$ and $\sum_j h_{i,j} \equiv 0 \bmod p$.*

There exist functions $\bar{u}_\alpha \in k(P'_\alpha)$ such that the differentials $\omega_\alpha = d\bar{u}_\alpha$ have divisor support in the points $\{t_{\alpha,n}\}_n \cup \{\infty_\alpha\}$ and $\mathrm{ord}_{t_{\alpha,n}}\omega_\alpha = -(m_{\alpha,n} + 1) < 0$ and $\mathrm{ord}_{\infty_\alpha}\omega_\alpha = -2 + \sum_n(m_{\alpha,n} + 1)$. Moreover, $(m_{\alpha,n}, p) = 1$ and $(-1 + \sum_n(m_{\alpha,n} + 1), p) = 1$.

The differentials come from the equations of the cover $\varphi_s : \mathcal{D}^o_s \to \mathcal{D}'^o_s$. The proof of this requires an analysis of the degeneration of μ_p-torsors of punctured closed discs. Namely, the variation of the degree of the different over concentric discs (Prop. III.1.2.), which we combine in the case where the μ_p-torsor is induced by σ as above, with the study of the different of the discrete valuations at the generic points of irreducible components in $\mathcal{D}^o_s$. A first notable application is the following:

Theorem III.3.1. *Let σ be an order p automorphism of $D^o := \mathrm{Spec}\, R[\![Z]\!]$ having $m+1$ geometric fixed points and suppose $0 < m < p$. Then $\mathcal{D}^o_s$ has only one component, which is a projective line; i.e. the fixed points are all equidistant.*

Moreover, one can show that up to automorphism of the affine line, the specialization of the fixed points ($(m + 1)$-tuples) on this projective line belong to a finite set. For automorphisms σ with no inertia at (π), the radius of the closed disc which corresponds to this component is $\frac{1}{m}v(\zeta - 1)$, and this provides us with a hint for the description of the conjugacy class in $\mathrm{Aut}_R R[\![Z]\!]$ of such σ. In the final chapter we prove:

Theorem V.6.3.1. *For $0 < m < p$, modulo a change of parameter, there are only a finite number of order p automorphisms of the open disc with no inertia at (π), i.e. in $\mathrm{Aut}_R R[\![Z]\!]$ there is only a finite set of conjugacy classes of such order p automorphisms. Moreover, they occur when considering the p-cyclic covers of $\mathbb{P}^1_{\mathbb{Q}_p^{ur}}$ with potentially good reduction of type A_m, and are defined by the equation $Y^p = \prod_{0 \leq i \leq m} (1 - T_i X)^{h_i}$, where $(T_i)_i \in ({\mathbb{Z}_p}^{ur})^{m+1}$ are in $m + 1$ distinct classes $\bmod p$ and satisfy $h_0 T_0^k + h_1 T_1^k + \cdots + h_m T_m^k = 0$, $0 \leq k \leq m - 1$, for $(h_i)_{0 \leq i \leq m} \in (\mathbb{Z} \setminus p\mathbb{Z})^{m+1}$.*

We remark that the situation in the case $m > p$ is far from understood; in this case transposing Deuring's theory of normal forms for elliptic curves ($p = 2, m = 3$), to p-cyclic covers of $\mathbb{P}^1$ we show that trees with more than one terminal component occur naturally (Chapter III.5).

In chapter IV we give applications of the previous chapters to the local lifting question; namely, we show:

Proposition IV.1.1. *If p is 2 or 3 and $G = (\mathbb{Z}/p\mathbb{Z})^2$, then there is a G-cover $k[\![z]\!]/k[\![z]\!]^G$ which can be lifted to a G-cover $R[\![Z]\!]/R[\![Z]\!]^G$, where $R = \mathbb{Z}_p[(\zeta - 1)^{1/(p-1)}]$.*

And concerning meta-cyclic groups we prove the following:

Proposition IV.2.2.2. *Let $G = \langle\sigma,\tau\rangle$, with $\mathrm{o}(\sigma) = p$, $\mathrm{o}(\tau) = p-1$ and $\tau\sigma\tau^{-1} = \sigma^{h^{-1}}$ (h is a primitive $(p-1)$-th root of 1 modulo p). If $p > 2$, then there is a G-cover $k[\![z]\!]/k[\![z]\!]^G$, which can be lifted to a G-cover $R[\![Z]\!]/R[\![Z]\!]^G$, for $R = \mathbb{Z}_p[\zeta]$ and ζ a primitive p-th root of 1.*

Chapter V is concerned with an attempt to parametrize automorphisms of order p of the open disc (resp. those with no inertia at (π)) and to describe their conjugacy classes in $\mathrm{Aut}_R R[\![Z]\!]$. Roughly speaking we look at the relation

$$\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots + a_m Z^m + \cdots) \in R[\![Z]\!]$$

in terms of the a_i considered as indeterminates and expand the p-th iterate as a series

$$\sigma^p(Z) = Z(1 + E_1 Z + \cdots + E_n Z^n + \cdots),$$

where $E_n \in \mathbb{Z}_p[\zeta][a_i]$. The object we study is the common zero set $(a_i \in R)_{i\in\mathbb{N}}$ of the E_n. We show that if we give weight i to a_i, then E_n is a homogeneous form of weight n in the a_i, which is due to the action of $\mathbb{G}_m$ on the parameter Z. Moreover, the group of parameters $U^1(R[\![Z]\!]) := Z(1+ZR[\![Z]\!])$ acts on σ via conjugation, and so induces an action on E_n when taking the p-th iterate. One shows that E_p is an invariant form.

We conclude this study with a description of conjugacy classes in the cases $m = 0$, and $0 < m < p$ with no inertia at (π).

This paper is a revised version of a preprint we distributed in 1996; at that time we were only able to prove Theorem III.3.1 for $m = 2, 3$ and 4 in the case where there is no inertia at (π); our method was based on the study of semi-stable reduction of p-cyclic covers of $\mathbb{P}^1_K$ and gave us enough confidence to pose this theorem as a conjecture. In November 1996, M. Raynaud ([Ra 4]) communicated a proof sketch to us in the general case. This provided the framework for further study of order p automorphisms into which the examples we had treated previously fits perfectly. We are very grateful to M. Raynaud for giving us the opportunity to present his proof here and thank him for helpful discussions. We are also grateful to the referee for the many helpful suggestions he made, and in particular for pointing out to us how to use formal groups in order to produce order p^n automorphisms of the p-adic open disc.

I. Notation and the geometry of p-adic discs

In this section we intend to fix the notation.

1. p-adic open (resp. closed) discs.

1.1. Open discs. Recall that by using the Weierstrass Preparation Theorem [B], Chap. 7, p. 38, we can describe the geometry of the R-scheme $D^o := \mathrm{Spec}\, R[\![Z]\!]$. Namely, the special fibre $D^o_s := D^o \times_R k$ has only one closed point which corresponds to the ideal (π, Z) of $R[\![Z]\!]$, and the closed points of the generic fibre, $D^o_K := D^o \times_R K$, correspond to the irreducible distinguished polynomials of $R[\![Z]\!]$. These polynomials have roots in the maximal ideal of the integral closure R^{alg} of R in the algebraic closure K^{alg}. This allows us to identify D^o_K with the open disc $\{z \in R^{alg} \mid v(z) > 0\}$ modulo Galois action, where v is the unique extension of the v-adic valuation on K to K^{alg}.

The v-adic distance on the open disc $\{z \in R^{alg} \mid v(z) > 0\}$, induces a distance on the set $D^o(K)$ of K-rational points of D^o which is independent of the choice of parameter Z of $R[\![Z]\!]$.

When speaking about the open disc over R in the sequel, we shall refer to D^o or D^o_K without distinction.

1.2. Closed discs. These are defined in the same way as above, but replacing $R[\![Z]\!]$ by $R\langle Z\rangle := \{\sum_{n\geq 0} a_n Z^n \mid v(a_n) \to \infty\}$ and D^o by D^c. Note that the localisation at π is the Tate algebra $K\langle Z\rangle$ and so D^c_K is a closed disc.

In the following paragraphs everything settled for an open disc can be transposed to the case of a closed disc; this is left to the reader.

2. Semi-stable models of marked p-adic open (resp. closed) discs and oriented trees.

Let $F := \{(s_i)_{0\leq i\leq m} : \operatorname{Spec} K \to D^o\}$ be a finite set of rational points in D^o_K. The pair (D^o, F) is called a marked open disc. Assume that $m > 0$, let $Z_i = s_i(K)$ and choose $\rho \in R$ so that $v(\rho) := \inf_{0\leq j\leq m} v(Z_j - Z_i)$ is the radius of the smallest closed disc containing all the Z_i. Observe that $v(\rho)$ is independent of i. Let ${}^bD^o$ be the blowing up of D^o with respect to the ideal $(\rho, Z - Z_0)$. The special fibre is a projective line attached to the original generic point (π) of D^o_s in D^o. Let $z_i := \operatorname{sp} Z_i$ be the specialization of Z_i in ${}^bD^o_s := {}^bD^o \times_R k$; the formal fibre at z_i is the class of $Z_i \bmod \rho$ and if there is another Z_j in the Z_i class, then the process can be repeated with a new blowing up until we get a model $\mathcal{D}^o$ of the open disc D^o_K with $m+1$ sections $\int_i : \operatorname{Spec} R \to \mathcal{D}^o$ extending the s_i and giving $m+1$ (smooth) points in the special fibre.

By construction the special fibre $\mathcal{D}^o_s$ gives a tree of projective lines linked to the original generic point (π) by double crossing points, and this enables us to orient the tree starting from this "root" point. Each successive blowing up enlarges the tree representing the special fibre by a copy of $\mathbb{P}^1_k$ attached to it at a double crossing point. In this way we have a canonical infinite point, ∞, on each component $\mathbb{P}^1_k$, namely the first closed point of this component we meet in an injective path starting from the root (π). We shall denote the terminal components by E_i and by P_α the internal components.

The minimality of the construction means that each terminal component contains at least two points of the form $\int_i(k)$, and each internal component contains at least three points from the set consisting of the points of the form $\int_i(k)$ and the crossing points with other components. This model $\mathcal{D}^o$ is uniquely defined and we call it *the minimal semi-stable model of the marked open disc* (D^o, F).

3. Automorphisms of an open (resp. closed) disc and fixed points.

Let σ be an R-automorphism of $R[\![Z]\!]$. Then σ is defined by a series

$$\sigma(Z) = a_0 + a_1 Z + \cdots + a_i Z^i + \cdots,$$

and as it is an automorphism we must have $a_0 \in \pi R$ and $a_1 \in R^\times$. Moreover σ induces a $\operatorname{Spec} R$ automorphism of the open disc D^o, which we call $\tilde{\sigma}$. For rational points $(Z - Z_0) \in D^o$ one has $\tilde{\sigma}((Z - Z_0)) = (Z - \tilde{Z}_0)$, where $\tilde{Z}_0 = \sum_{i=0}^{\infty} a_i Z_0^i$. Such a point is a fixed point if and only if $Z_0 \in \pi R$ and $Z_0 = \sum_{i=0}^{\infty} a_i Z_0^i$. More generally, $P \in D^o$ is a fixed point if and only if $P = (\pi, Z), (\pi), (0)$ or is of height 1 and $P \supset (\sigma(Z) - Z)$. In the sequel we shall refer to this last set when we speak about fixed points. Moreover, we use the terminology *geometric fixed points* and denote by F_σ the points they define in the geometric generic fibre i.e. the zeroes in the maximal ideal of R^{alg} of the series $\sigma(Z) - Z$. Throughout the paper we shall always work with R-automorphisms and so drop the reference to R.

II. Order p automorphisms of p-adic discs

1. Automorphisms of order p with fixed points, the semi-stable model marked by the fixed points and variation of the different along a path.

If σ is an automorphism of $R[\![Z]\!]$ of order p, then it can happen that σ has no fixed point. From now on we shall consider σ's for which $F_\sigma \neq \phi$, say $F_\sigma := \{Z_0, ..., Z_m\}$; note that in [G-M] we have shown that if σ doesn't induce the identity residually (we say that σ has no inertia at (π)), then $|F_\sigma| = m+1$, where $m+1$ is the Hasse conductor of $\sigma \bmod \pi$ and $(m,p) = 1$. Moreover, as we are not working in a fixed discrete valuation ring, for convenience of the calculus we shall often assume that the Z_i are in R and so we can consider the minimal semi-stable model $(\mathcal{D}^o, F_\sigma)$ of the marked open disc (D^o, F_σ) (see I.2.). We denote by $\int_i : \operatorname{Spec} R \to \mathcal{D}^o$ the section such that $\int_i(K) = Z_i$. In this paragraph we describe the relevant elementary metric facts on fixed points in terms of the oriented tree $\mathcal{D}^o_s$.

After a translation we shall center the disc D^o in one of these points, say in $0 \in F_\sigma$. Then it follows ([Co], Lemma 14 p. 245) that there is a primitive p-th root $\zeta \in R$ giving the action of σ on the tangent space at 0, i.e.

$$\sigma(Z) = \zeta Z(1 + a_1 Z + a_2 Z^2 + \cdots).$$

This gives

$$\frac{\sigma(Z)}{Z} - 1 = (\zeta - 1) + a_1\zeta Z + a_2\zeta Z^2 + \cdots = \zeta(a_0 + a_1 Z + a_2 Z^2 + \cdots),$$

where $a_0 = \zeta^{-1}(\zeta - 1)$. In particular the roots of $\sigma(Z) - Z$ are distinct and using the Weierstrass Preparation Theorem we have the following factorisation:

$$\frac{\sigma(Z)}{Z} - 1 = \zeta a_m f_m(Z) u(Z),$$

where $m = \inf_{l \geq 0}\{l \,:\, v(a_l) \leq v(a_i) \text{ for all } i\}$, $u(Z) - 1 \in (\pi, Z)$ and $f_m(Z)$ is a unitary distinguished polynomial of degree m, so that $|F_\sigma| = m+1$. We remark that the integer m is also referred to as the Weierstrass degree of the series $\dfrac{\sigma(Z)}{Z} - 1$ in the literature.

Given $Z_i \in F_\sigma$, we want to study the tree $\mathcal{D}^o_s$ in a "neighborhood" of $z_i = \int_i(k)$. As said previously, for convenience we can assume that $Z_i = 0$. Given $\rho \in R^{alg}$ with $v(\rho) \geq 0$, after enlarging R so that $\rho \in R$, we let v_ρ be the Gauss valuation on $\operatorname{Fr}(R[\![Z]\!])$ relative to $\dfrac{Z - Z_i}{\rho} = \dfrac{Z}{\rho}$ and $d(v(\rho))$ be the degree of the different of the v_ρ-valued extension $\operatorname{Fr}(R[\![Z]\!])/\operatorname{Fr}(R[\![Z]\!]^{\langle\sigma\rangle})$. The Gauss valuation on $\operatorname{Fr}(R[\![Z]\!])$ relative to $\dfrac{Z}{\rho}$ is defined by

$$v_\rho\big(\sum_{n\geq 0} a_n Z^n\big) := \inf_{n \geq 0}\,\big(v(a_n) + n v(\rho)\big)$$

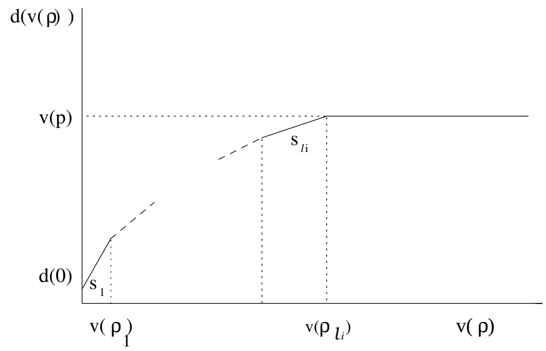
for $\sum_{n\geq 0} a_n Z^n \in R[\![Z]\!]$ and extended to $\operatorname{Fr}(R[\![Z]\!])$ in the canonical way. We remark that the residual extension is purely inseparable of degree p and $\dfrac{Z}{\rho}$ generates the valuation ring in $\operatorname{Fr}(R[\![Z]\!])$ over that of $\operatorname{Fr}(R[\![Z]\!]^{\langle\sigma\rangle})$. Therefore one has

$$d(v(\rho)) = (p-1)v_\rho\Big(\frac{\sigma(Z)}{Z} - 1\Big) = (p-1)\inf_{n\geq 0}(v(\zeta - 1), v(a_n) + n v(\rho)) \leq v(p).$$

Let $d(\sigma, Z_i)$ be the graph of $d(v(\rho))$ for $v(\rho) \in \mathbb{Q}^+$. One has $f_m(Z) = \prod_{Z_j \in F_\sigma, j \neq i} (Z - Z_j)$ and it follows that $d(\sigma, Z_i)$ is piecewise linear with breaks in the set $\{v(Z_j - Z_i),\ j \neq i\} := \{v(\rho_1), v(\rho_2), ..., v(\rho_{\ell_i})\}$, where $v(\rho_1) < v(\rho_2) < ... < v(\rho_{\ell_i})$.

Let μ_k, $1 \leq k \leq \ell_i$, be the cardinality of the set of $Z_j \in F_\sigma$ such that $v(\rho_k) \leq v(Z_j - Z_i) < \infty$; in particular $\mu_1 = m$ doesn't depend on the center Z_i. Then the gradient of $d(\sigma, Z_i)$ in the $\mathbb{Q}$-interval $]0, v(\rho_1)[$ is $s_1 := (p-1)m$ and in $]v(\rho_k), v(\rho_{k+1})[$ it is $s_{k+1} := (p-1)\mu_{k+1} < s_k := (p-1)\mu_k$. Note that $v(a_m) + \sum_{j\neq i} v(Z_j - Z_i) = v(\zeta - 1)$ so $d(0) = (p-1)v(a_m) \leq (p-1)v(\zeta - 1) = v(p)$ and for $v(\rho) \geq v(\rho_{\ell_i})$ one has $d(v(\rho)) = v(p)$.

We can represent the graph $d(\sigma, Z_i)$ as follows:



d(σZ i) graph

From its definition it follows that $d(0)$ is independent of the center Z_i; so we can assert:

Proposition 1.1. *If we let $\mu_{\ell_i+1} := 0$, then*

$$\sum_{1\leq j\leq \ell_i} (\mu_j - \mu_{j+1}) v(\rho_j) = \sum_{j\neq i} v(Z_j - Z_i) = -v(a_m) + v(\zeta - 1) = \frac{1}{p-1}(-d(0) + v(p))$$

is independent of i.

More generally we remark that if the two points Z_i, Z_j are near to each other, the two graphs $d(\sigma, Z_i)$ and $d(\sigma, Z_j)$ look the same. Precisely, from the definition of the different they coincide for $v(\rho) \leq v(Z_i - Z_j)$. In particular, in the case where $v(\rho_{\ell_i}) \leq v(Z_i - Z_j)$ (see definition above) it follows that $d(\sigma, Z_i)$ and $d(\sigma, Z_j)$ are equal and so $v(\rho_{\ell_i}) = v(\rho_{\ell_j})$, i.e. the fixed points which are in the immediate neighborhood of Z_i for the v-adic topology are equidistant and so a blowing up of D^o centered in the ideal $(\rho_{\ell_i}, Z - Z_i)$ distinguishes the specialization of these points. In other words:

Proposition 1.2. *The specializations of the fixed points in the minimal semi-stable model $(\mathcal{D}^o, F_\sigma)$ are in the terminal components.*

Remark 1.3. The graph $d(\sigma, Z_i)$ describes the Newton polygon of the polynomial $(Z - Z_i) f_m(Z - Z_i)$ and gives metric conditions on the minimal path on the tree between ∞ and $\int_i(k)$. Namely, the components we meet correspond to the breaks $v(\rho_k)$, $1 \leq k \leq \ell_i$, the value $d(v(\rho_k))$ to the different at the generic point of the component and the graph in the interval $]v(\rho_k), v(\rho_{k+1})[$ to the variation of the different in the formal fibre at the crossing point of the two corresponding components (this is an open annulus centered in Z_i).

Remark 1.4. Assume that the automorphism σ above is given by $\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots + a_m Z^m + \cdots)$, where $a_i \in \mathbb{Z}_p[\zeta]$. Then $f_m(Z) = \zeta - 1 + b_1 Z + \cdots + b_m Z^m \in \mathbb{Z}_p[\zeta][Z]$ is an Eisenstein polynomial and it follows that the fixed points are in the immediate neighborhood of 0, so that they are equidistant and the tree $\mathcal{D}_s^o$ has only one component.

2. Hurwitz data.

Definition 2.1. *Let σ be an order p automorphism of the open disc such that $F_\sigma = \{Z_0, Z_1, ..., Z_m\} \neq \phi$. Then $\sigma(Z - Z_i) = f'(Z_i)(Z - Z_i)(1 + b_1(Z - Z_i) + \cdots)$, where $f(Z)$ denotes the power series corresponding to the automorphism σ. As $\mathrm{o}(\sigma) = p$ it follows that $f'(Z_i)$ is a primitive p-th root of 1. We shall call the Hurwitz data of σ the $(m+1)$-tuple of integers, $H_\sigma = (h_0, h_1, ..., h_m)$, such that $f'(Z_i) = \zeta^{h_i^{-1}}$, where the integers h_i and their inverses are defined* $\bmod p$ *and are distinct* *from the class* $0 \bmod p$. *If* $e \in \mathbb{N}$ *with* $(e,p)=1$, *then* $H_{\sigma^{e^{-1}}} = (eh_0, eh_1, ..., eh_m)$. *Hence, when we speak of the Hurwitz data of the cover* $R[\![Z]\!]/R[\![Z]\!]^{\langle\sigma\rangle}$ *we mean the equivalence class of* H_σ *modulo the multiplication by* $\mathbb{F}_p^\times$.

As H_σ represents the action of σ on the tangent space at the fixed points, it follows that this doesn't depend on the choice of parameter for the open disc D^o.

3. Automorphisms with no inertia at (π) and p-cyclic covers of $\mathbb{P}^1_R$.

Order p automorphisms of the open disc with no inertia at (π) can be compactified as order p automorphisms of a complete smooth curve, and so doing generate p-cyclic covers of $\mathbb{P}^1_K$. We characterise these among p-cyclic covers of $\mathbb{P}^1_K$ in terms of their semi-stable reduction. We shall then use p-cyclic covers of $\mathbb{P}^1_K$ in order to produce order p automorphisms of the open disc with given Hurwitz data.

3.1. Compactification process.

We first introduce a definition which we shall use throughout the paper:

Definition 3.1.1. *Let k an algebraically closed field of characteristic $p>0$ and C be a smooth proper curve over k; let σ be a k-automorphism of C of order p. We shall say that the p-cyclic* cover $C \to C/\langle\sigma\rangle$ is of type A_m *if this is an étale cover of the affine line and the Hasse conductor at ∞ is $m+1$.*

Theorem 3.1.2. *Suppose R contains the p-th roots of unity and let σ be an automorphism of order p of $R[\![Z]\!]$ with no inertia at (π). Then there is a p-cyclic cover of $\mathbb{P}^1_K$ which has good reduction* mod π, *whose special fibre is totally ramified at a point say ∞, i.e. is a p-cyclic cover of $\mathbb{P}^1_k$ of type A_m, and is such that the cover induced at the formal fibre at ∞ is isomorphic to $R[\![Z]\!]/R[\![Z]\!]^{\langle\sigma\rangle}$.*

Proof. The extension $R[\![Z]\!]/R[\![Z]\!]^{\langle\sigma\rangle}$ is $k[\![z]\!]/(k[\![z]\!]^{\langle\sigma\rangle} = k[\![t]\!])$ modulo (π). Generically $k[\![z]\!]/k[\![t]\!]$ is defined by an Artin-Schreier equation $x^p - x = q(1/t)$, for a polynomial q without p-powers and of degree say $m = 1$ (so having Hasse conductor 2). If we set $s = 1/t$, then the extension of Dedekind domains $k[s,x]/k[s]$ can be lifted to an extension of affinoid algebras $K\langle S\rangle[X]/K\langle S\rangle$, where $[(\lambda X+1)^p - 1]/\lambda^p = Q(S)$ for some polynomial Q of degree m which lifts q. This p-cyclic cover extends to the disc $|S| \le |\pi'|^{-1}$ for some $|\pi'|<1$. Moreover, the germ of prolongation is unique up to isomorphism (see [Ra 1], Prop. 3.4.1) and determined by the extension $k[\![z]\!]/k[\![z]\!]^{\langle\sigma\rangle}$, thus one can apply the Prolongation Lemma III.1.1. of [G-M] in order to glue with the morphism of open discs $R[\![Z]\!]/R[\![Z]\!]^{\langle\sigma\rangle}$. This gives a p-cyclic cover of $\mathbb{P}^1_K$ which is étale outside $|S|>1$, ramified at the set of fixed points of σ, and which has good reduction given by the equation $x^p - x = q(s)$.

3.2. p-rank.

In order to characterise the p-cyclic covers which occur in this way, we recall some classical definitions concerning p-rank of curves (see [Ra 2]).

Let k be an algebraically closed field of characteristic $p>0$. Let X be a proper connected k-curve and J_X be its jacobian variety. The p-rank r_X of X is the dimension of the étale cohomology group $H^1(X, \mathbb{Z}/p\mathbb{Z})$ over $\mathbb{Z}/p\mathbb{Z}$.

Let μ_p be the kernel of the multiplication by p in $\mathbb{G}_m$. The canonical isomorphism $H^1(X,\mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{Hom}(\mu_p, J_X)$, implies that r_X is also the k-dimension of $H^1(X, \mathcal{O}_X)^{ss}$, which by definition is the biggest k-vector space in $H^1(X,\mathcal{O}_X)$ on which the Frobenius F of X is bijective. In particular $r_X \le g_X$, the genus $\dim_k H^1(X,\mathcal{O}_X)$ of X.

Assume that the curve X is reduced with only ordinary double points as singularities (a semi-stable curve). To this curve one associates a graph Γ_X whose vertices are the irreducible components of X and whose edges correspond to the double points. If $\tilde{X}$ be the normalisation of X, then $r_X = r_{\tilde{X}} + \dim_{\mathbb{Z}} H^1(\Gamma_X, \mathbb{Z})$ and in particular $r_X = 0$ if and only if the p- rank of each normalised irreducible component is 0 and the graph Γ_X is a tree.

Assume now that X is a smooth proper connected curve and is a p-cyclic cover of $\mathbb{P}^1_k$. One has $r_X - 1 = p(0-1) + r(p-1)$, where r is the number of ramified points (Deuring-Šafarevič formula [D1], [Sa]; see [Cr] for a modern treatment). In particular $r_X = 0$ if and only f $r = 1$; in other words if and only if the cover is totally ramified say at ∞ and so is given by an Artin-Schreier equation $x^p - x = q(1/t)$, where q is a polynomial which can be taken without p-powers and of degree say m (so having conductor $m+1$ at ∞). This is a p-cyclic cover of $\mathbb{P}^1_k$ of type A_m. Hence we have proved that:

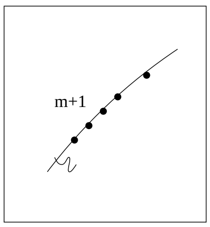
Proposition 3.2.1. *The p-cyclic covers of $\mathbb{P}^1_K$ which occur in the theorem above are those which have good reduction with p-rank equal to 0.*

Remark 3.2.2. One cannot expect a characterisation without fixing the type of reduction (here potentially good reduction) because there are p-cyclic covers of $\mathbb{P}^1_K$ which have a semi-stable reduction with p-rank zero, but are not smooth (see [Ra 3], Th.2).

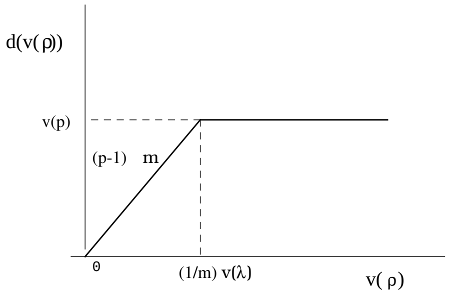
In conclusion, the theory of automorphisms of order p of the p-adic open disc (with no inertia at (π)) is a by-product of the study of the semi-stable reduction of p-cyclic covers of $\mathbb{P}^1_K$. In sections III and V we shall use this correspondence in order to build and classify order p automorphisms of the open disc.

3.3. Examples.

3.3.1. [O–S–S] example. Let $(m,p) = 1$ and $\sigma(Z) = Z(\zeta + Z^m)^{-1/m}$. Note that here there is no ambiquity in the sense that among the m-th roots of $\zeta + Z^m$ we mean the one which expanded at 0 gives $\sigma(Z) = \zeta^{-1/m}Z + \cdots$. Then $\mathrm{o}(\sigma) = p$, the inertia group of σ at (π) is trivial, F_σ consists of $m+1$ fixed points, the oriented tree $\mathcal{D}^o_s$ has one component (compare with Remark 1.4. above) and $H_\sigma = (-m, 1, 1, ..., 1)$, i.e. at least m values are the same.



$\mathcal{D}^o_s$



d(σ, 0) graph

Proof. Consider the Artin-Schreier cover $x^p - x = \dfrac{1}{t^m}$ that we lift to

$$\frac{(\lambda X + 1)^p - 1}{\lambda^p} = \frac{1}{T^m},$$

(here $\lambda := \zeta - 1$). This is a p-cyclic cover of $\mathbb{P}^1$ with good reduction of type A_m, moreover $Z = X^{-1/m}$ is a parameter for the disc over $|T| < 1$. Let σ be the automorphism such that $\sigma(\lambda X + 1) = \zeta(\lambda X + 1)$. Then

$$\frac{\sigma(Z)}{Z} = (\zeta + Z^m)^{-1/m}, \quad \text{with series} \quad f(Z) = Z(\zeta + Z^m)^{-1/m} = \zeta^{-1/m}Z + \cdots$$

and

$$F_\sigma := \{0\} \cup \{\, m\text{-th roots of } -\lambda \,\}.$$

In order to describe H_σ one can easily calculate the derivative f' at the fixed points. Another way that we shall use in the sequel is use the global equation between X and T in order to calculate locally the action of σ on the tangent spaces at the ramification locus. One obtains $H_\sigma = (-m, 1, 1, \ldots, 1)$.

3.3.2. Automorphisms of order p which are p-powers.

Here we use [G-M]: Let $(m_1, p) = 1$ and consider the extension of $k[\![t]\!]$ defined by

$$x^p - x = c(t^{-pm_1}, -t^{-m_1}),$$

where $c(x,y) := [(x+y)^p - x^p + (-y)^p]/p$ and the conductor is $m+1 = pm_1(p-1) + m_1 + 1$.

Note that $\sigma(x) = x+1$ is the p-th power of the automorphism defined by

$$\tau(t^{-m_1}) = t^{-m_1} + 1, \quad \tau(x) = x - c(t^{-m_1}, 1).$$

We could lift in the [O-S-S] manner, but prefer to lift τ, i.e. we lift σ as a p-power. Consider the p-cyclic cover of $\mathbb{P}^1$ defined by the equation

$$\big(\lambda X + \mathrm{Exp}_p(\frac{\mu}{T^{m_1}})\big)^p = (1 + \frac{\lambda}{T^{m_1}})\mathrm{Exp}_p(\mu^p Y)$$

where $Y = \big((\frac{\lambda}{T^{m_1}} + 1)^p - 1\big)/\lambda^p$, $\lambda = \zeta_{(2)}^p - 1$, $\pi := \zeta_{(2)} - 1$ and $\mu = \mathrm{Log}_p(1+\pi)$ (here $\zeta_{(2)}$ denotes a primitive p^2-root of unity and we use the notation G_p to indicate the truncation at Z^p of $G \in R[\![Z]\!]$).

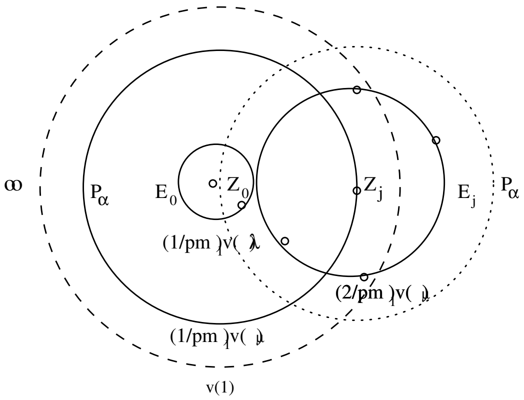
The branch locus is

$$\{0\} \cup \{\text{ roots of } T^{m_1} = -\lambda\} \cup \{\text{ roots of } \mathrm{Exp}_p(\mu^p Y) = 0\}$$

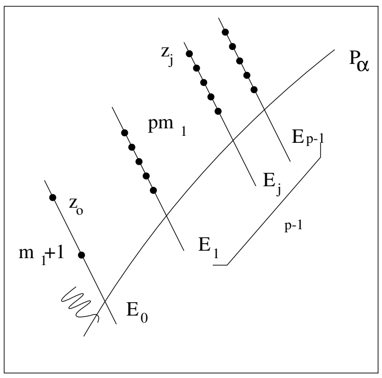
so over the open disc $|T| < 1$, the generic different $d_\eta = (1 + m_1 + p(p-1)m_1)(p-1)$ and the special different $d_s = (m+1)(p-1)$ are equal. It follows (see [G-M] I.3.4), that the cover is of type A_m and above the disc $|T| < 1$ we have a disc with parameter $Z = X^{-1/m}$ and a Galois generator is given by $\sigma(X) = \zeta X + \mathrm{Exp}_p(\frac{\mu}{T^{m_1}})$.

As the roots giving the branch locus at finite distance are simple it follows as in the preceding case that $H_\sigma = (-m, 1, 1, \ldots, 1)$.

Representative diagram (geometry of F_σ): We intend to represent F_σ inside the generic fibre D_K, using the following convention: Open (resp. closed) discs are represented by dotted (resp. solid) circles. Moreover, the class of a point in a given closed disc is represented by an open disc with the same radius centered at a point of the closed disc.

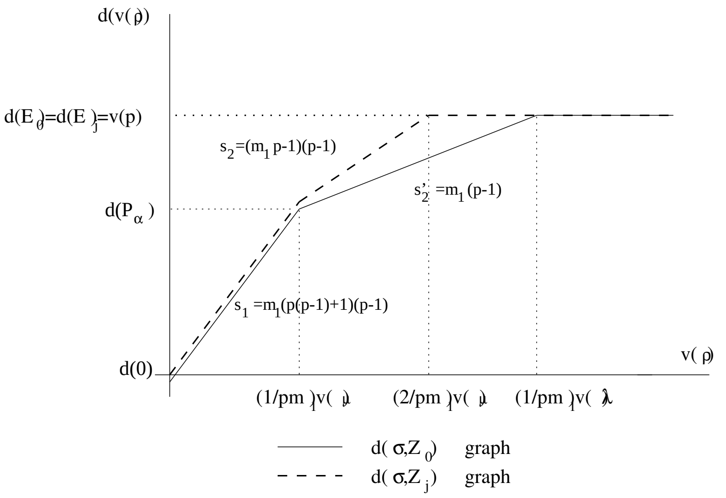


Geometry of F σ



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

The graphs $d(\sigma, Z_0)$ and $d(\sigma, Z_j)$:



3.3.3. Automorphisms of order p^ℓ and Lubin-Tate formal groups.

We would like to thank the referee for pointing out the following method of producing order p^ℓ automorphisms of p-adic open discs without inertia at π, for $\ell \geq 1$. Although these automorphisms have quite special numerical data, for $\ell \geq 3$ this is the only way we know of producing such automorphisms. Although we will concentrate on the case $\ell = 1$ below, the reader may easily adapt the reasoning to the general case. Our reference to formal groups is [H].

Let K be a finite totally ramified degree n extension of $\mathbb{Q}_p[\zeta]$, where ζ is a primitive p-th root of unity. Let R be the ring of integers in K and π be a uniformizing parameter. We consider the series

$$f(Z) := Z + \frac{Z^p}{\pi} + \ldots + \frac{Z^{p^k}}{\pi^k} + \ldots \in K[\![Z]\!],$$

observing the important fact that $f(Z)$ converges on the open disc $\{z \in K \mid v(z) > 0\}$.

Then (see [H] p. 46)

$$F(Z_1, Z_2) := f^{-1}(f(Z_1) + f(Z_2)) \in R[\![Z_1, Z_2]\!]$$

and

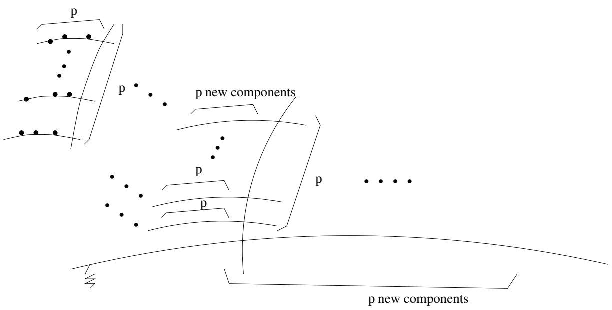
$$[\pi]_F(Z) := f^{-1}(\pi f(Z)) \in R[\![Z]\!],$$

and so defines a Lubin-Tate formal group, i.e., $[\pi]_F(Z) \equiv \pi Z \bmod Z^2$ and $f(Z) \equiv Z^p \bmod \pi$. It is easily seen that for any $a \in R$ there is a unique series $[a]_F(Z) \in R[\![Z]\!]$ such that $[a]_F(F(Z_1, Z_2)) = F([a](Z_1), [a](Z_2))$ and $[a]_F(Z) \equiv aZ \bmod Z^2$. Moreover, the map $a \to [a]_F(Z)$ defines an injective homomorphism from R to the endomorphism ring of the formal group law $F(Z_1, Z_2)$. Hence, in particular, $\sigma(Z) := [\zeta](Z) = f^{-1}(\zeta f(Z))$ is an order p-automorphism of $R[\![Z]\!]$.

We now describe the fixed points of $\sigma(Z)$ and the corresponding Hurwitz data. Using the equality $\zeta - 1 = u\pi^n$ for some unit $u \in R$, it follows that $[\zeta - 1](X) \equiv (\zeta - 1)Z \bmod Z^2$ and that $[\zeta - 1](Z) \equiv Z^{p^n} \bmod \pi$. One deduces that $\sigma(Z) - Z$ has Weierstrass degree p^n (see II.1) and so σ has p^n fixed points. If we let z be such a fixed point, then the relation $f(\sigma(Z)) = \zeta f(Z)$ shows that z is a root of $f(Z)$ in the open disc (although the converse is false). Moreover, differentiating and evaluating at z one obtains $f'(z)\sigma(Z)'_{Z=z} = \zeta f'(z)$, and as $f'(z) \equiv 1 \bmod \pi$, it follows that $\sigma(Z)'_{Z=z} = \zeta$, i.e. $H_\sigma = (1, 1, \ldots, 1)$.

Now we describe the geometry of F_σ : First we remark that it is easy to describe the zeroes of $f(Z)$ inside the open disc. Indeed, examining the Newton polygon of the Laurent series $f(Z)$ we see that the non-trivial zeroes lie on circles centered at 0 and having radii $v(z) = 1/(n(p-1)^2 p^{m-1})$, for any $1 \leq m$. On each such circle there are $p^m - p^{m-1}$ zeroes and an exercise shows that these points are in p distinct classes counting the zero class. Moreover, the geometry in each class mimics that in the zero class. In fact the congruence $\sigma(Z) \equiv Z^{p^n} \bmod \pi$ shows that the zeroes z of $f(Z)$, which are also fixed points of σ, have radius $v(z) > 1/(n(p-1)^2 p^n)$. As $p^n = 1 + (p-1) + (p^2 - p) + \cdots + (p^n - p^{n-1})$ it follows that the fixed points of σ are exactly 0 and the zeroes of f on the circles of radius $v(z) = 1/(n(p-1)^2 p^{m-1})$ about 0, for $1 \leq m \leq n$. It follows that the oriented tree $\mathcal{D}_s^o$ is characterized by the property that on each internal component there are p new branching components and that there are p fixed points on each terminal component. (One could equally well say that the dual graph is a tree having valency p at each vertex). Note that each oriented path of maximal length has n edges, which is the same as asserting that the graphs $d(\sigma, Z_i)$ have n breaks. Moreover, these graphs all coincide and this gives us a way of producing trees of arbitrary length.

The oriented tree for $\mathcal{D}_s^o$ has the following representation:



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

III. Geometry of the fixed points of order p automorphisms

The aim of this section is to define geometric data associated with the minimal semi-stable model $(\mathcal{D}^o, F_\sigma)$. Namely, we want to describe the morphism

$$(\mathcal{D}^o, F_\sigma) \to (\mathcal{D}^o, F_\sigma)/\langle\sigma\rangle.$$

We first give the equation of a μ_p-torsor over a punctured closed disc which is trivial $\bmod \pi$, and combining this with our study of the variation of the different in II.1, we are able to describe the μ_p-torsors which occur in the case of order p automorphisms.

1. Degeneration of μ_p-torsors over a punctured closed disc.

Recall that R contains ζ, a primitive p-th root of unity. The following proposition is a geometric version of known results on the classification of p-cyclic extensions of discrete valuation rings with non-perfect residue fields.

Proposition 1.1. *Let $A := R\langle T\rangle$, $D^c := \mathrm{Spec}\ A$ and $\varphi : X \to D^c$ be a normal generic μ_p-torsor (i.e. a μ_p-torsor on some open $U \subset D^c$) such that X_s is reduced and the branch locus* Br *strictly contains $V(\pi)$. Let $\Delta \in R[T]$ be unitary such that the branch locus Br_K of φ_K is $V(\Delta)$. We write $X = \mathrm{Spec}\ B$ and let $d(0)$ be the degree of the different of the extension $\mathcal{O}_{X,\pi}/\mathcal{O}_{D^c,\pi}$, where $\mathcal{O}_{X,\pi}$ (resp. $\mathcal{O}_{D^c,\pi}$) denotes the local ring of X (resp. D^c) at (π). Then, after suitably enlarging R, two cases can occur:*

1. μ_p-type degeneration: $d(0) = v(p) := e$. An equation of the torsor is $Y^p = u$ where $u \in A[\frac{1}{\Delta}]^\times$. Let $\bar{u}$ be the image of u in $k(t) := \mathrm{Fr}(A/(\pi))$. Then $\bar{u} \notin k(t)^p$ is uniquely defined up to multiplication by a p-power. Moreover, $A[\frac{1}{\Delta}][Y]$ is integrally closed and so $\varphi^{-1}(D^c \setminus V(\Delta)) =$ $\mathrm{Spec}\, A[\frac{1}{\Delta}][Y]$.

2. α_p-type degeneration: $d(0) < v(p) = e$. There is a unitary polynomial $\Delta_1 \in R[T]$ such that $V((\pi, \Delta_1)) = V((\pi, \Delta))$, and an equation for the torsor is $Y^p = 1 + \pi^{pt} u \in A[\frac{1}{\Delta_1}]^\times$, where $u \in A[\frac{1}{\Delta}]$. Here $\bar{u} \notin k(t)^p$ is uniquely defined up to addition of a p-power. It follows that $A[\frac{1}{\Delta_1}][\frac{Y-1}{\pi^t}]$ is integrally closed, so $\varphi_s^{-1}(D_s^c \setminus V((\pi, \Delta)) = \mathrm{Spec}\, A/(\pi)[\frac{1}{\Delta}][(\overline{\frac{Y-1}{\pi^t}})]$. Moreover, $0 < t < \frac{e}{p-1}$ and $d(0) = e - (p-1)t$.

Proof. By Kummer theory the torsor is defined by an equation $Y^p = UP$, where U is a unit in A congruent to $1 \bmod \pi$, the polynomial $P = \prod_{i,j}(T - T_{i,j})^{n_{i,j}} \in R[T]$, with $n_{i,j} \in \mathbb{N} \setminus p\mathbb{N}$, and the pairwise distinct $T_{i,j} \in R$ are listed in such a way that T_{i_1,j_1} and T_{i_2,j_2} are in the same class mod π if and only if $i_1 = i_2$. Now we can distinguish two cases:

1) There exists i such that $p \not| \sum_j n_{i,j}$: Then $\mathcal{O}_{X,\pi} = \mathcal{O}_{D^c,\pi}[X]$ and $d(0)$ is the valuation of the derivative pY^{p-1}, i.e. $d(0) = v(p)$. Let $\Delta = \prod_{i,j}(T - T_{i,j})$. Then φ is étale outside $V(\pi\Delta)$ so $\varphi^{-1}(D^c \setminus V(\pi\Delta)) = \mathrm{Spec}\ KA[\frac{1}{\Delta_1}][Y]$, and as $\mathcal{O}_{X,\pi} = \mathcal{O}_{D^c,\pi}[Y]$ it follows that $\varphi^{-1}(D^c \setminus V(\Delta)) =$ $\mathrm{Spec}\, A[\frac{1}{\Delta}][Y]$.

2) P is a p-th power mod π, i.e. $n_i = \frac{1}{p}\sum_j n_{ij} \in \mathbb{N}$. Then setting

$$\Delta = \prod_{i,j}(T - T_{i,j}) \qquad \text{and} \qquad P^\star := \prod_i (T - T_{i,0})^{n_i},$$

it follows $UP = UP^{\star p}\frac{P}{P^{\star p}} = P^{\star p}(1 + \pi^{s_1}P_1)$, where $P_1 \in A[\frac{1}{\Delta}]$, $P_1 \not\equiv 0 \bmod \pi$ and $s_1 \in \mathbb{N}^\times$.

Now an equation of our μ_p-torsor is $Y_1^p = 1 + \pi^{s_1}P_1 \in A[\frac{1}{\Delta}]^\times$. Let $\lambda = \zeta - 1$ and write $Y_1 = \lambda X_1 + 1$. Then $\frac{(\lambda X_1 + 1)^p - 1}{\lambda^p} = \frac{\pi^{s_1}}{\lambda^p}P_1$. As the inertia group at π is the full group $\langle\sigma\rangle$, it follows that $v(\frac{\pi^{s_1}}{\lambda^p}) < 0$, i.e. $s_1 < \frac{pe}{p-1}$. Moreover $s_1 = pt_1$, $t_1 \in \mathbb{N}$, for otherwise we contradict the reducedness of X_s.

If P_1 is a p-power mod π we write $P_1 = -{Q_1}^p + \pi R_1$, where $Q_1, R_1 \in A[\frac{1}{\Delta}]$, and then ${Y_1}^p = 1 - \pi^{pt_1}{Q_1}^p + \pi^{pt_1+1}R_1$. As $v(p\pi^{pt_1}) \geq pt_1 + 1$, one can write $Y_1^p = (1 - \pi^{t_1}Q_1)^p + \pi^{pt_1+1}R_2$, for $R_2 \in A[\frac{1}{\Delta}]$. Setting $c := 1 + \pi^{t_1}Q_1$ it follows that $(cX_1)^p = (1 - (\pi^{t_1}Q_1)^2)^p + \pi^{pt_1+1}R_2(1 + \pi^{t_1}Q_1)^p =$ $1 + \pi^{s_2}P_2$, with $P_2 \in A[\frac{1}{\Delta}] \neq 0 \bmod \pi$ and $s_2 > pt_1$. Note that c has no reason to be invertible in $A[\frac{1}{\Delta}]$, nevertheless mod π its zero set lies in $V((\pi, \Delta))$ and so for suitable Δ_1 as in the statement of 2) one has $1 + \pi^{s_2}P_2 \in A[\frac{1}{\Delta_1}]^\times$.

Now as for s_1 one proves that $s_2 = pt_2$ with $t_2 \in \mathbb{N}$ and $0 < t_1 < t_2 < \frac{e}{p-1}$. So after a finite number of steps, for suitable Δ_1 as in the statement of 2) we get the desired form of the equation, $Y^p = 1 + \pi^{pt}u \in A[\frac{1}{\Delta_1}]^\times$, where u is not a p-th power mod π. By setting $Y = \pi^t Z + 1$ it follows that $Z^p = u \bmod \pi$, and if $f(Z) := \dfrac{(\pi^t Z+1)^p-1}{\pi^{pt}} - u$, then $f'(Z) = \dfrac{p}{\pi^{(p-1)t}}(\pi^t Z+1)^{p-1}$, so that $d(0) = v(\dfrac{p}{\pi^{(p-1)t}})$ as announced.

Suppose we have another equation $Y'^p = 1+\pi^{ps}v$ for the torsor, where v is not a p-power mod π. Then $s=t$, via calculation of the different. Moreover,

$$\frac{1+\pi^{pt}v}{1+\pi^{pt}u} = 1+\pi^{pt}(v-u) + \text{ something small}$$

is a p-power in $\mathrm{Fr}(A)$ and so the equation $Z^p = \dfrac{1+\pi^{pt}v}{1+\pi^{pt}u}$ is reducible. It follows $v-u$ is a p-power mod π.

The remaining assertions follow from similar valuation theoretic arguments to those of case 1) and are left to the reader.

In the case of α_p degeneration we can study the gradient of the different for concentric closed discs.

Proposition 1.2. *We keep the same hypotheses as above and assume the degeneration is of α_p-type. Let $\omega_\alpha := d\bar{u}$. Then ω_α is uniquely determined, has its set of poles in $V(\bar{\Delta})$, and if m_0+1 is the order of a pole, then $(m_0,p)=1$. After a translation we can assume that $0 \in V(\Delta)$ gives a pole in reduction. Let $\rho \in R^{alg}$, then after enlarging the base ring, the degree of the different $d(v(\rho))$ in the torsor above the annulus of zero thickness $v(T) = v(\rho^p)$, centered in $0 \in V(\Delta)$, is a linear function of gradient $(p-1)m_0$ for $v(\rho)$ small enough.*

Proof. Suppose $Y^p = 1+\pi^{pt}u$ is an equation of the torsor such that $\bar{u}$ has a pole at 0 of order m_0. Then if $p|m_0$, after multiplying the equation defining the torsor by

$$(1-c\frac{\pi^t}{T^{m_0/p}})^p,$$

for conveniently chosen $c \in R^{alg}$, we get a new equation and in reduction a pole of order smaller than m_0. Hence after iteration of this procedure we can assume that $(m_0,p)=1$ and so ω_α has the good order at 0. Now one can write $u = \dfrac{P}{\Delta_0\Delta_1}$ where $P \in A$, $\Delta_0 = \prod_{0\le j\le m_0}(T-T_{0,j})$, $v(T_{0,j})>0$ and $\Delta_1 = \prod_{i>0}(T-T_{i,j})$ with $v(T_{i,j}) = 0$. Moreover in reduction $\overline{P}$ and $\overline{\Delta_0\Delta_1}$ are coprime. Suppose $T = \rho^p S$, then for $pv(\rho) < \inf v(T_{0,j})$ it follows that $u = \rho^{-pm_0}(\dfrac{1}{S^{m_0}} + \text{something small})$; here we mean small for the S-Gauss valuation. As $(m_0,p)=1$, it follows that if we replace Y by $\pi^t\rho^{-m_0}Z+1$ in the equation of the torsor we get an integral equation for Z and from this we deduce $d(v(\rho)) = d(0) + (p-1)m_0 v(\rho)$ as claimed.

2. The geometric tree of an order p automorphism.

Now we present the principal theorem of this paper, first recalling the notations for convenience:

Let σ be an order p automorphism of $D^o := \mathrm{Spec}\, R[[Z]]$, with a nonempty set F_σ of geometric fixed points. $\mathcal{D}^o$ denotes the minimal semi-stable model of the marked open disc (D^o, F_σ) (cf. II.1) and $\varphi : \mathcal{D}^o \to \mathcal{D}^o/\langle\sigma\rangle := \mathcal{D}'^o$. The special fibres $\mathcal{D}^o_s$ (resp. $\mathcal{D}'^o_s$) are endowed with tree structure and oriented from the original generic point (π) of D^o_s in D^o, (cf. I.2). Moreover, they are homeomorphic via φ_s.

Let E_i, E'_i (resp. P_α, P'_α) denote the terminal (resp. the internal) components of $\mathcal{D}^o_s$ and $\mathcal{D}'^o_s$. The canonical infinite points on these components determined by the tree structure are denoted by ∞_i (resp. ∞_α). Suppose $\{Z_{i,j},\ 0\le j\le m_i\}$ is the set of σ's fixed points whose specialization $z_{i,j}$ lies in E_i and let $T_{i,j} = \varphi(Z_{i,j})$, $t_{i,j} := \varphi_s(z_{i,j}) \in E_i'$ and $h_{i,j}$ be the Hurwitz data at $Z_{i,j}$. Given an internal component P_α' let $t_{\alpha,n} \in P_\alpha'$, $1 \leq n \leq n_\alpha$, be its crossing points. To each point $t_{\alpha,n}$ we associate the terminal components E_i', indexed by $i \in I_n$, which are connected to $t_{\alpha,n}$ by a positive path. We set $m_{\alpha,n} + 1 := \sum_{i \in I_n}(m_i + 1)$. Then:

Theorem 2.1. *There exist functions $\bar{u}_i \in k(E_i')$ with $\operatorname{ord}_{\infty_i}\bar{u}_i = 0$, such that the differentials $\omega_i = d\bar{u}_i$ have divisor support in $\{t_{i,j}\}_j \cup \{\infty_i\}$ and satisfy $\operatorname{ord}_{t_{i,j}}\omega_i \equiv h_{i,j} - 1 \bmod p$ and $\operatorname{ord}_{\infty_i}\omega_i = m_i - 1$. Moreover, $(m_i, p) = 1$ and $\sum_j h_{i,j} \equiv 0 \bmod p$.*
There exist functions $\bar{u}_\alpha \in k(P_\alpha')$ such that the differentials $\omega_\alpha = d\bar{u}_\alpha$ have divisor support in the points $\{t_{\alpha,n}\}_n \cup \{\infty_\alpha\}$ and $\operatorname{ord}_{t_{\alpha,n}}\omega_\alpha = -(m_{\alpha,n} + 1) < 0$ and $\operatorname{ord}_{\infty_\alpha}\omega_\alpha = -2 + \sum_n(m_{\alpha,n} + 1)$. Moreover, $(m_{\alpha,n}, p) = 1$ and $(-1 + \sum_n(m_{\alpha,n} + 1), p) = 1$.

Proof. We first prove the result for the terminal components. From Prop. II.1.2 we know that for given i the fixed points $Z_{i,j}$ have equal mutual distance. Hence an equation for the torsor induced by σ above the closed disc $\operatorname{Spec} R\langle T\rangle$ corresponding to $E_i \setminus \{\infty_i\}$ is $X^p = u_i \in R\langle T\rangle$, with $u_i = \prod_j (T - T_{i,j})^{n_{i,j}}(1 + \text{something small})$, $(n_{i,j}, p) = 1$ and the $T_{i,j}$ in distinct classes. Moreover, as the equation is defined modulo multiplication by p-th powers it follows that the indices $n_{i,j}$ are equal $\bmod p$ to the Hurwitz data $h_{i,j}$.

Now we know (Prop. III.1.1.) that outside ∞_i and the specialization $t_{i,j}$ of $T_{i,j}$, the equation mod π defines a smooth k-curve. It follows that the divisor of $\omega_i := d\bar{u}_i$ has support in $\{\infty_i\} \cup \{t_{i,j}\}_j$. For the rest of the assertion we remark that $\operatorname{ord}_{\infty_i}\bar{u}_i = 0 \bmod p$; otherwise we can assume that $(\operatorname{ord}_{\infty_i}\bar{u}_i, p) = 1$ so $\operatorname{ord}_{\infty_i}\omega_i = \operatorname{ord}_{\infty_i}\bar{u}_i - 1$ and $-2 = \deg \omega_i = \sum_j (n_{i,j} - 1) + \operatorname{ord}_{\infty_i}\bar{u}_i - 1$; i.e. $m_i = 0$ which contradicts the minimality of $\mathcal{D}^o$. So $\operatorname{ord}_{\infty_i}\bar{u}_i = 0$, and this implies that $\sum_j h_{i,j} = 0 \bmod p$, moreover the same calculation now gives $\operatorname{ord}_{\infty_i}\omega_i \equiv m_i - 1 \bmod p$. By multiplying u_i by a suitable p-power of T we can assume that $\operatorname{ord}_{\infty_i}\bar{u}_i = \sum_j n_{i,j} = 0$ and $\operatorname{ord}_{\infty_i}\omega = m_i - 1$.

Now we prove the result for the internal components. By consideration of the variation of the different along a path, see II.1, it follows that the μ_p-torsor over the closed disc corresponding to $P_\alpha \setminus \{\infty_\alpha\}$ is of α_p-type, see Prop. III.1.1, and we have an equation $X^p = 1 + \pi^{pt_\alpha}u_\alpha$. We know, by Prop. III.1.1, that after writing $X = \pi^{t_\alpha}Z + 1$ this equation induces the equation $z^p = \bar{u}_\alpha$ of the cover P_α/P_α', outside the crossing points $t_{\alpha,j}$ and ∞_α. As P_α is a projective line it follows that this equation defines a smooth k-curve outside the crossing points $t_{\alpha,j}$ and ∞_α. Hence $\omega_\alpha := d\bar{u}_\alpha$ has divisor support in $t_{\alpha,j}$ and ∞_α. In order to calculate the order in $t_{\alpha,j}$ we use Prop. III.1.2, which expresses the gradient of variation of the different near the boundary as $(p-1)(-\operatorname{ord}_{t_{\alpha,j}}\omega_\alpha - 1)$. On the other hand in II.1 we show that the gradient is $(p-1)m_{\alpha,n}$ where $m_{\alpha,n} + 1$ is the number of σ fixed points which specialize to points of the tree after $t_{\alpha,n}$, so $\operatorname{ord}_{t_{\alpha,n}}\omega_\alpha = -(m_{\alpha,n} + 1)$.

Corollary 2.2. *Let σ be an order p automorphism of $D^o := \operatorname{Spec} R[\![Z]\!]$ with $m+1$ geometric fixed points. Then $m = 0$ or $(m, p) = 1$.*

3. Geometric trees in case $m \leq p + 1$.

As an application of Theorem III.2.1 we prove:

Theorem 3.1. *Let σ be an order p automorphism of $D^o := \operatorname{Spec} R[\![Z]\!]$ having $m+1$ geometric fixed points and suppose $0 < m < p$. Then $\mathcal{D}_s^o$ has only one component, which is a projective line; i.e. the fixed points are all equidistant.*

Proof. Assume that $1 < m < p$ and that the tree $\mathcal{D}_s^o$ has more than one terminal component. Choose a path originating at ∞ (which is given by the original closed point (π, Z)) of maximal length. At the end of the path we have an internal component P_α' with only terminal components say E_i', $1 \leq i \leq I$, and $I > 1$ due to the minimality of the model. Let t be a parameter for $P_\alpha' \setminus \{\infty_\alpha\}$ and $t = t_i$ be the crossing points, all of them are assumed to be distinct from 0, after a possible translation. Then $\omega_\alpha = d\bar{u}_\alpha$ and we can assume that the poles of $\bar{u}_\alpha$, which are contained in $\{t_i\}_i$, have orders m_i which are prime to p (see the notations in Th. III.2.1). We can write

$$\bar{u}_\alpha = \frac{P(t)}{\prod_i (t-t_i)^{m_i}}.$$

As ω_α has a zero at ∞_α of order $-2+\sum_i(m_i+1) > 0$, it follows that $\bar{u}_\alpha$ is defined at ∞_α, so $\deg P \leq n := \sum_i m_i$. Changing $\bar{u}_\alpha$ to $a\bar{u}_\alpha + b$ if necessary, one can assume that

$$\bar{u}_\alpha = \frac{\prod_{1\leq j\leq n}(1-a_j s)}{\prod_i (1-t_i s)^{m_i}}$$

where $s = t^{-1}$ is a parameter at ∞_α.

The Taylor expansion at $s=0$ gives

$$1 + cs^{-1+\sum_i (m_i+1)}(1+o(s)) + r(s)$$

where the differential $d(r) = 0$. Now we remark that $\sum_i (m_i+1) \leq m+1 < p+1$, i.e. $-1+\sum_i(m_i+1) < p$ and so we can assume that $r(s)=0$. Examining the identity

$$\prod_{1\leq j\leq n}(1-a_j s) = (1+cs^{-1+\sum_i(m_i+1)}(1+o(s)))(\prod_i (1-t_i s)^{m_i})$$

together with the inequality $n = \sum_i m_i < -1+\sum_i(m_i+1)$ we deduce that $\bar{u}_\alpha = 1$, which is a contradiction.

Remark 3.1.1. In order to achieve the result in the proof above we could also remark that $t \to \overline{u}_\alpha$ defines a cover of $\mathbb{P}^1_k$, whose branch locus is given by the image of the support of $d\overline{u}_\alpha$, i.e. $0, \infty$. Moreover, the ramification indices are the the set of m_i and $-1+\sum(m_i+1) \leq m < p$, so the cover is a tame cover of $\mathbb{P}^1_k \setminus \{0,\infty\}$. Now we know that such a cover is as in char. 0, i.e. it is cyclic, so totally ramified. In particular above ∞ there is only one point; consequently $\overline{u}_\alpha$ has only 1 pole, which contradicts the minimality of the model.

Following the same line of reasoning from Theorem III.2.1 we deduce:

Theorem 3.2. *Let σ be an order p automorphism of $D^o := \operatorname{Spec} R[[Z]]$ with $m+1$ geometric fixed points. If $m = p+1$, then the tree $\mathcal{D}^o_s$ has at most two terminal components.*

Proof. Assume $m = p+1$ and that the tree has at least 3 terminal components and consider a path of maximal length. If we get the same picture as in the preceeding theorem with $I > 2$, then $n = \sum_i m_i \leq p+2-I < p$ giving the same contradiction. If we get $I=2$, then necessarily at least 2 fixed points specialize to another terminal component and then $(m_1+1)+(m_2+1) \leq p+2-2 = p$. Once more we have the same contradiction.

Remark 3.2.1. One can give examples with $m = p+1$ and 2 terminal components; for an example see III.5 below.

Now we can describe the trees which occur in the $m < p$ case. Precisely, we describe the trees marked by the specialization of the fixed points.

Proposition 3.3. *Let σ be an order p automorphism of $D^o := \operatorname{Spec} R[[Z]]$ with $m+1 > 1$ geometric fixed points. As in III.2 let $\mathcal{D}'^o := \mathcal{D}^o/\langle\sigma\rangle$. If $m < p$, then $\mathcal{D}'^o_s$ has only one component which is a projective line and is equipped with a canonical point ∞ given by the original closed point (π, Z). Let t be a parameter for this line minus ∞. We denote the specialization of the branch locus by*

$\overline{\mathrm{Br}} := \{t_0, t_1, t_2, ..., t_m\}$ where the t_i are distinct. Then there is an $(m+1)$-tuple $(h_i)_i \in (\mathbb{Z}\setminus p\mathbb{Z})^{m+1}$ such that $\sum_{0\le i\le m} h_i = 0$ and

$$h_0 t_0^k + h_1 t_1^k + \cdots + h_m t_m^k = 0, \quad 0 \le k \le m-1. \tag{$*$}$$

In particular if we fix t_0 and t_1 in ${\mathbb{F}_p}^{alg} \subset k$, then there are only a finite number of solutions such that $\prod_{i<j}(t_i - t_j) \neq 0$ and they are in $\mathbb{F}_p^{alg}$.

Proof. Let $(h_i)_{0\le i\le m}$ be the Hurwitz data for σ as defined in II.2. Then by Th. III.2.1, $\sum_i h_i \equiv 0 \bmod p$ and hence we may normalize so that $\sum_i h_i = 0$. Setting $s = t^{-1}$ there is a function $\bar{u} := \prod_{0\le i\le m}(1 - t_i s)^{h_i}$ such that $\mathrm{ord}_{s=0} d\bar{u} = m - 1$ (Th. III.2.1 Proof). Considering the Taylor expansion of $\dfrac{\bar{u}'}{\bar{u}}$ at $s = 0$, we obtain the system of equations $(*)$ above.

Now we show that the m equations define a finite number of marked affine lines as soon as t_0 and t_1 are fixed and distinct in ${\mathbb{F}_p}^{alg}$. Let $(t_0, ..., t_m)$ be a solution of $(*)$ such that $\prod_{i<j}(t_i - t_j) \neq 0$, and for t_0 and t_1 fixed we calculate the jacobian determinant of $h_2 {t_2}^i + \cdots + h_m {t_m}^i = -(h_0 {t_0}^i + h_1 {t_1}^i)$, $1 \le i \le m-1$. Consider the affine variety in the $m-1$ indeterminates, $x_2, x_3, \cdots, x_m$, defined by the equations $h_2 {x_2}^i + \cdots + h_m {x_m}^i = -(h_0 {t_0}^i + h_1 {t_1}^i)$, for $1 \le i \le m-1$, where t_0 and t_1 fixed and distinct. As $m < p$ using the jacobian determinant criterion it follows that $(t_2, ..., t_m)$ is a smooth point of this variety. It follows that the dimension of the set of such solutions is zero and the finiteness follows.

4. Hurwitz data when $m < p$.

When $m = 1$, up to multiplication by an element in $\mathbb{F}_p^\times$, there is a unique possible $(m+1)$-tuple determining the Hurwitz data and the [O-S-S] example gives a realization. Now we would like to describe Hurwitz data when $1 < m < p$. Following II.3.1.2 and II.3.2.1 we know that this is strongly related to the type of reduction of p-cyclic covers of $\mathbb{P}^1$.

Definition 4.1. *Let $1 < m < p$ and $h_i \in \mathbb{Z}\setminus p\mathbb{Z}$ for $0 \le i \le m$, and suppose that $\sum_{0\le i\le m} h_i = 0$. We say that $(h_0, h_1, h_2, .., h_m)$ satisfies the condition $(*)$ if the system of equations in $\mathbb{F}_p[X_0, ..., X_m]$:*

$$h_0 X_0^k + h_1 X_1^k + \cdots + h_m X_m^k = 0, \quad 0 \le k \le m-1, \tag{$*$}$$

has a solution $(t_i)_i \in (\mathbb{F}_p^{alg})^{m+1}$ in which all $m+1$ components are distinct, i.e. such that $P((t_i)_i) \neq 0$, where $P((X_i)_i) := \prod_{0\le i<j\le m}(X_i - X_j)$. Such a solution will be called "a proper solution" of $(*)$.

Clearly "proper solutions" correspond to possible Hurwitz data. Here we can prove the following:

Theorem 4.2. *Let p be a prime, m an integer with $0 < m < p$, and suppose $h_i \in \mathbb{Z}\setminus p\mathbb{Z}$ for $0 \le i \le m$, with $\sum_i h_i = 0$. We assume that condition $(*)$ is satisfied and let $(t_i)_i \in (\mathbb{F}_p^{alg})^{m+1}$ be a proper solution of $(*)$ with $(T_i)_i \in ({\mathbb{Z}_p}^{ur})^{m+1}$ a lifting. Then the cover of $\mathbb{P}^1_{\mathbb{Q}_p^{ur}}$ defined by the equation $Y^p = \prod_{0\le i\le m}(1 - T_i X)^{h_i} := f(X)$ has potentially good reduction of type A_m. This induces an order p automorphism σ of the p-adic open disc over $\mathbb{Z}_p^{ur}[\zeta]$ (for ζ a primitive p-th root of unity), which is the formal fiber above ∞. It has no inertia at (π), the conductor is $m+1$ and the Hurwitz data is $(h_0, h_1, ..., h_{m-1}, h_m)$.*

Proof. First we prove that the cover $Y^p = f(X)$ has good reduction of type A_m over $\mathbb{Z}_p^{ur}[\zeta]$. Writing $f(X) = 1 + s_1 X + s_2 X^2 + \cdots + s_m X^m + \cdots \in \mathbb{Z}_p^{ur}[\![X]\!]$, we show that $v(s_i) \ge v(p)$ for $i < m$ and $v(s_m) = 0$. This result can be easily deduced from induction formulas relating the elementary symmetric functions with Newton's symmetric functions; here we give a proof which is in the spirit of Th. III.2.1 and Prop. III.3.3.

Taking the logarithmic derivative one has

$$\frac{\overline{f'(X)}}{\overline{f(X)}} = \sum_{0\leq i\leq m} \frac{-h_i t_i}{1-t_iX} = -\sum_{\substack{0\leq i\leq m\\ 0\leq j\leq m-2}} h_i t_i^{j+1}X^j - \sum_{0\leq i\leq m} \frac{h_i t_i^m X^{m-1}}{1-t_iX} = -\sum_{0\leq i\leq m} \frac{h_i t_i^m X^{m-1}}{1-t_iX}.$$

This last fraction, when expressed over the same denominator, is equal to $\dfrac{X^{m-1}N(X)}{\prod_{0\leq i\leq m}(1-t_iX)}$, where $N(X)$ is a polynomial. Now we compare the degree at ∞ on each side: for $\dfrac{\overline{f'(X)}}{\overline{f(X)}}$ it has to be negative (in fact -1) and on the right side it is $-1+degN$. This means that $N(X)$ is a constant which we evaluate easily and obtain $-\sum_{0\leq i\leq m} h_i t_i^m$.

Note that $\sum_{0\leq i\leq m} h_i t_i^m \neq 0$, for otherwise using $(*)$ this would imply that the h_i are all zero. Hence $\overline{f'(X)} \equiv -(\sum_{0\leq i\leq m} h_i t_i^m)X^{m-1} \pmod{X^m}$, and as $m<p$ this implies $v(s_i)\geq v(p)$ for $i<m$ and $v(s_m)=0$. Set $X=\lambda^{p/m}S$, then for $i<m$, $v(s_i\lambda^{ip/m})>v(\lambda^p)$ and so if $Y=\lambda Z+1$, the equation of the cover is $\dfrac{(\lambda Z+1)^p-1}{\lambda^p} = (-1/m)(\sum_i h_i T_i^m)S^m +$ something small. Now mod π for the S-Gauss valuation we obtain $z^p-z=(-1/m)(\sum_i h_i t_i^m)S^m$, which is a cover of $\mathbb{P}^1$ of type A_m.

Finally, we remark that the branch locus of the cover is concentrated in the formal fibre at infinity, and so applying the local criterion of good reduction, see [G-M] I.3.4, the cover of $\mathbb{P}^1_{\mathbb{Q}_p^{ur}}$ has potentially good reduction of type A_m and the given Hurwitz data.

Remark 4.2.1. Observe that there is a canonical lifting, which we obtain by applying [Mi], Th. 4.2. p.32, in order to lift the proper solution $(t_i)_i\in(\mathbb{F}_p^{alg})^{m+1}$ to a solution of $(*)$ in $(T_i)_i\in({\mathbb{Z}_p}^{ur})^{m+1}$; here we mean that

$$h_0T_0^k + h_1T_1^k + \cdots + h_mT_m^k = 0, \quad 0\leq k\leq m-1.$$

Note that (see proof above)

$$\frac{f'(X)}{f(X)} = \frac{-(\sum_{0\leq i\leq m} h_iT_i^m)X^{m-1}}{\prod_{0\leq i\leq m}(1-T_iX)}$$

and so it follows that $X\to f(X)$ defines an étale (genus 0) cover of $\mathbb{P}^1\setminus\{0,1,\infty\}$.

We next illustrate the $(*)$ condition:

4.3. The case $m=2$, $p>2$: In this case one can easily parametrize proper solutions of $(*)$; namely up to homographical transformation one obtains $(h_0,-h_1,h_0-h_1)$ and the cross-ratio $[h_0,-h_1,h_0-h_1,\infty]=-\dfrac{h_1}{h_0}$.

Now in the spirit of Th. III.4.2. we consider the cover:

$$Y^p = (1+h_0X)^{h_0}(1-h_1X)^{h_1}(1+(h_0-h_1)X)^{-(h_0+h_1)}.$$

If we set $W := -\dfrac{h_1}{h_0}\dfrac{1-h_1X}{1+h_0X}$, the equation of the cover becomes

$$Y^p = (-1)^{h_1}\frac{(h_0+h_1)^{h_0+h_1}}{h_0^{h_0}h_1^{h_1}}W^{h_1}(1-W)^{-(h_0+h_1)}.$$

In this special case this means that every p-cyclic cover of $\mathbb{P}^1$ with branch locus $\{0,1,\infty\}$ has potentially good reduction of type A_2 (compare with [Co-Mc]), and so, modulo a change of parameter, there is only a finite set of order p automorphisms of a p-adic open disc with no inertia at (π) and 3 fixed points (see V.6.3 for a generalisation).

4.4. Examples of $(m+1)$-tuples with $2<m<p$ which are not Hurwitz data.

Here we give an example for which $(*)$ is not satisfied.

Consider $h_1 = h_2 = ... = h_{m-1} = 1$ and let h_m be such that $m-1+h_m \not\equiv 0 \bmod p$ and $h_0 = -\sum_{1\le i\le m} h_i$. Then if $-h_m \in \{1,2,...,m-2\}$, each solution of the system of equations

$$h_0X_0^k + X_1^k + X_2^k + \cdots + X_{m-1}^k + h_mX_m^k = 0, \quad \text{for } i = 1,..,m-1$$

in $\mathbb{F}_p^{alg}$ satisfies $X_i - X_0 = 0$ for some i, and so isn't proper. *In particular,* $(-m+1-h_m, 1, ..., 1, h_m)$ *cannot occur as an* $(m+1)$*-tuple of Hurwitz data, for* $-h_m \in \{1,2,...,m-2\}$.

Proof. Set $Y_i = X_i - X_0$ for $1 \le i \le m$. Then we can replace the system $(*)$ by the system:

$$Y_1^k + Y_2^k + \cdots + Y_{m-1}^k + h_mY_m^k = 0 \quad \text{for} \quad 1 \le k \le m-1. \tag{$**$}$$

Assume there is a solution for which none of the Y_i is 0; say $Y_m = 1$. Setting $p_k := Y_1^k + Y_2^k + \cdots + Y_{m-1}^k$ for each k, we can use Newton's formulas ($m<p$) in order to calculate the values of the elementary symmetric functions s_k.

For $1 \le k \le m-1$ one has:

$$p_k - p_{k-1}s_1 + p_{k-2}s_2 + \cdots + (-1)^{k-1}p_1s_{k-1} + (-1)^k ks_k = 0,$$

where s_k is the k-th elementary symmetric function on the Y_i, $1 \le i \le m-1$. In order to simplify the formuli we call $h := -h_m$. Then replacing p_k by its value h we get:

$$h(1 - s_1 + s_2 + \cdots + (-1)^{k-1}s_{k-1}) + (-1)^k ks_k = 0,$$

which immediately gives the following inductive formula:

$$s_k = \frac{h-k+1}{k}\, s_{k-1}.$$

As $s_1 = h$ we obtain:

$$s_k = h(h-1)(h-2)...(h-k+1)/k!.$$

This means that for $i = 1,...,m-1$ the Y_i are the roots of the polynomial

$$Y^{m-1} - s_1Y^{m-2} + \cdots + (-1)^{m-1}s_{m-1} = 0.$$

As $s_{m-1} = 0$ for $h \in \{1,2,...,m-2\}$, the result follows.

4.5. Critical locus for the condition $(*)$.

Proposition 4.5.1. *Let $1<m<p$, and let H_i be indeterminates for $1 \le i \le m$. We consider the following polynomial in $\mathbb{F}_p[H_i]$:*

$$Q := \prod_{1\le n\le m} Q_n,$$

where $Q_n := \prod (H_{i_1} + \cdots + H_{i_n})$ and the product is taken over the $i_k \in \{1,...,m\}$, $i_1 < i_2 < ... < i_n$. We define the critical locus for the condition $(*)$ to be the set of m-tuples $(h_1, h_2, ..., h_m) \in \mathbb{Z}^m$ such that $Q(h_i) = 0$. Take (h_i) such that $Q(h_i) \neq 0$, then setting $h_0 = -\sum_{1\le i\le m} h_i$, the system $(*)$ has only proper solutions in the sense of III.4.1 and the trivial solution $(0,0,...,0)$. Moreover,

$(-\sum_{1\leq i\leq m} h_i, h_1, h_2, .., h_m)$ is the Hurwitz data for an order p automorphism of the p-adic open disc.

Proof. Let $(h_1, h_2, ..., h_m) \in \mathbb{Z}^m$ such that $Q(h_i) \neq 0$ be given, and setting $h_0 = -\sum_{1\leq i\leq m} h_i$ consider the system $(*)$ as defined in III.4.1. As done previously, set $Y_i = X_i - X_0$ for $1 \leq i \leq m$, replacing the system $(*)$ by the system $(**)$ $h_1Y_1^i + h_2Y_2^i + \cdots + h_{m-1}Y_{m-1}^i + h_mY_m^i = 0$ for $1 \leq i \leq m-1$. By a dimension argument we know that $(**)$ has at least one solution, say $(y_1, y_2, ..., y_m) \in \mathbb{F}_p^{alg}$, which is distinct from $(0, 0, ..., 0)$. After a permutation of the y_i, and the corresponding coefficient's in the system $(**)$, we can assume that

$$\begin{gathered} y_1 = ... = y_{j_1} \\ y_{j_1+1} = ... = y_{j_2} \\ etc... \end{gathered}$$

where the lines correspond to the set of distinct values in the y_i, i.e. $y_{j_1}, y_{j_2}, ..., y_{j_s}$, where $j_s = m$. Assume that $\prod_i y_i \prod_{i<j} (y_i - y_j) = 0$ (see III.4.1).

There are two cases:

Case 1. One of the y_{j_i} is zero; say for example that $y_{j_s} = 0$, then $(**)$ can be written in the following way:

$$\begin{aligned} (h_1 + \cdots + h_{j_1})y_{j_1} + (h_{j_1+1} + \cdots + h_{j_2})y_{j_2} + \cdots \\ +(h_{j_{s-2}+1} + \cdots + h_{j_{s-1}})y_{j_{s-1}} = 0 \\ (h_1 + \cdots + h_{j_1})y_{j_1}^2 + (h_{j_1+1} + \cdots + h_{j_2})y_{j_2}^2 + \cdots \\ +(h_{j_{s-2}+1} + \cdots + h_{j_{s-1}})y_{j_{s-1}}^2 = 0 \\ . \\ . \\ (h_1 + \cdots + h_{j_1})y_{j_1}^{m-1} + (h_{j_1+1} + \cdots + h_{j_2})y_{j_2}^{m-1} + \cdots \\ +(h_{j_{s-2}+1} + \cdots + h_{j_{s-1}})y_{j_{s-1}}^{m-1} = 0. \end{aligned}$$

Now looking at the first $s-1$ lines one gets a Vandermonde type system whose determinant is non-zero. This contradicts $Q(h_i) \neq 0$.

Case 2: None of the y_i is zero. As $\prod_i y_i \prod_{i<j} (y_i - y_j) = 0$ it follows $s < m$; so the same reasoning as above works.

Note that in the previous example III.4.4 we meet the critical locus for $(*)$.

4.6. If $m \notin p\mathbb{Z}$, then $(1, 1, ..., 1, -m)$ is Hurwitz data.

Proof. Take $Y^p = 1 - X^m$; this is the [O-S-S] example, see II.3.3.

4.7. Special Hurwitz data for $m = p-2$.

There is a pleasing case where the condition $(*)$ is always satisfied. Namely, let $m = p-2$ and $h \in \mathbb{Z}$ be a primitive $(p-1)$-th root of unity mod p. Then

$$\{h_0, h_1, ..., h_{p-3}\} = \{1, h, h^2, ..., h^{p-2}\}$$

is such that $(t_0, ..., t_{p-2}) = (1, h, h^2, ..., h^{p-2}) \in \mathbb{F}_p^{p-1}$ is a proper solution of the corresponding system $(*)$, and by Th. III.4.2 $(1, h, h^2, ..., h^{p-2})$ is Hurwitz data for some order p automorphism. As $h^{(p-1)/2} \equiv -1 \bmod p$ we meet the critical locus for condition $(*)$.

In particular, lifting $(t_0, ..., t_{p-2})$ to $(1, \alpha, \alpha^2, ..., \alpha^{p-2})$, for $\alpha \in \mathbb{Z}_p$ a primitive $(p-1)$-th root of unity such that $h \equiv \alpha \bmod p$, it follows from Th. III.4.2 that:

Proposition 4.7.1. *Let $\alpha \in \mathbb{Z}_p$ be a primitive $(p-1)$-th root of unity and $h \in \mathbb{Z}$ with $h \equiv \alpha \bmod p$. Then the cover of $\mathbb{P}^1_{\mathbb{Q}_p}$ given by the equation*

$$Y^p = (1+X)(1+\alpha X)^h(1+\alpha^2 X)^{h^2} ... (1+\alpha^{p-2}X)^{h^{p-2}} = g(X)$$

has potentially good reduction and defines an automorphism of $\mathbb{Z}_p[\zeta][\![Z]\!]$, whose Hurwitz data is $(1, h, h^2, ..., h^{p-2})$.

We shall use these covers in section IV.

5. Geometric trees in the case $m > p$.

In this paragraph we intend to show that in general the tree is not reduced to one component when $m > p$.

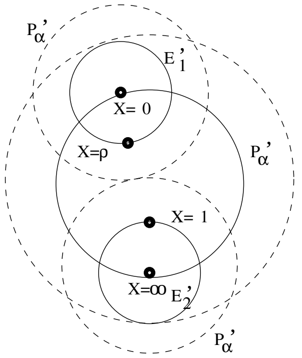
5.1. The case $p = 2$ and $m = 3$.

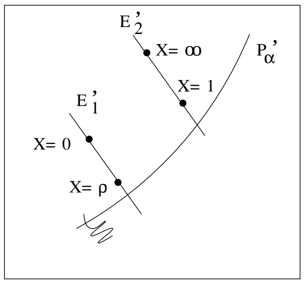
In order to introduce the method we first recall the case where $p = 2$ and $m = 3$ and show how this relates to what is known on elliptic curves over 2-adic fields.

By virtue of the correspondence with $p = 2$-cyclic covers of $\mathbb{P}^1_K$ we have to look at the Legendre equation for elliptic curves, that is the equation $Y^2 = X(X-1)(X-\rho)$, whose potential good reduction is read off from the 2-adic valuation of

$$j(\rho) = \frac{2^8(\rho^2 - \rho + 1)^3}{\rho^2(\rho - 1)^2}.$$

We will have potentially good reduction if and only if $v(j(\rho)) \geq 0$, in which case the j invariant of the curve in reduction is the image of $j(\rho)$. Moreover, the 2-rank is 0 if and only if the j invariant is residually 0; so we conclude that such a cover will induce an automorphism of the type we desire if and only if $v(j(\rho)) > 0$. If $v(\rho) > 0$ this means that $4v(2) > v(\rho)$. So we see immediately in the case $p = 2$ and $m = 3$ that there are automorphisms for which the branch locus does not consist of points of equal mutual distance.





$\mathcal{D}_s'^{o}$

This is well understood from Deuring's normal form (valid in char. $\neq 3$) ([D2], see also [Si], Appendix A). Recall that over an algebraically closed field of char. $\neq 3$ any elliptic curve has a model $Z^2 + \alpha XZ + Z = X^3$ for some α and the j invariant is $j = \dfrac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}$. So over a 2-adic field this gives a smooth model, whose special fiber has p-rank 0 (étale cyclic cover of $\mathbb{A}^1$ of conductor 4) if and only if $v(\alpha) > 0$.

Moreover, one can also describe the formal fiber at ∞. Namely, setting $Y = 2Z + (1 + \alpha X)$ in the equation above, one obtains $Y^2 = 4X^3 + (1 + \alpha X)^2$ and so the geometric tree corresponding to the formal fiber at ∞ is reduced to one component if and only if $v(\alpha) \geq \frac{2}{3}v(2)$.

5.2. General case $p < m$.

Now consider any p with $m > p$ and call q the integral part of m/p. Choose $(\alpha_i)_{1 \le i \le q}$ in R^{alg}, $v(\alpha_i) > 0$, and consider the p-cyclic cover of $\mathbb{P}^1$ defined by the equation:

$$Y^p = \lambda^p X^m + (1 + \alpha_1 X + \cdots + \alpha_q X^q)^p$$

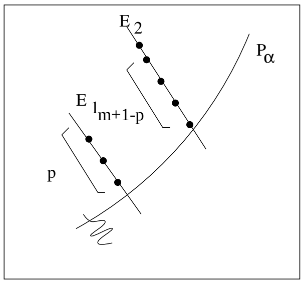
and set $Y = \lambda Z + 1 + \alpha_1 X + \cdots + \alpha_q X^q$. Then mod π this induces the cover $z^p - z = x^m$ which is of type A_m. Now the branch locus is given by ∞ and the zeros of

$$\lambda^p X^m + (1 + \alpha_1 X + \cdots + \alpha_q X^q)^p$$

whose degree is m (note that a derivation shows that the roots are all distinct, although in fact it is not necessary to say this), it follows that the cardinality of the branch locus is at most $m+1$ so the generic different is less than or equal to the special different, hence they are equal and we have a good reduction of type A_m. Note that X^{-1} is a parameter for the disc at the bottom so we can directly read the distance between fixed points from the size of root of

$$\lambda^p X^m + (1 + \alpha_1 X + \cdots + \alpha_q X^q)^p = 0.$$

Note that ∞ is a fixed point. In order to simplify the situation, we assume that $\alpha_i = 0$ for $i > 1$. Then a look at Newton's polygon shows that if $v(\alpha_1) < \dfrac{p}{m} v(\lambda)$, the roots take two values and the tree is:



$\mathcal{D}_s^o$

Remark 5.2.1. Following Theorem 3.1 it is tempting to conjecture that if $m > p$ there is a bound for the number of terminal components which is given by the integral part of $\dfrac{m}{p}$. The following example shows that here the answer is no.

Let $p > 2$ and following the notations in the proof of Theorem 3.1 we consider the function over $\mathbb{P}^1_k$ defined by $\overline{u}_\alpha := \dfrac{s^p}{1 + s^{p-1} + s^p}$. The poles of $\overline{u}_\alpha$ are at p distinct points with simple multiplicities ($m_i = 1$). The differential $d\overline{u}_\alpha$ has a zero at ∞ whose order is $2p-2 = -2 + \sum_i (m_i + 1)$. Therefore we expect an order p automorphism of the open disc whose semi-stable tree has one internal and p terminal components, each containing the specialization of 2 fixed points. We construct such an example below.

Let π be the uniformizing parameter for R and assume there is positive integer l such that $|\lambda| < |\pi|^l$; this means in particular that the absolute ramification index is big. We consider the following p-cyclic cover of $\mathbb{P}^1_K$:

$$Y^p = \frac{1 + S^{p-1} + S^p + (\pi^{pl} S^p + p\pi^l S)}{1 + S^{p-1} + S^p} := f(S)$$

Note that if we set $Y = \pi^l Z + 1$, then in reduction for the S-Gauss valuation this equation gives the equation:

$$z^p = \frac{s^p}{1 + s^{p-1} + s^p} = \overline{u}_\alpha$$

Now we show that this cover has potentially good reduction of type A_m for $m = 2p-1$.
We can write

$$f(S) = (1+\pi^l S)^p - p\pi^l S^2 - \cdots - p\pi^{(p-1)l} S^{p-1} - \pi^{pl}\frac{S^{2p-1}(1+S)}{1+S^{p-1}+S^p} - p\pi^l \frac{S^p(1+S)}{1+S^{p-1}+S^p}.$$

Next we set $S := \rho T$ where $\rho^{2p-1}\pi^{pl} = -\lambda^p$. Then $|p\pi^l\rho^p| = |\lambda^p||\frac{\lambda}{\pi^l}|^{\frac{(p-1)^2}{2p-1}} < |\lambda^p|$ and $|p\pi^l\rho^2| = |\lambda^p||\frac{\lambda}{\pi^l}|^{\frac{1}{2p-1}} < |\lambda^p|$. Writing $Y = \lambda Z + (1+\pi^l S)$, in reduction for the T-Gauss valuation we obtain $z^p - z = t^{2p-1}$, which is of type A_m for $m = 2p-1$. Now we remark that the generic cover is ramified at $m+1$ points which lie in the disc $|T| > 1$, so this cover has potentially good reduction (see [G-M], I.3.4). Moreover, it follows from the choice of $f(S)$ (each root of the numerator is close to one from the denominator) that we get the desired tree.

IV. Local obstructions to the lifting

The aim of this section is to give obstructions for a given group of automorphisms G of $k[\![z]\!]$ to be lifted to an automorphism group of the formal power series ring $R[\![Z]\!]$, and to give examples of liftable groups.

1. Abelian groups.

We first recall that by [G-M] it is always possible to construct liftings of $p^a e$-cyclic covers for $a \leq 2$ and $(e,p) = 1$, and that this is an open question for higher p-exponents. There we have also shown that for $G = (\mathbb{Z}/p\mathbb{Z})^2$, if the lifting of a G-cover is possible, then there are serious geometric constraints on the conductors of the p-cyclic subcovers. Moreover, these constraints imply a group theoretic condition on G-covers for $G = (\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}/n\mathbb{Z}$ to be liftable; namely, that the primes dividing n are congruent to 1 mod p.

In this chapter we apply the previous chapters to the local lifting question, in particular studying the situation for $p = 2$ and 3. We also show that there are obstructions to the liftability of certain meta-cyclic groups and finally we present examples of meta-cyclic groups which can be lifted. As an application of III.5.2 we first show:

Proposition 1.1. *If p is 2 or 3 and $G = (\mathbb{Z}/p\mathbb{Z})^2$, then there is a G-cover $k[\![z]\!]/k[\![z]\!]^G$ which can be lifted to a G-cover $R[\![Z]\!]/R[\![Z]\!]^G$, where $R = \mathbb{Z}_p[\lambda^{1/(p-1)}]$, and $\lambda = \zeta - 1$.*

Proof. The case $p = 2$ is considered in ([G-M]). We assume that $p = 3$ and suppose one cover is given by the equation $Y_1^3 = \lambda^3 X^2 + 1$ (those of [O-S-S] type with $m_1 = 2$), and a second is of the type considered in III.5.2, i.e. $Y_2^3 = \lambda^3 X^4 + (1+\alpha X)^3$ (here the conductor is $m_2 + 1 = 5$).

For the first cover the branch locus is located at ∞, $x_1 = (-\lambda)^{-3/2}$ and $x_2 = -x_1$.

For the second we choose α in such a way that ∞ and x_1 are in the branch locus; namely we take $\alpha = (1+\lambda)(-\lambda)^{1/2}$. One can check directly that x_2 is not in the branch locus (We further remark that $v(\alpha) < \frac{p}{m_2} v(\lambda)$ and that the geometry of the branch locus is as in III.5.2). As the two branch loci meet in $2 = (p-1)(m_1+1)/p$ points we can apply [G-M] Th. I.5.1.

Remark. Recently Matignon, [M], has obtained a realisation of $(\mathbb{Z}/p\mathbb{Z})^n$ as an automorphism group (without inertia at (π)) of the p-adic open disc for any p and $n > 1$.

2. Meta-cyclic groups

2.1. Obstructions to lifting of covers.

Suppose $G = \langle \tau, \sigma \rangle$ with $\mathrm{o}(\tau) = e$ for e prime to p, $\mathrm{o}(\sigma) = p$ and $\tau\sigma = (\sigma)^a\tau$ where $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a primitive e-th root of unity (so $e|(p-1)$).

Assume that G is an automorphism group of $k[[z]]$ which can be lifted to a subgroup of $\mathrm{Aut}_R R[[Z]]$ and $\zeta \in R$, where ζ is a primitive p-th root of 1 (this is necessary when $p > 0$; see [Co] section 5).

We denote the liftings of τ and σ by the same letter. Let $m+1$ be the conductor of σ. Then $e|(m+1)$, because the group generated by τ acts on the set F_σ of σ fixed points. Note that this action is free, otherwise by [Co] Lemma 14 p.125, we would obtain a cyclic subgroup in G of order pe' with $1 < e'|e$ (see also [O], example in l.c p.166, which is a global argument as opposed to the one we have given).

Application to Roquette's curve. (Compare with [Ga] Ex. 3.9.) Suppose $e = p-1$ and let $\mathbb{P}^1_k$ be the projective line over k with coordinate x. We look at automorphisms which fix the infinite point. We can realise the previous group G ($e = p-1$) as a group of automorphisms of $\mathbb{P}^1_k$ fixing ∞ by taking $\sigma(x) = x+1$ and $\tau(x) = a^{-1}x$; so $G \subset \mathrm{PGL}_2(\mathbb{F}_p)$. The conductor of σ is 2, so if $p > 3$ one cannot lift the curve $(\mathbb{P}^1_k, G)$ over any R.

A corollary is a local obstruction to the lifting in char. 0 of $(C, \mathrm{Aut}_k(C))$ for the Roquette curve $C: y^2 = x^p - x$. Recall that for $p > 2$, $g(C) = (p-1)/2$ and $|\mathrm{Aut}_k C| = 2p(p^2-1)$; so $|\mathrm{Aut}_k C| > 84(g-1)$ as soon as $p > 3$. This contradicts the Hurwitz bound in char. 0 and so gives a global obstruction for the lifting in char. 0. The local reason is the following: Let ι be the hyperelliptic involution. Then $C/\langle\iota\rangle \simeq \mathbb{P}^1_k$. Moreover the group $\mathrm{PGL}_2(\mathbb{F}_p) \subset \mathrm{Aut}_k \mathbb{P}^1_k$ extends to a subgroup of $\mathrm{Aut}_k C$. So the lifting of $(C, \mathrm{Aut}_k(C))$ would imply that of $(\mathbb{P}^1_k, G)$, which is a contradiction if $p > 3$.

2.2. Some meta-cyclic liftings.

We can prove the following:

Proposition 2.2.1. *Let $p > 2$ and $G = \langle \sigma, \tau \rangle$, with $\mathrm{o}(\sigma) = p$, $\mathrm{o}(\tau) = 2$ and $\tau\sigma\tau^{-1} = \sigma^{-1}$. Then there is a G-cover $k[[z]]/k[[z]]^G$ which can be lifted to a G-cover $R[[Z]]/R[[Z]]^G$, where $R = \mathbb{Z}_p[\zeta]$ and ζ is a primitive p-th root of 1.*

Proof. Consider the Artin-Schreier equation $x^p - x = 1/t$ with $p > 2$. We set $z = 1/x$ and consider the two automorphisms of $k((z))$ defined by the conditions:

$$\sigma(x) = x+1,\ \sigma(t) = t \quad \text{and} \quad \tau(t) = -t,\ \tau(x) = -x.$$

One has

$$\tau\sigma\tau^{-1}(x) = \tau\sigma(-x) = \tau(-x-1) = x-1$$

and so $\tau\sigma\tau^{-1} = \sigma^{-1}$. Let $G := \langle \sigma, \tau \rangle$. The fixed field $k((z))^G$ is $k((t^2 = y))$ where one has $(x^p - x)^2 = y^{-1}$.

Now we shall see that one can lift this cover to a Galois cover of $\mathbb{P}^1_R$ for $R = \mathbb{Z}_p[\zeta]$. We set $\lambda = \zeta - 1$ and consider the equation:

$$\big((\lambda X + 1)^p - 1\big)/\lambda^p = 1/T. \tag{$*$}$$

One can lift σ to

$$\sigma(X) = \zeta X + 1, \qquad \sigma(T) = T$$

and τ to

$$\tau(T) = -T - \lambda^p, \qquad \tau(\lambda X + 1) = (\lambda X + 1)^{-1}.$$

Then $\tau(X) = -X/(\lambda X+1)$ and the relation between τ and σ is still satisfied. The fixed field is $K(T^2)$ and our G-cover is $K(T^2)[X]$ with equation $(*)$. This it induces a G cover $R[[Z]]/R[[Z]]^G$ where $Z = X^{-1}$.

Now we can mimic the previous proof in order to get other meta-cyclic groups; here the lifting process is less evident and will depend on our knowledge of Hurwitz data.

Proposition 2.2.2. *Let $G = \langle\sigma,\tau\rangle$, with $\mathrm{o}(\sigma) = p$, $\mathrm{o}(\tau) = p-1$ and $\tau\sigma\tau^{-1} = \sigma^{h^{-1}}$ (h is a primitive $(p-1)$-th root of 1 modulo p). If $p > 2$, then there is a G-cover $k[[z]]/k[[z]]^G$, which can be lifted to a G-cover $R[[Z]]/R[[Z]]^G$, for $R = \mathbb{Z}_p[\zeta]$ and ζ a primitive p-th root of 1.*

Proof. First assume that we have such a lifting $G := \langle\sigma,\tau\rangle \subset \mathrm{Aut}_R R[[Z]]$. Let $m+1$ be the conductor of σ, the fixed point set $F_\sigma := \{Z_0, Z_1, \ldots, Z_m\}$ and $(h_0, h_1, \ldots, h_m)$ its Hurwitz data. As $(p-1)|(m+1)$ (see 2.1 above), it is natural to consider the first case which can occur, namely $m = p-2$. Writing $\sigma(Z) := f(Z) \in R[[Z]]$, we have $\tau(Z_0) \in F_\sigma$ and $f'(\tau Z_0) = f'(Z_0)^h$ for each $Z_0 \in F_\sigma$. This implies that the Hurwitz data $(h_0, h_1, h_2, ..., h_m)$ is invariant with respect to multiplication by h and this leads us (by III.4.7) to consider the cover

$$Y^p = (1+X)(1+\alpha X)^h(1+\alpha^2X)^{h^2}...(1+\alpha^{p-2}X)^{h^{p-2}} := g(T),$$

which we proved has good reduction of type A_m over $\mathbb{Z}^{ur}[\zeta]$. Setting $T := \lambda^{p/(p-2)}X^{-1}$ this cover induces a p-cyclic cover $R[[Z]]/R[[T]]$ over the open disc $|T| < 1$. Denote by σ the order p automorphism of $R[[Z]]/R[[T]]$ such that $\sigma(Y) = \zeta Y$ and $\sigma(T) = T$. Now let τ be the K-automorphism of $K(X)$ defined by $\tau(X) = \alpha^{-1}X$ (α is the primitive $(p-1)$-th root of unity such that $\alpha \equiv h \bmod p$). Then we remark that

$$\tau(g(X)) = g^h\frac{1+\alpha^{-1}X}{(1+\alpha^{p-2}X)^{h^{p-1}}} = (1+\alpha^{-1}X)^{1-h^{p-1}}.$$

As the factor $(1+\alpha^{-1}X)^{1-h^{p-1}}$ is a non-trivial p power this allows us to extend τ to an R-automorphism of $K(X,Y)$ by setting

$$\tau(Y) := P(X)Y^h \quad \text{where} \quad P(X) := (1+\alpha^{-1}X)^{(1-h^{p-1})/p}.$$

We remark that $\tau^{p-1}(g(X)) = g(X)$ and so $\dfrac{\tau^{p-1}(Y)}{Y} \in K(X,Y)$ is a p-th root of 1; specializing at $T = \infty$ this shows that $\tau^{p-1} = \mathbf{1}$, the identity of G. Moreover, $\tau\sigma\tau^{-1}(Y) = \tau\sigma\tau^{p-2}(Y) = \zeta^{h^{p-2}}Y$. This is deduced as follows: writing $\tau^{p-2}(Y) = Y^{h^{p-2}}F(X)$ for suitable $F(X)$ it follows that $\tau\sigma\tau^{-1}(Y) = \tau\sigma(Y^{h^{p-2}}F(X)) = \tau(\zeta^{h^{p-2}}Y^{h^{p-2}}F(X)) = \zeta^{h^{p-2}}\tau(Y^{h^{p-2}}F(X)) = \zeta^{h^{p-2}}Y$ and so $\tau\sigma\tau^{-1} = \sigma^{h^{-1}}$. Note that $\tau(R[[T]]) = R[[T]]$; it follows that τ induces an R-automorphism of $R[[Z]]$ and $G := \langle\sigma,\tau\rangle \subset \mathrm{Aut}_R R[[Z]]$ has the desired property.

V. The moduli of order p automorphisms

This section is an attempt to parametrize automorphisms of $R[[Z]]$ of order p which admit 0 as a fixed point, so we shall fix a parameter Z for the disc and consider those automorphisms which fix 0. In fact it is more convenient to parametrize the group they generate by fixing the action on the tangent space. This will be done by fixing a given primitive p-th root of unity ζ, and studying the relationship among the coefficients in

$$\sigma(Z) = \zeta Z(1 + a_1Z + \cdots + a_mZ^m + \cdots)$$

under iteration of σ (composition with itself). We set $R := \mathbb{Z}_p[\zeta]$ and view the a_i as indeterminates, so that $\sigma(Z) \in R[a_i]_i[[Z]]$. We express the p-th iterate as

$$\sigma^p(Z) = Z(1 + E_1Z + \cdots + E_nZ^n + \cdots),$$

where $E_n \in \mathbb{Z}_p[\zeta][a_i]_i$ and for later use define $E_0 = 0$. We denote by I_n the ideal of $R[a_1, a_2, \ldots, a_n]$ generated by $(E_j)_{0\le j\le n}$.

Proposition 1. *Using the notations above, the E_i are homogeneous polynomials of degree i in the a_j with coefficients in R, where for each j, a_j is given the weight j. Moreover*

i) $E_0 = E_1 = \ldots = E_{p-1} = 0$

ii) $E_p, E_{p+1}, \ldots, E_{2p-1} \in R[a_1, a_2, \ldots, a_p]$, *and more generally for each positive integer* n, $E_{np}, E_{np+1}, \ldots, E_{(n+1)p-1} \in R[a_1, a_2, \ldots, a_{np}]$.

iii) The coefficent of a_{np} *in* E_{np} *is* p.

Proof. Introducing a new variable X and replacing Z by XZ, in σ each a_i is replaced by $a_i X^i$. After iteration one obtains $E_n((a_i X^i)_i) = X^n E_n((a_i)_i)$ which shows that after assigning weights the polynomials are homogeneous. Note that from this it follows that $E_n \in R[a_1, \ldots, a_n]$ and the coefficient of a_n in E_n is constant.

Proof of i) If we let $B = R[a_1, \ldots, a_p]$, then by truncation σ induces an endomorphism $\tilde{\sigma}$ of $BZ \oplus BZ^2 \oplus \cdots \oplus BZ^p$. The characteristic polynomial is $\prod_{1 \le i \le p} (X - \zeta^i) = X^p - 1$, and so by the Cayley-Hamilton Theorem $\tilde{\sigma}^p = \mathbf{1}$, the identity. This is equivalent to (i).

Proof of ii) In order to tackle assertion ii) of the proposition we first show:

Lemma 2. *Let J_{np} be the ideal of $R[a_1, \ldots, a_s]$ generated by $(E_{jp})_{0 \le j \le n}$. Then for $np < l < (n+1)p$ one has $E_l \in J_{np} \otimes K =: KJ_{np}$, where $K = \mathrm{Fr}(R)$.*

Proof of the lemma. We prove the lemma by induction, assuming it proved for $0 \le n' < n$ and $np < l' < l$. One has

$$\sigma(Z) \equiv \zeta Z(1 + a_1 Z + \cdots + a_l Z^l) \bmod Z^{l+2}$$

and by the inductive hypothesis

$$\sigma^p(Z) \equiv Z(1 + E_l Z^l) \bmod (KJ_{np}, Z^{l+2}).$$

Using the identity $\sigma \circ \sigma^p(Z) = \sigma^p \circ \sigma(Z)$ one obtains

$$\zeta^{l+1} E_l Z^{l+1} \equiv \zeta E_l Z^{l+1} \bmod (KJ_{kp}, Z^{l+2}).$$

Since $p \not| l$ the result follows.

Returning to the proposition, assertion (ii) now follows from the fact that $E_{np} \in R[a_1, \ldots, a_{np}]$ and $K[a_1, \ldots, a_{np}] \cap R[a_1, \ldots, a_{(n+1)p}] = R[a_1, \ldots, a_{np}]$.

Proof of iii) It remains to prove that the coefficient of a_{np} in E_{np} is p. From the first part of the proposition we know that the coefficient is a constant. Let I be the ideal $(a_1, \ldots, a_{np-1}, Z^{np+2})$ in $R[(a_i)_i][\![Z]\!]$. Then

$$\sigma(Z) \equiv \zeta Z(1 + a_{np} Z^{np}) \bmod I,$$

and recurrently

$$\begin{aligned} \sigma^p(Z) &\equiv \zeta^p Z(1 + p a_{np} Z^{np}) \bmod I \\ &\equiv Z(1 + E_{np} Z^{np}) \bmod I \end{aligned}$$

finishing the proof.

Proposition 3. *For each $n \in \mathbb{N}$ we denote the image of E_n in $k[(a_i)_i]$ by $E_n v$. Then*

i) $E_i v = 0$, *for* $0 \le i \le p$;

ii) $E_i v \in k[a_1, \dots, a_p]$, *for* $p+1 \le i \le 2p$, *and more generally* $E_i v \in k[a_1, \dots, a_{(n-1)p}]$, *for* $(n-1)p + 1 \le i \le np$.

Proof. The only assertions which don't follow directly from Prop. V.1 are that $E_p v = 0$ and $E_{np} v \in k[a_1, \dots, a_{(n-1)p}]$ for $n > 1$. These follow from the commutativity of σ and σ^p in $k[\![z]\!]$. Namely, one has:

$$\sigma^p(z) = z(1 + E_{np} v z^{np} + E_{np+1} v z^{np+1}) \bmod (I_{np-1} v, z^{np+3})$$

and

$$\sigma(z) = z(1 + a_1 z + \cdots + a_{np+1} z^{np+1}) \bmod (I_{np-1} v, z^{np+3}).$$

Therefore

$$\begin{aligned} \sigma \circ \sigma^p(z) &= z(1 + a_1 z + \cdots + a_{np+1} z^{np+1}) \\ &\qquad (1 + E_{np} v z^{np} + E_{np+1} v z^{np+1}) \bmod (I_{np-1} v, z^{np+3}), \\ \sigma^p \circ \sigma(z) &= z(1 + a_1 z + \cdots + a_{np+1} z^{np+1} + a_1 E_{np} z^{np+1}) \\ &\qquad (1 + E_{np} v z^{np} + E_{np+1} v z^{np+1}) \bmod (I_{np-1} v, z^{np+3}) \end{aligned}$$

and so $a_1 E_{np} v \equiv 0 \bmod (I_{np-1} v)$. The result now follows from Prop. V.1.

4. An Example. In order to illustrate the difficulties we present the first few E_i expressions for the case $p = 3$: Setting $\lambda = \zeta - 1$ one computes

$$\begin{aligned} E_3 &= (-a_1 a_2 + a_1^3)\lambda + 6a_1^3 - 9a_1 a_2 + 3a_3 \\ E_4 &= (4a_1^4 + 2a_1 a_3 - 6a_1^2 a_2)\lambda + 10a_1^4 - 16a_1^2 a_2 + 6a_1 a_3 \\ E_5 &= (6a_1^5 + 4a_1^2 a_3 - a_2 a_3 + 2a_1 a_2^2 - 11a_1^3 a_2)\lambda + 8a_1^5 - 13a_1^3 a_2 + 6a_1^2 a_3 - a_1 a_2^2 \\ E_6 &= \big(-12a_1^3 a_3 - 6a_1^4 a_2 - 4a_1(a_2 a_3 + a_5) + a_1^2(11a_2^2 + 12a_4) + \\ &\qquad 2a_2 a_4 + 4a_1^6 - 3a_2^3\big)\lambda + 3a_6 + \cdots \\ &\ \ \vdots \\ E_9 &= \dots . \end{aligned}$$

As $E_3 v = 0$ it follows that $f_1 := E_3/\lambda \in R[a_1, a_2, a_3]$.
We define $f_2 := \big(E_6 - (a_1(a_1^2 - a_2) + a_3) f_1\big)/\lambda \in R[a_1, \dots, a_6]$ and $f_3 := E_8$. Then

$$\begin{aligned} f_1 v &= a_1(a_1^2 - a_2) \\ f_2 v &= 2(f_1 v)^2 + (2a_1^3 + a_3)(-f_1 v) + a_3 a_1^3 + a_3^2 + 2a_2 a_4 + 2a_1 a_5 \\ f_3 v &= (a_2 + a_1^2)(f_1 v)^2 + (a_1^5 + 2a_3 a_2 + a_4 + 2a_2 a_1^3)(f_1 v) + \\ &\qquad (a_1^2 - a_2)(a_4(a_1^2 + a_2) - a_3^2) \end{aligned}$$

One checks that

$$\begin{aligned} E_4 v &= a_1(f_1 v) \\ E_5 v &= 2(a_2 - a_1^2)(f_1 v) \\ E_6 v &= (a_1(a_1^2 - a_2) + a_3)(f_1 v) \\ E_7 v &= a_1(f_2 v) + (2a_1^4 + a_3 a_1 + a_4)(f_1 v) - a_1(f_1 v)^2 \\ E_9 v &\in ((f_1 v), (f_2 v)), \quad \text{noting that } a_1 f_3 v \in (f_1 v) \end{aligned}$$

Remark 4.1. Take $p = 3$, ζ a primitive 3-rd root of unity in R and $m = 2$ so that

$$\sigma(Z) = \zeta Z(1 + a_1 Z + a_2 Z^2 + a_3 Z^3 + \cdots), \qquad a_1 \in \pi R,\ a_2 \in R^\times.$$

Setting $\lambda = \zeta - 1$ it follows that $v(\lambda) = 1/2$, where v is the normalized exponential valuation on R. By Prop. V.1 and the example above it follows that

$$\sigma^3(Z) = Z\big(1 + E_3 Z^3 + \cdots\big)$$

with $f_1 := E_3/\lambda \in \mathbb{Z}_p[\lambda][a_1, a_2, a_3]$ and $f_1 v = a_1(a_1^2 - a_2)$. As σ has order 3 it follows that $E_3 = 0$ and so

$$a_1(a_1^2 - a_2) = a_1(a_1^2 - a_2) - f_1 \; \in \; \lambda\mathbb{Z}_p[\lambda][a_1, a_2, a_3].$$

Therefore $v(a_1(a_1^2 - a_2)) \geq v(\lambda) = 1/2$ and as $v(a_1) > 0$ and $v(a_2) = 0$ we conclude that $v(a_1) \geq 1/2$.

Looking at the Newton polygon for $\sigma(Z) - Z$, one deduces that the σ fixed points are at mutual distance $|\lambda|^{1/2}$; in this way we recover the very special case $p = 3, m = 2$ of III.3.1. Knowledge of the E_p expressions implies analogous proofs for $p = 5$, 7 and 11. It seems unreasonable to expect a proof of Th. III.3.1 for higher m by this method, nevertheless a characterisation of the E_p seems a very interesting question which we shall return to at the end of this section.

Remark 4.2. The relation $E_3/\lambda \in R[a_1, a_2, a_3]$ shows that in general one has π-torsion in

$$R[a_1, \ldots, a_n]/I_n.$$

In order to find a flat R-model we consider $\mathcal{I}_n := I_n K \cap R[a_1, \ldots, a_n]$ and define

$$\mathcal{X}_n := \operatorname{Spec} R[a_1, \ldots, a_n]/\mathcal{I}_n.$$

Here it is easy to describe the generic fibre of $\mathcal{X}_n$. Indeed, by induction one deduces from Prop. V.1.iii) that

$$E_{lp} = p a_{lp} + P_l\big((a_i)_{1 \leq i \leq lp,\,(i,p)=1}, (E_{jp})_{1 \leq j < l}\big),$$

where $P_l \in K[(a_i)_{1 \leq i \leq lp,\,(i,p)=1}, (E_{jp})_{1 \leq j < l}]$. From this it follows one has an equality of graded K-algebras

$$K[(a_i)_{1 \leq i \leq np,\,(i,p)=1}, (E_{jp})_{1 \leq j \leq n}] \cong K[a_1, a_2, ..., a_{np}],$$

where $\text{weight}(a_i) = i$ and $\text{weight}(E_{jp}) = jp$. The identification is given by sending a_i to a_i for $(i,p) = 1$ and E_{lp} to its expression as a polynomial in $R[a_1, \ldots, a_{np}]$; in the reverse direction the homomorphism is defined by sending a_{lp} to $(1/p)(E_{lp} - P_l)$. Then

$$\mathcal{X}_n(K) := \operatorname{Spec} K[a_1, \ldots, a_n]/\mathcal{I}_n K \cong \operatorname{Spec} K[X_j]_{j \in J},$$

where $J = \{j < n, \text{ prime to } p\}$.

The inclusion of ideals $\mathcal{I}_n R[a_1, a_2, ..., a_{n+1}] \subset \mathcal{I}_{n+1}$ induces an R-homomorphism

$$R[a_1, a_2, ..., a_n]/\mathcal{I}_n \longrightarrow R[a_1, a_2, ..., a_{n+1}]/\mathcal{I}_{n+1}$$

so that one can define:

5. Definition. We define the *"moduli space of order p automorphisms with fixed points"* of the open disc $\operatorname{Spec} R[\![Z]\!]$ to be the R-scheme $\mathcal{X} := \varprojlim \mathcal{X}_n$, where the projective limit is compatible with the ideal inclusions $\mathcal{I}_n \subset \mathcal{I}_{n+1}$.

Note that $\mathcal{X}(k)$ corresponds to automorphisms of order p (or the identity) of $k[\![z]\!]$, and for R'/R a finite discrete valuation ring $\mathcal{X}(R')$ corresponds bijectively to automorphisms of order p of

$R'[\![Z]\!]$ such that $\sigma(Z) = \zeta Z + \cdots$. Moreover, the [O–S–S] example (cf III, 3.3.1) shows that any k-section of $\mathcal{X}$ extends to an R-section:

$$\begin{array}{ccc} \operatorname{Spec} k & \longrightarrow & \mathcal{X} \\ \downarrow & \nearrow & \\ \operatorname{Spec} R & & \end{array}$$

On the ideals this has the interpretation:

$$\sqrt{\sum_{n\in\mathbb{N}^\times} \mathcal{I}_{np}v} = \sqrt{\sum_{n\in\mathbb{N}^\times} I_{np}v}.$$

6. Action via conjugation of the group $U(R[\![Z]\!])$.

Let R' be a complete discrete valuation ring dominating R. Then the group $U(R'[\![Z]\!]) = \{u_0 Z(1 + u_1 Z + \cdots) \mid u_i \in R',\ u_0 \text{ unit}\}$ acts via conjugation on $\mathcal{X}(R')$. One expects a structural result concerning the set of orbits through this action. These orbits can be seen as the automorphisms of order p without referring to a parameter centered in 0. Note that the action of the homothety $u_0 Z$ corresponds to an action of $\mathbb{G}_m$ and this explains the homogeneity of E_i with respect to weight$(a_i) = i$. The action of $U^1(R'[\![Z]\!]) := \{Z(1 + u_1 Z + \cdots) \mid u_i \in R'\}$ can be described as follows:

Let $\sigma(Z) = \zeta Z(1+a_1 Z+\cdots+a_i Z^i+\cdots)$ as above and $\tau(Z) = Z(1+t_1 Z+....+t_i Z^i+\cdots) \in U^1(R'[\![Z]\!])$; one calculates $\tau^{-1}\sigma\tau(Z) = \zeta Z(1 + A_1^\tau Z + ... + A_i^\tau Z^i + ...)$, where $A_n^\tau \in Z[\zeta, a_i, t_i]$ is homogeneous of weight n if we give the weight i to a_i and t_i.

For example one gets: $A_1^\tau := a_1 + (\zeta-1)t_1$, $A_2^\tau := (-2+2\zeta)t_1 a_1 + a_2 + (-2\zeta+2)t_1^2 + (\zeta^2-1)t_2$, $A_3^\tau := t_1\zeta a_1^2 + ((5-6\zeta)t_1^2 + (-2+3\zeta^2)t_2)a_1 + (2\zeta-3)t_1 a_2 + a_3 + (5\zeta-5)t_1^3 + (-3\zeta^2+5-2\zeta)t_2 t_1$.

Now the action of τ on E_n is given by $E_n^\tau := E_n(A_i^\tau)$, which is no longer homogeneous in the a_i. One can ask if there are invariant polynomials with respect to this action. We have the following:

Proposition 6.1. *The form E_p is invariant with respect to the action of $U^1(R'[\![Z]\!])$.*

Proof. Let $\tau(Z) = Z(1 + t_1 Z + ... + t_i Z^i + \cdots \in U^1(R'[\![Z]\!])$. We remark that mod Z^{p+2}, τ commutes with $\rho(Z) = Z(1 + aZ^p)$. The result now follows from Prop. V.1.

Remark. Note that $\mathbb{Z}_p[\zeta][E_p/\lambda] \subset \mathbb{Z}_p[\zeta][a_i]$ is $U^1(\mathbb{Z}_p[\zeta][\![Z]\!])$ invariant.

6.2. Order p automorphisms with 1 fixed point.

Proposition 6.2.1. *Let σ be an order p automorphism of $R[\![Z]\!]$ with only one geometric fixed point. Then this point is R-rational and σ is linearizable, i.e. after conjugation by some $\tau \in \operatorname{Aut}_R R[\![Z]\!]$ one has $\tau\sigma\tau^{-1}(Z) = \zeta^a Z$, for some $0 < a < p$.*

Proof. Applying the Weierstrass Preparation Theorem it follows directly that if there is only one fixed point it must be R-rational. Hence we can assume that $\sigma(Z) = \zeta Z(1 + a_1 Z + ...) \in R[\![Z]\!]$, and then for all $i \geq 1$, we must have $a_i \in \lambda R$, where $\lambda = \zeta - 1$ (see II.1). We build τ by approximation. Let $\tau_1(Z) := Z(1 + a_1\lambda^{-1}Z)$. Then $\tau_1\sigma\tau_1^{-1}(Z) = \zeta Z(1 + b_2\lambda Z^2) \bmod Z^3$. Now assume that we have built $\tau_n(Z)$ such that $\tau_n\sigma\tau_n^{-1}(Z) = \zeta Z(1 + b_{n+1}\lambda Z^{n+1}) \bmod Z^{n+2}$ and remark that if $(p, n+1) \neq 1$, then it follows from Prop. V.1, that $b_{n+1} = 0$. Now assume that $(p, n+1) = 1$ and set $\nu(Z) := Z(1 + \dfrac{\zeta-1}{\zeta^{n+1}-1} b_{n+1} Z^{n+1})$. Then $\tau_{n+1} := \nu\tau_n$ satisfies the congruence up to the level $n+1$ and the sequence τ_n converges to $\tau \in U^1(R[\![Z]\!])$.

Remark 6.2.2. The same proof method shows that any finite order automorphism with only one geometric fixed point is linearizable.

6.3. Order p automorphisms with no inertia at (π) and $0 < m < p$.

Theorem 6.3.1. *For $0 < m < p$, modulo a change of parameter, there are only a finite number of order p automorphisms of the open disc with no inertia at (π), i.e. in $\mathrm{Aut}_R R[\![Z]\!]$ there is only a finite set of conjugacy classes of such order p automorphisms. Moreover, they occur when considering the p-cyclic covers of $\mathbb{P}^1_{\mathbb{Q}_p^{ur}}$ with potentially good reduction of type A_m, and are defined by the equation $Y^p = \prod_{0\le i\le m}(1-T_iX)^{h_i}$, where $(T_i)_i \in (\mathbb{Z}_p{}^{ur})^{m+1}$ are in $m+1$ distinct classes mod p and satisfy $h_0T_0^k + h_1T_1^k + \cdots + h_mT_m^k = 0$, $0\le k\le m-1$, for $(h_i)_{0\le i\le m} \in (\mathbb{Z}\setminus p\mathbb{Z})^{m+1}$.*

Proof. Let σ be an order p automorphism of $D^o = \mathrm{Spec}\, R[\![Z]\!]$ with no inertia at (π), conductor $m+1$ and $(h_0,...,h_m)$ its Hurwitz data with $\sum_i h_i = 0$. By Th. II.3.1.2 σ corresponds to a generic μ_p-torsor of $\mathbb{P}^1_K$ with equation:

$$Y^p = \prod_{0\le i\le m}(1-X_iX)^{h_i} := f(X).$$

Moreover, as it has good reduction of type A_m relative to some Gauss valuation, it follows from Lemma V.6.3.2 below that there is an equation such that:

- $v(X_i)\ge 0$ for each i, the X_i give $m+1$ distinct points mod π, and one can prescribe the classes $\bar{X}_0 = t_0$ and $\bar{X}_1 = t_1$ in $\mathbb{F}_p^{alg}$;
- the Gauss valuation relative to $T := \lambda^{p/m}X^{-1}$ induces the good reduction and so $f(X) = 1 + s_1X + \cdots + s_mX^m + \cdots$ satisfies $v(s_k) \ge (m-k)\dfrac{p}{m}v(\lambda)$, for $1\le k\le m$ and $v(s_m) = 0$.

Let $p_k := h_0X_0^k + h_1X_1^k + \cdots + h_mX_m^k$ for $0\le k\le m$. Then considering the Newton formuli:

$$p_k - p_{k-1}s_1 + p_{k-2}s_2 + \cdots + (-1)^{k-1}p_1s_{k-1} + (-1)^k s_k = 0$$

and an inductive argument shows that $v(p_k) \ge (m-k)\dfrac{p}{m}v(\lambda)$, for $1\le k\le m$, and $v(p_m) = 0$. This means that the X_i satisfy the system

$$h_0X_0^k + h_1X_1^k + \cdots + h_mX_m^k = p_k, \quad 1\le k\le m, \tag{$**$}$$

subject to the conditions $v(X_i)\ge 0$, $v(X_i - X_j) = 0$ and $v(p_k) \ge (m-k)\dfrac{p}{m}v(\lambda)$.

Let $(t_0, t_1, \ldots, t_m)$ be the residue classes of $X_i \bmod \pi$ which give a proper solution of III.4.1 $(*)$, and moreover are in $\mathbb{F}_p^{alg}$. By III.4.2.1 we can lift this solution to $(T_0, T_1, \ldots, T_m) \in (\mathbb{Z}_p^{ur})^{m+1}$ such that the T_i satisfy the system

$$h_0T_0^k + h_1T_1^k + \cdots + h_mT_m^k = 0, \quad 1\le k\le m-1,$$

and by construction one has $v(T_i - X_i) > 0$ for $0\le i\le m$.

The next step is to inductively build an automorphism τ of the open disc $v(T = \lambda^{p/m}X^{-1}) > 0$ such that $\tau(\lambda^{p/m}T_i) = \lambda^{p/m}X_i$. In order to simplify the equations that follow we will write $r := \lambda^{p/m}$. Let

$$\tau(T) := rX_0\frac{T - rT_1}{rT_0 - rT_1} + rX_1\frac{T - rT_0}{rT_1 - rT_0} \in R[\![T = rX^{-1}]\!].$$

Then τ sends rT_0 (resp. rT_1) to rX_0 (resp. rX_1). Now assume we have found an automorphism τ_n of $R[\![T]\!]$ which satisfies $\tau_n(rT_i) = rX_i$ for $i\le n-1$. (Observe that such an automorphism preserves the closed disc $v(T)\ge v(r)$.) So applying Lemma V.6.3.3 below, after a change of parameter we can assume that $T_i = X_i$ for $i\le n-1$. After renumbering we can assume that $v(\rho) := v(X_n - T_n) = \inf_{n\le i\le m} v(X_i - T_i)$ and we show that $v(\rho)\ge (n-1)v(r)$. If $v(\rho) < (n-1)v(r)$, then we can write the system $(**)$ in the following way:

$$h_n(X_n^k - T_n^k) + \cdots + h_m(X_m^k - T_m^k) = p_k, \quad 1\le k\le m-1 \tag{$***$}$$

and set h_i' equal to the image of $h_i\dfrac{X_i-T_i}{\rho} \bmod \pi$. Then we remark that

$$\frac{X_i^k-T_i^k}{\rho}=kh_i'T_i^{k-1} \bmod \pi$$

and as

$$v(\frac{p_k}{\rho})\geq (m-k)v(r)-v(\rho)>(m-n+1-k)v(r)\geq 0,$$

the first $m-n+1$ equations of the system $(***)$ induce a Vandermonde type system $\bmod \pi$ with non-zero determinant. This contradicts the fact that the $h_i\not\equiv 0 \bmod p$. Now if we consider

$$\tau_{n+1}(T)=T+\frac{rX_n-rT_n}{\prod\limits_{0\leq i<n}(rT_n-rT_i)}\prod_{0\leq i<n}(T-rT_i)\in R[\![T]\!],$$

the conditions $\tau_{n+1}(T_i)=X_i$ are satisfied for $i\leq n$.

So we have two μ_p-torsors of the open disc $\operatorname{Spec} R[\![T]\!]$ with the same branch locus, say $Y_1^p=\prod\limits_{0\leq i\leq m}(1-T_iX)^{h_i}$ and $Y_2^p=\prod\limits_{0\leq i\leq m}(1-T_iX)^{h_i}U(T)$, where $U(T)=1+$ something small. It follows from Abhyankar's lemma and purity of the branch locus that the compositum gives p copies of the open disc. Hence the two torsors are equal (they have the same Hurwitz data).

Lemma 6.3.2. *Let C be a given generic μ_p-torsor of $\mathbb{P}^1_K$, which has good reduction of type A_m and suppose $m<p$. Then there is an equation of the torsor*

$$Y^p=\prod_{0\leq i\leq m}(1-X_iX)^{h_i}=:f(X)$$

for $X_i\in R$ reducing to $m+1$ distinct classes $\bmod \pi$ and such that the T-Gauss valuation for $T=\lambda^{p/m}X^{-1}$ induces the good reduction. Moreover, $f(X)=1+s_1X+\cdots+s_mX^m+\cdots$ satisfies the inequalities $v(s_k)\geq (m-k)\dfrac{p}{m}v(\lambda)$ for $1\leq k\leq m$ and $v(s_m)=0$.

Proof. The existence of an equation as above such that $T=\lambda^{p/m}X^{-1}$ induces the good reduction follows immediately from Th. III.3.1. Now we prove that for such an equation one has the desired inequalities. To do so we write:

$$\begin{aligned}f(X)&=1+s_1X+\cdots+s_mX^m+\cdots\in R[\![X]\!]\\&=1+s_1rT^{-1}+\cdots+s_mr^mT^{-m}+\cdots\in R\langle T^{-1}\rangle\end{aligned}$$

where $r=\lambda^{p/m}$. One has to prove that $v(s_kr^k)\geq v(\lambda^p)$, for $1\leq k\leq m$, and $v(s_mr^m)=v(\lambda^p)$, (i.e. $v(s_m)=0$). We prove this assertion by contradiction.

Let $\delta:=\inf_{1\leq k\leq m}v(s_kr^k)$, and suppose that $\delta<v(\lambda^p)$. Then there exists $k_0<m$ such that $\delta=v(s_{k_0}r^{k_0})<v(s_kr^k)$ for $k>k_0$. We write $X=\dfrac{r}{\rho^p}\big(\dfrac{T}{\rho^p}\big)^{-1}$, with $0<v(\rho^p)$ for $\rho\in R^{alg}$. We study $f(X)$ on the closed disc $v(T)\geq v(\rho^p)$ and so use the writing:

$$f(X)=1+s_1\big(\frac{r}{\rho^p}\big)\big(\frac{T}{\rho^p}\big)^{-1}+s_2\big(\frac{r}{\rho^p}\big)^2\big(\frac{T}{\rho^p}\big)^{-2}+\cdots.$$

Now for $0<v(\rho^p)$ small enough one has

$$\inf_{1\leq k\leq m}v\big(s_k\big(\frac{r}{\rho^p}\big)^k\big)=v\big(s_{k_0}\big(\frac{r}{\rho^p}\big)^{k_0}\big)<v(\lambda^p).$$

Then, by Prop. III.1.2 it follows that the gradient of the different above the annulus $v(T) = v(\rho^p)$ for $v(\rho)$ small enough is $(p-1)k_0$. However, as the torsor has good reduction of type A_m it follows from II.1 that this gradient is in fact $(p-1)m$, which is a contadiction. Therefore $\delta \geq v(\lambda^p)$.

It remains to show that $v(s_m) = 0$. Assume otherwise, then $v(s_m) > 0$ and so we have $v(s_k) > 0$ for $1 \leq k \leq m$ which implies $v(p_k) > 0$ for $1 \leq k \leq m$ where $p_k = h_0 X_0^k + \cdots + h_m X_m^k$. Letting t_i denote the residue of $X_i \bmod \pi$, we obtain the system

$$h_0 t_0^k + h_1 t_1^k + \cdots + h_m t_m^k = 0, \quad 0 \leq k \leq m,$$

whose determinant is non-zero; this implies $h_i \equiv 0 \bmod p$, which is a contradiction.

Lemma 6.3.3. *Let $1 < m < p$, and $r = \lambda^{p/m} \in R$. Let $\tau \in \mathrm{Aut}_R R[\![T]\!]$ be such that $\tau(T) = a_0 + a_1 T + \cdots \in R[\![T]\!]$ and $a_0 \in rR$. Let $(X_0, X_1, \ldots, X_m) \in R^{m+1}$ satisfy the following conditions*

i) $v(X_i) \geq 0$, $v(X_i - X_j) = 0$ *for* $i \neq j$,

ii) $v(p_k r^k) \geq v(\lambda^p)$ *where* $p_k := h_0 X_0^k + h_1 X_1^k + \cdots + h_m X_m^k$, $0 \leq k \leq m$.

Let $X_i' := r^{-1}\tau(rX_i) = r^{-1}(a_0 + a_1 r X_i + a_2 r^2 X_i^2 + \cdots)$, then the $(m+1)$-tuple $(X_0', X_1', \ldots, X_m') \in R^{m+1}$ satisfies the same conditions.

The proof follows directly and is left to the reader.

VI. References

[B] N. Bourbaki, *Algèbre Commutative*, Hermann, Paris 1961.

[Co] R. F. Coleman, *Torsion points on Curves*, Advanced Studies in Pure Mathematics 12, (1987), Galois Representations and Arithmetic Algebraic Geometry, 235–247.

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

[Cr] R. Crew, *Etale p-covers in characteristic p*, Compositio Math. 52 (1984), 31–45.

[D1] M. Deuring, *Automorphismen und Divisorenklassen der Ordnung l in algebraischen Funktionenkörpern*, Math. Ann. 113, 208–215 (1936).

[D2] M. Deuring, *Invarianten und Normalformen elliptischer Funktionenkörper*, Math. Zeit. 47 (1941), 47–56.

[Ga] M. Garuti, *Prolongement de revêtement galoisiens en géométrie rigide*, Compositio Math., 104 (1996), 305-331.

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

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

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

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

[O] F. Oort, *Lifting Algebraic Curves, Abelian Varieties, and Their Endomorphisms to Characteristic Zero*, Proceedings of Symposia in Pure Mathematics, Vol 46 (1987).

[O-S-S] F. Oort, T. Sekiguchi, N. Suwa, *On the deformation of Artin-Schreier to Kummer*, Ann. scient. Éc. Norm. Sup., 4e série, t. 22 (1989), 345–375.

[Ra 1] M. Raynaud, *Revêtements dela droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar*, Invent. Math. 116 (1994), 425–462.

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

[Ra 3] M. Raynaud, *p-groupes et réduction semi-stable des courbes*, The Grothendieck Festschrift, Vol III, Progress in Mathematics 88 (1990), Birkhaüser, 179–197.

[Ra 4] M. Raynaud, *Letter to the authors, November 15th 96.*

[Ro] P. Roquette, *Abschätzung der Automorphismenzahl von Funktionenkörpern bei Primzahlcharacteristik*, Math. Zeit., 117 (1970), 157–163.

[Sa] I.R. Šafarevičh, *On p-extensions*, AMS Transl. series II, 4 (1954), 59–72.

[Si] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer Verlag, 1986.

B. W. Green
Department of Mathematics
University of Stellenbosch
Stellenbosch, 7602
South Africa
email: bwg@land.sun.ac.za

M. Matignon
Mathématiques Pures de Bordeaux
E.R.S. 0127 C.N.R.S.
Université de Bordeaux I
351, cours de la Libération
33405 – Talence, Cedex
France
email: matignon@math.u-bordeaux.fr