代数幾何学シンポジウム記録
2000年度 pp.168-181

On the moduli space of order p^n automorphisms of the p-adic open disc

By

Barry Green [1])

1. Introduction

The aim of this talk is to survey and build on recent work on liftings of galois covers of smooth curves defined over an algebraically closed field k of characteristic p, to relative smooth galois covers of curves over a suitable valuation ring R of characteristic 0, dominating the Witt vectors $W(k)$. In the first five sections we draw attention to the recent results and methods used to attack this problem.

Due to a *local-global-principle* for lifting galois covers of smooth curves, this problem reduces to the problem of lifting groups of automorphisms of a formal power series ring over k to groups of automorphisms of a formal power series ring over the valuation ring R dominating $W(k)$. Thus we are led to the study of finite order automorphisms of the p-adic open disc and the geometry of their fixed points. In this context those of p-power order are crucial to this study as we show in section four.

The *local-global-principle for liftings* gives necessary and sufficient conditions, whereby liftings of the inertia groups acting on the completions of the local rings at the points of a galois cover of smooth curves over k to smooth galois covers of the p-adic open disc over R, ensures a global lifting to a galois covering of smooth relative curves over R. The completed local rings are formal power series rings over k and R respectively, and so provide the setting for this investigation.

In the final section we present a moduli space parametrization of order p^n automorphisms of of the p-adic open disc $\operatorname{Spec} R[\![Z]\!]$ with fixed points, and discuss its elementary properties. We also show how the *Oort-Sekiguchi conjecture* for galois

---

[1]) The author would like to express his thanks to Professors Sekiguchi and Suwa for their hospitality during his visit to the Mathematics Department at Chuo University, Tokyo.

liftings of covers of smooth curves from characteristic p to characterisitic 0 can be interpreted in this situation and discuss Hensel's lemma type conditions on the parametrization which would imply this conjecture.

2. Motivating Questions

We are interested in the following situation and questions:

Situation and Notation: Let k be an algebraically closed field of characteristic $p > 0$, and C/k be a complete, non-singular, irreducible curve of genus g. Let R be a complete discrete valuation ring dominating the ring of Witt vectors $W(k)$ and having uniformizing parameter π. We denote the quotient field of R by K, which is assumed finite over $\mathrm{Quot}(W(k))$, and the corresponding integral and algebraic closures by $\tilde{R}$ and $\tilde{K}$.

Motivating Questions: *Let G be a finite subgroup of $\mathrm{Aut}_k(C)$ and suppose $C \longrightarrow D = C/G$ is a finite galois cover of smooth proper integral curves over k.*

1. Global question: *Is it possible to find R as above and a finite galois cover of smooth proper integral relative curves over R, $\mathcal{C} \longrightarrow \mathcal{D} = \mathcal{C}/G$, which lifts the given cover $C \longrightarrow D$?*

2. Local question: *Let $y \in C$ and $I_y \subseteq \mathrm{Aut}_k(\hat{\mathcal{O}}_{C,y} \cong k[\![z]\!])$ be the associated inertia group. Is it possible to find R as above such that the inertia group lifts to $I_y \subseteq \mathrm{Aut}_R R[\![Z]\!]$?*

Remark. Clearly if the global question is satisfied then for each $y \in C$, we have $I_y \subseteq \mathrm{Aut}_R(\hat{\mathcal{O}}_{\mathcal{C},y} \cong R[\![Z]\!])$, so the local question is satisfied for each point $y \in C$. It turns out that the converse of this result is also true. This non-trivial theorem is the *local-global-principle for liftings* referred to in the introduction. We briefly sketch the proof method of this result in the next section and refer the reader to [G-M1] for details and to [Be-Me] and [H1] for alternative proofs.

Historical background:

- If $(|G|, p) = 1$ the answer to the global question is yes for any R, by Grothendieck, SGA I.
- If $|G| > 84(g-1)$ then the answer is no, due to a contradiction using Hurwitz bounds. In chararacteristic p there exist curves C/k such that one can choose G with $|G| > 84(g-1)$, see [Ro], but in characteristic 0 the order of the automorphism group of a curve of genus g is at most $84(g-1)$.

  One remarks that if G is abelian then by Nakajima, [N], the bounds for $G \subset \mathrm{Aut}_k(C)$ are the same in any characteristic and so in this case one doesn't expect a contradiction using bounds. So one speculates that for such G smooth liftings may always exist, and the first case one studies is for G cyclic. Here one knows:

- If G is cyclic of order pe, with $(e,p) = 1$, the answer is yes if R contains a primitive p-th root of unity, say ζ. This result is due to Oort–Sekiguchi–Suwa, [O–S–S].

Following these results it became natural to conjecture the following generalisation (see [S], [O1] and [O2]):

Oort-Sekiguchi Conjecture: *The answer to the global lifting question is positive if G is a cyclic group.*

In a number of recent papers, see for example [G-M1], [Be], [M] and [G] necessary conditions for the solvability of the lifting problem when the p-parts of the inertia groups aren't cyclic are given. Concerning the conjecture one of the main results of [G-M1] answers it positively for G-galois covers whose inertia groups are $p^a e$-cyclic with $a \leq 2$ and $(e,p) = 1$. More precisely one has:

Theorem [G-M1]. *Let $f: C \longrightarrow C/G := D$ be a G-galois cover of proper smooth curves over k. Assume that the inertia groups are $p^a e$-cyclic with $a \leq 2$ and $(e,p) = 1$. Then f can be lifted over $R = W(k)[\zeta_{(2)}]$ as a G-galois cover of smooth R-curves, where $\zeta_{(2)}$ is a primitive p^2-root of unity.*

By the *local-global-principle for liftings* the crucial question is the local one, namely that of the existence of liftings of G-galois covers of formal power series rings $k[\![z]\!]/k[\![z]\!]^G = k[\![t]\!]$ over k to G-galois covers of the formal power series rings $R[\![Z]\!]/R[\![Z]\!]^G = R[\![T]\!]$ over R, for R and G as above. This is the condition which ensures smoothness of the lifting of curves. In contrast, the methods used by Oort, Sekeguchi and Suwa to attack the lifting question are global in the sense that they use generalized Jacobians.

When trying to construct a lifting of a G-galois cover of formal power series rings $k[\![z]\!]/k[\![z]\!]^G = k[\![t]\!]$ over k to one of the formal power series rings over R, there is a useful *smoothness criterion* based on a result of Kazuya Kato in [K], which we use. In our situation suppose $k[\![z]\!]/k[\![z]\!]^G = k[\![t]\!]$ and $E = \mathrm{Quot}(R[\![T]\!])$ are given. Then if we can find a finite G-galois field extension F of E such that for the integral closure of $R[\![T]\!]$, say B,

i) $\mathrm{Quot}(B/\pi B) = k((z))$ and

ii) the different of B over $R[\![T]\!]$ equals that of $k[\![z]\!]$ over $k[\![t]\!]$,

it follows $B \cong R[\![Z]\!]$, with $B/\pi B \cong k[\![z]\!]$ and $R[\![Z]\!]/R[\![Z]\!]^G = R[\![T]\!]$ as desired.

Consequently we are led to study liftings determined by equations and comparison of the generic and special differents. For p^2-cyclic extensions one needs a presentation from which one can easily read the degree of the different; this is done via Artin-Schreier-Witt Theory in [G-M1] (see Lemma 5.1 in Section II). The first challenge is to lift the equations as a p^2-cyclic cover of the open disc, $\mathrm{Spec}\, R[\![T]\!]$, and this can be done using Sekiguchi and Suwa's recent work *"On the* *unified Kummer-Artin-Schreier-Witt theory"*, [S-S1] and [S-S2]. However, in order to cover the disc by discs (i.e ensuring that the integral closure determines a disc, so introducing no new "genus") one needs to minimize the degree of the generic different. This is done in [G-M1] by developing the theory from [S-S1] in an effective way, so giving explicit equations for liftings over open discs. As a result this gives rise to p^2-order and so (taking the p-power composition) p-order automorphisms of the open disc which are not defined over $W(k)[\zeta]$ and so are of quite distinct nature from those appearing in [O-S-S] for p-cyclic covers. Although one hopes to be able to study the p^3 and general cases in this way, at present this appears to be technically very difficult.

We remark that for lifting order p automorphisms one can show that $\bmod \pi$, the automorphisms

$$Z \mapsto Z(\zeta^{-m} + Z^m)^{-1/m},$$

for $(m,p) = 1$ and ζ a primitive p-th root of unity, define the extension of $k((t))$ given by the Artin-Schreier equation:

$$x^p - x = 1/t^m$$

and one can use these in a way that mimics [O-S-S] in order to lift galois covers whose p-inertia at each point is cyclic of order at most p.

3. The local-global-principle for liftings

In this section we briefly sketch how rigid analytic geometry is used to solve the lifting problem, under the assumption that for each $y \in C$, $I_y \subseteq \mathrm{Aut}_k \hat{\mathcal{O}}_{C,y}$ lifts to $I_y \subseteq \mathrm{Aut}_R [\![Z]\!]$, for suitable R. We remark that in [G-M1] this local-global-principle was only proved for $p^a e$-cyclic covers, $a \leq 2$, as that was the context we were concerned with. The method explained there is general though and one has:

Theorem. *In the situation above, given $(C/k, G)$ with $G \subseteq \mathrm{Aut}_k C$, we can find a smooth proper connected galois lifting $(\mathcal{C}/R, G)$ for suitable R dominating $W(k)$ if and only if for each $y \in C$, $I_y \subseteq \mathrm{Aut}_k(\hat{\mathcal{O}}_{C,y} \cong k[\![z]\!])$ lifts to $I_y \subseteq \mathrm{Aut}_R R[\![Z]\!]$?*

Proof sketch. Suppose $f: C \longrightarrow D = C/G$ and let $\mathcal{D}$ denote a smooth relative curve over $W(k)[\zeta_{(2)}]$ whose special fiber is D. Denote by $\mathcal{D}^{\mathrm{an}}$ the generic fibre endowed with rigid analytic structure and let $r: \mathcal{D}^{\mathrm{an}} \longrightarrow D$ be the reduction map. Let $U \subset D = C/G$ be the étale locus, and $\mathcal{U} \subset \mathcal{D}^{\mathrm{an}}$, be the affinoid defined by $\mathcal{U} = r^{-1}(U)$. Then by Grothendieck, up to isomorphism one can lift in a unique diagram

$$\begin{array}{ccc} \mathcal{V} & \xrightarrow{\tilde{f}} & \mathcal{U} \subset \mathcal{D}^{\mathrm{an}} \\ \downarrow r & & \downarrow r \\ V & \xrightarrow{f} & U \subset D \end{array}$$

where $V = f^{-1}(U) \subset C$ and $\mathcal{U} = \mathcal{V}/G$. The aim is to compactify the morphism $\tilde{f} : \mathcal{V} \longrightarrow \mathcal{U}$ with a morphism of discss in a G-galois way. For this one extends $\tilde{f}$ to a G-galois étale cover $\tilde{f}' : \mathcal{V}' \longrightarrow \mathcal{U}' \subset \mathcal{D}^{\mathrm{an}}$ where $\mathcal{U}'$ is the union of $\mathcal{U}$ and suitable annuli. On the other hand, for each $x \in D - U$, if we are able to lift

$$\coprod_{y:\, f(y)=x} \operatorname{Spec} \hat{\mathcal{O}}_{C,y} \longrightarrow \operatorname{Spec} \hat{\mathcal{O}}_{D,x}$$

in a G-galois cover of open discs, then using a prolongation lemma (see [G-M1] or [H1]) one can glue this cover to $\tilde{f}' : \mathcal{V}' \longrightarrow \mathcal{U}'$ along the morphisms induced on the annuli $\mathcal{U}' - \mathcal{U}$. In this we we obtain a global lifting of the cover.

Hence the global lifting question reduces to the local one, i.e. whether over the open disc $\operatorname{Spec} R[[T]]$, we have open discs, and this investigation reduces to studying the geometry of automorphisms of open discs.

4. Finite order automorphisms of the p-adic open disc

As in the previous sections the rings of formal power series over k and R are denoted by $k[[z]]$ and $R[[Z]]$, respectively. Note that $R[[Z]]$ is a two dimensional local ring with maximal ideal generated by Z and π, and its height one prime ideals are all principal. If $\sigma \in \operatorname{Aut}_R(R[[Z]])$ then we can write

$$\sigma(Z) = a_0 + a_1 Z + a_2 Z^2 + a_3 Z^3 + \cdots,$$

where $a_0 \in \pi R$ and $a_1 \in R^\times$. We denote the identity morphism on $R[[Z]]$ (respectively $k[[z]]$) by $\mathbf{1}$. From the context this will not lead to confusion. Observe that reducing the coefficients of σ modulo (π), we obtain a canonical surjective group homomorphism

$$\Psi : \operatorname{Aut}_R(R[[Z]]) \longrightarrow \operatorname{Aut}_k(k[[z]]).$$

In view of the discussion in the previous sections we are interested in the following questions:

Lifting Questions: *1. If $\overline{\sigma}$ is a k-automorphism of $k[[z]]$ of finite order, when can we find a lifting of σ to an R-automorphism of $R[[Z]]$ of the the same order, i.e. an R-automorphism σ of $R[[Z]]$ of the the same order such that $\Psi(\sigma) = \overline{\sigma}$?*

More generally if $\overline{G}$ is a finite subgroup of $\mathrm{Aut}_k(k[\![z]\!])$, when can one find a section of $\overline{G}$ in $\mathrm{Aut}_R(R[\![Z]\!])$ with respect to Ψ?

2. If G is a finite group, give criteria depending on the structure of the group, which need to be satisfied in order that a realisation $G \subset \mathrm{Aut}_k(k[\![z]\!])$ can be lifted to $G \subset \mathrm{Aut}_R(R[\![Z]\!])$, for some complete discrete valuation ring R dominating $W(k)$?

The first question is the one we are concerned with here, For the others we refer the reader to [G-M1], [G-M2], [Be], [M] and [G].

4.1. Automorphisms and their fixed points

In order to investigate the questions mentioned above it is useful to study data associated with the fixed points determined by the action of $\sigma \in \mathrm{Aut}_R(R[\![Z]\!])$ on the open disc $D = \mathrm{Spec}\, R[\![Z]\!]$.

Given $\sigma(Z) = \sum_{i=0}^{\infty} a_i Z^i \in \mathrm{Aut}_R(R[\![Z]\!])$, it induces a $\mathrm{Spec}\, R$ automorphism of the open disc $D = \mathrm{Spec}\, R[\![Z]\!]$, which we call $\tilde{\sigma}$. For rational points $(Z - \alpha) \in D$, ($\alpha \in \pi R$), one has $\tilde{\sigma}((Z - \alpha)) = (Z - \tilde{\alpha})$, where $\tilde{\alpha} = \sum_{i=0}^{\infty} a_i \alpha^i$. Such a point is a fixed point if and only if $\alpha = \tilde{\alpha}$. More generally $P \in D$ is a fixed point of $\tilde{\sigma}$ if and only if $P = (\pi, Z)$, (π), (0), or a height one prime ideal of $R[\![Z]\!]$ and $P \supset (\sigma(Z) - Z)$. When we speak of fixed points we shall always mean the points this last set defines in the geometric generic fibre and denote this set by F_σ. These points correspond to the zeros of the series $\sigma(Z) - Z$ in $\tilde{R}$, and to simplify our discussion we shall enlarge R suitably so that they are R-rational. Using the Weierstrass Preparation Theorem they can be described as follows.

Let $m_\sigma = \inf_{l \geq 0}\{i : v(a_l) \leq v(a_i) \text{ for all } i\}$, then

$$\sigma(Z) - Z = a_{m_\sigma} f_{m_\sigma}(Z)\, u(Z),$$

where $u(Z) - 1 \in (\pi, Z)$ and $f_{m_\sigma}(Z)$ is a unitary distinguished polynomial of degree m_σ, so that $|F_\sigma| = m_\sigma$. Note that if $m_\sigma \neq 0$, so that for some α, $v(\alpha) > 0$ we have $(Z - \alpha) \in F_\sigma$, we can centre σ at $Z = \alpha$ (replace the parameter Z by $Z - \alpha$) and so obtain $\sigma(Z) = \sum_{i=1}^{\infty} b_i Z^i$, for suitable b_i with $v(b_1) = 0$. If σ has finite order, say $o(\sigma) = n$, then $\zeta = b_1$ is an n-th root of unity which must be primitive by 4.2.1 below, so we can express σ by

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

where the coefficients a_i are distinct from those used previously. We next recall a number of elementary facts on finite order automorphisms needed for our discussion. The first five can be found in [G-M1] and for the sixth we give a proof.

4.2. Elementary Facts: *Suppose that $\sigma \in \mathrm{Aut}_R(R[\![Z]\!])$ has finite order, say $o(\sigma) = n$. Then:*

4.2.1. *If $\sigma(Z) \equiv Z \bmod Z^2$ then $\sigma = \mathbf{1}$, i.e. $n = 1$.*

4.2.2. *If $\Psi(\sigma) \neq \mathbf{1}$ then σ can be represented as*

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

where ζ is a primitive n-th root of 1.

4.2.3. *If $(n,p) = 1$, then σ is linearizable and consequently $\bar{\tau}$ has exactly one fixed point.*

We first note that by [G-M1], p. 242, σ has a fixed point and so can be represented by $\sigma(Z) = \zeta Z(1+a_1Z+a_2Z^2+\cdots)$, where ζ is a primitive n-th root of 1. Now set $Z' = Z + \zeta^{-1}\sigma(Z) + \cdots + \zeta^{-(n-1)}\sigma^{n-1}(Z)$. Then $\sigma(Z') = \zeta Z'$, $Z' \equiv nZ \bmod Z^2$ and as $n \in R^\times$, we have $R[\![Z]\!] = R[\![Z']\!]$.

Note that this argument works over positive characteristic fields with characteristic prime to n as well, provided they contain the required roots of unity.

4.2.4. *If $o(\sigma) = p^r$ and $\Psi(\sigma) \neq \mathbf{1}$, then σ isn't linearizable.*

If it were then $\sigma(Z) = \zeta Z$, which implies $\Psi(\sigma) = \mathbf{1}$, a contradiction.

4.2.5. *If $\bar{\sigma} \in \mathrm{Aut}_k(k[\![z]\!])$ with $o(\bar{\sigma}) = n$ and $(n,p) = 1$ then there exists $\sigma \in \mathrm{Aut}_R(R[\![Z]\!])$ with $\Psi(\sigma) = \bar{\sigma}$ and $o(\sigma) = n$.*

This follows directly from 4.2.3 above.

4.2.6. *If $\bar{\sigma} \in \mathrm{Aut}_k(k[\![z]\!])$ with $o(\bar{\sigma}) = n = ep^r$, $(e,p) = 1$, and if we are able to lift automorphisms of $k[\![z]\!]$ of order p^r, then there exists $\sigma \in \mathrm{Aut}_R(R[\![Z]\!])$ with $\Psi(\sigma) = \bar{\sigma}$ and $o(\sigma) = n$.*

Let $\bar{\sigma} \in \mathrm{Aut}_k(k[\![z]\!])$ with $o(\bar{\sigma}) = n = ep^r$, $(e,p) = 1$, be given and set $\bar{\tau} = \bar{\sigma}^{p^r}$. Then $o(\bar{\tau}) = e$ and so for some primitive e-th root of 1, say $\bar{\gamma}$, and parameter z' we have $\bar{\tau}(z') = \bar{\gamma} z'$ and $k[\![z']\!] = k[\![z]\!]$. If we let $t = z'\bar{\tau}(z')\cdots\bar{\tau}^{e-1}(z') = \left(\bar{\gamma}^{(e-1)/2}z'\right)^e$, then $k[\![z']\!]^{\langle\bar{\tau}\rangle} = k[\![t]\!]$. For convenience we replace $\bar{\gamma}^{(e-1)/2}z'$ by z'' and note that $k[\![z'']\!] = k[\![z']\!]$. Now $\bar{\sigma}|_{k[\![t]\!]}$ has order p^r and power series representation

$$\bar{\sigma}(t) = t(1 + \bar{a}_1 t + \cdots).$$

Rewriting in terms of z'' we have

$$\bar{\sigma}(z''^e) = z''^e(1 + \bar{a}_1 z''^e + \cdots)$$

and so

$$\bar{\sigma}(z'') = z''(1 + \bar{a}_1 z''^e + \cdots)^{1/e}.$$

Now let $\sigma(T) = \zeta T(1 + a_1 T + \cdots)$ be an order p^r automorphism lifting $\bar{\sigma}$ to $R[\![T]\!]$, where ζ is a suitable primitive p^r-th root of 1. Next we consider the tame extension E of $F = \mathrm{Quot}(R[\![Z]\!])$ defined by $Z''^e = T$. Then the integral closure of $R[\![T]\!]$ in E is $R[\![Z'']\!]$ and as $\sigma(Z''^e) = \zeta Z''^e(1 + a_1 Z''^e + \cdots)$, it follows σ extends to an order $n = ep^r$ automorphism of $R[\![Z'']\!]$ defined by $\sigma(Z'') = \zeta^{1/e} Z''(1 + a_1 Z''^e + \cdots)^{1/e}$. Furthermore with respect to the morphism $\Psi : \mathrm{Aut}_R(R[\![Z'']\!]) \longrightarrow \mathrm{Aut}_k(k[\![z'']\!])$, we have $\Psi(\sigma) = \overline{\sigma}$ as desired.

Hence the first *lifting question* reduces to:

Given $\overline{\sigma} \in \mathrm{Aut}_k(k[\![z]\!])$ with $o(\overline{\sigma}) = p^r$, find $\sigma \in \mathrm{Aut}_R(R[\![Z]\!])$ with $\Psi(\sigma) = \overline{\sigma}$ and $o(\sigma) = p^r$.

Note the by the local-global-principle for liftings a positive answer to this question would imply the *Oort-Sekiguchi Conjecture.* As mentioned in the introduction we have:

Theorem 4.3. *Let $\overline{\sigma} \in \mathrm{Aut}_k(k[\![z]\!])$ with $o(\overline{\sigma}) = p^r$, with $r = 1, 2$. Then there exists $\sigma \in \mathrm{Aut}_R(R[\![Z]\!])$ with $\Psi(\sigma) = \overline{\sigma}$ and $o(\sigma) = p^r$.*

The case $r = 1$ is treated in [O-S-S], and $r = 1, 2$ in [G-M1].

5. Comparison of the different: a local criterion for good reduction

In this section we draw attention to the smoothness criterion mentioned in section two, which is useful when trying to construct a lifting of a G-galois cover of formal power series rings $k[\![z]\!]/k[\![z]\!]^G = k[\![t]\!]$ over k to one of the formal power series rings over R. At present this is the only criterion we know of for attacking the lifting question, which has been used successfully. We include a brief outline here, but refer the reader to [G-M1] for details.

Let σ be an automorphism of $R[\![Z]\!]$ of finite order n, which we assume doesn't induce the identity residually $\bmod \pi$, so that σ has at least one fixed point. Enlarging R we can assume that 0 is such a fixed point and that $\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots)$, where ζ is a primitive n-th root of unity.

5.1. *Let $T = Z\sigma(Z) \cdots \sigma^{n-1}(Z) = \epsilon Z^n(1 + \cdots)$ where $\epsilon = (-1)^{(n-1)}$. Then $R[\![Z]\!]^{\langle\sigma\rangle} = R[\![T]\!]$.*

From [Bo], chap. 7, corollary, p. 40, one knows that $R[\![Z]\!]$ is a finite free $R[\![T]\!]$-module of rank n, generated by $1, Z, Z^2, \ldots, Z^{n-1}$. On the other hand by a dimension consideration it follows that $\mathrm{Fr}(R[\![Z]\!]^{\langle\sigma\rangle}) = \mathrm{Fr}(R[\![T]\!])$. As $R[\![Z]\!]^{\langle\sigma\rangle}$ is integral over $R[\![T]\!]$ which is integrally closed, the claim follows.

5.2. *Let d_η, resp. d_s, be the degrees of the generic, resp. special differents for the extension $R[\![Z]\!]/R[\![T]\!]$. Then $d_\eta = d_s$.*

On the moduli space of order p^n automorphisms of the p-adic open disc

Let $f(X) = \prod_{0 \leq i < n} (X - \sigma^i(Z))$ be the irreducible polynomial of Z over $R[\![T]\!]$. Then $f'(Z) = p(Z)u(Z)$ where $p(Z)$ is a distinguished polynomial and $d_\eta = \deg_Z p(Z)$. For the special different we have

$$d_s = v_z\big(\prod_i (z - \bar{\sigma}^i(z))\big)$$

and so the result follows by the Weierstrass Preparation Theorem.

Note that the same equality for the differents clearly holds for towers of such cyclic extensions. For the higher p-power oder cyclic lifting problem, however, the tower has to be built in such a way that in characteristic 0, the composite extension is galois, i.e. cyclic of the same p-power oder. Hence for this lifting problem we need:

i) equality of the differents to guarantee smoothness, and

ii) for the extension determining the cover to be galois.

For 5.2 there is a converse in the germ of curves context following from a formula given by Kato [K], section 5, which we have used successfully to satisfy i) above, when attacking the lifting problem. Adapting Kato's result to our situation we have:

5.3. Local criterion for good reduction. *Let $A = R[\![T]\!]$ and B be a finite A-module which is a normal integral local ring, and set $A_K = A \otimes_R K$, resp. $B_K = B \otimes_R K$. We assume that $B/\pi B = B_0$ is reduced and setting $A_0 := A/\pi A$, that the extension B_0/A_0 is generically étale. Let $\tilde{B}_0$ be the integral closure of B_0 and define $\delta_k(B) = \dim_k \tilde{B}_0/B_0$. Let d_η resp. d_s be the degrees of the generic resp. special differents, i.e. the degrees of the differents for the extensions B_K/A_K resp. B_0/A_0. Then $d_\eta = d_s + 2\delta_k(B)$ and moreover if $d_\eta = d_s$ it follows that $\delta_k(B) = 0$ and $B = R[\![Z]\!]$.*

Observation: Note that in order to apply 5.3 in our context, given $k[\![z]\!]/k[\![z]\!]^G = k[\![t]\!]$ and $A = R[\![T]\!]$ we need to construct B such that $\mathrm{Quot}(B_0) \cong k((z))$ and $d_\eta = d_s$.

6. Parametrizing order p^n automorphisms of $R[\![Z]\!]$

In this section we describe a moduli space parametrization of order p^n automorphisms of of the p-adic open disc $\operatorname{Spec} R[\![Z]\!]$ with fixed points, and discuss its elementary properties. We show how the *Oort-Sekiguchi conjecture* can be interpreted in this situation and discuss Hensel's lemma type conditions on the parametrization which would imply this conjecture. This work builds on results in [G-M2] where order p automorphisms with fixed points were considered.

Without loss of generality we work with $q = p^n$ automorphisms of $R[\![Z]\!]$, which have 0 as a fixed point and describe a parametrization of these. This will be done by fixing a given primitive q-th root of unity ζ, and studying the relationship between the coefficients in

$$\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots + a_m Z^m + \cdots)$$

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 q-th iterate as

$$\sigma^q(Z) = Z(1 + E_1 Z + \cdots + E_m Z^m + \cdots),$$

where $E_m \in \mathbb{Z}_p[\zeta][a_i]_i$. Let I_m denote the ideal of $R[a_1, a_2, \ldots, a_m]$ generated by $(E_j)_{1\leq j\leq m}$.

Theorem 6.1. *Using the notations above we have:*

- *i)* *The E_i are homogenous polynomials of degree i in the a_j with coefficients in R, where for each j, a_j is given the weight j.*
- *ii)* $E_1 = \ldots = E_{q-1} = 0$
- *iii)* $E_q, E_{q+1}, \ldots, E_{2q-1} \in R[a_1, a_2, \ldots, a_q]$, *and more generally for each positive integer m,*
  $E_{mq}, E_{mq+1}, \ldots, E_{(m+1)q-1} \in R[a_1, a_2, \ldots, a_{mq}]$.
- *iv)* *The coefficent of a_{mq} in E_{mq} is q.*
- *v)* *Let J_{mq} be the ideal of $R[a_1, \ldots, a_s]$ generated by $(E_{jq})_{1\leq j\leq m}$. Then for $mq < l < (m+1)q$ one has $E_l \in J_{mq} \otimes K =: KJ_{mq}$, where $K = \mathrm{Quot}(R)$.*
- *vi)* *For each $m \in \mathbb{N}$ we denote the image of E_m in $k[(a_i)_i]$ by $E_m v$. Then $E_i v = 0$, for $1 \leq i \leq q$, $E_i v \in k[a_1, \ldots, a_q]$, for $q + 1 \leq i \leq 2q$, and more generally $E_i v \in k[a_1, \ldots, a_{(m-1)q}]$, for $(m-1)q + 1 \leq i \leq mq$.*

Proof. i) 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 $E_m((a_i X^i)_i) = X^m E_m((a_i)_i)$, which shows that after assigning weights the polynomials are homogenous. Note that from this it follows that $E_m \in R[a_1, \ldots, a_m]$ and the coefficient of a_m in E_m is constant.

ii) Let $B = R[a_1, \ldots, a_q]$, then by truncation σ induces an endomorphism $\tilde{\sigma}$ on $BZ \oplus BZ^2 \oplus \cdots \oplus BZ^q$. The characteristic polynomial is $\prod_{1\leq i\leq q} (X - \zeta^i) = X^q - 1$, and so by the Cayley-Hamilton Theorem $\tilde{\sigma}^q = \mathbf{1}$, the identity. This is equivalent to ii).

We shall need to first prove v) in order to show iii):

v) We prove v) by induction, assuming it proved for $1 \leq m' < m$ and $mq < l' < l$. One has

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

and by the inductive hypothesis

$$\sigma^q(Z) = Z(1 + E_l Z^l) \bmod (K J_{mq}, Z^{l+2})$$

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

$$\zeta^{l+1} E_l Z^{l+1} \equiv \zeta E_l Z^{l+1} \bmod (K J_{kq}, Z^{l+2}).$$

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

iii) This assertion now follows from the fact that $E_{mq} \in R[a_1, \ldots, a_{mq}]$ and $K[a_1, \ldots, a_{mq}] \cap R[a_1, \ldots, a_{(m+1)q}] = R[a_1, \ldots, a_{mq}]$.

iv) From i) we know that the coefficient of a_{mq} in E_{mq} is a constant. Let I be the ideal $(a_1, \ldots, a_{mq-1}, Z^{mq+2})$ in $R[(a_i)_i][\![Z]\!]$. Then

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

and recurrently

$$\begin{aligned} \sigma^q(Z) &= \zeta^q Z(1 + q a_{mq} Z^{mq}) \bmod I \\ &= Z(1 + E_{mq} Z^{mq}) \bmod I \end{aligned}$$

finishing the proof.

vi) The only assertions which don't follow directly from the assertions already proved are that $E_q v = 0$ and $E_{mq} v \in k[a_1, \ldots, a_{(m-1)q}]$ for $m > 1$. This follows from the commutativity of σ and σ^q in $k[\![z]\!]$. Namely one has:

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

and

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

Therefore

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

so that $a_1 E_{mq} v \equiv 0 \bmod (I_{mq-1} v)$ which implies the result.

6.2. Remark: For takling the lifting problem we note that if

$$\bar{\sigma}(z) = z(1 + \bar{a}_1 z + \cdots) \in \mathrm{Aut}_k k[\![z]\!]$$

and $o(\bar{\sigma}) = q$, then by v) above, provided we can find a lifting

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

such that $E_{mq}\big((a_i)_i\big) = 0$ for $m \geq 1$, we will have $E_r\big((a_i)_i\big) = 0$ for each $r \geq 1$, so $o(\sigma) = q$.

It is tempting to try to apply the *Generalized Hensel's Lemma* to this question (see [Gr]). By the remark above it suffices to apply this to the equations to $E_{mq}\big((a_i)_i\big) = 0$ for each $m \geq 1$, and here the condition becomes:

For each $m \geq 1$ there exists constants $N_m \geq 1$, $c_m \geq 1$ and $s_m \geq 0$ such that if $\boldsymbol{a} = (a_1, a_2, \ldots, a_{mq}) \in R^{mq}$ satisfies $E_{mq}(\boldsymbol{a}) \equiv 0 \bmod \pi^{N_m}$ then there exists $\boldsymbol{b} = (b_1, b_2, \ldots, b_{mq})$ with $E_{mq}(\boldsymbol{a}) = 0$ and $\boldsymbol{b} \equiv \boldsymbol{a} \bmod \pi^{[N_m/c_m]-s_m}$.

For the lifting problem we need to find constants such that

$$[N_m/c_m] - s_m \geq 1.$$

Progress in this direction, even for special families of automorphisms where restrictions are placed on the equations $E_r\big((a_i)_i\big)$, would be very interesting.

6.3. The moduli space of order q automorphisms of $\mathrm{Spec}\, R[\![Z]\!]$

In our final paragraph we show how to associate an R-model with the ideals I_n, which parametrizes the order q automorphisms of $\mathrm{Spec}\, R[\![Z]\!]$ with 0 a fixed point. Computations show that in general there is π-torsion in the rings $R[a_1, \ldots, a_n]/I_m$ (For example for $q = p = 3$ one checks that $E_3/\lambda \in R[a_1, a_2, a_3]$, see [G-M2] p. 298), so in order to find a flat R-model we consider $\mathcal{I}_m := I_m K \cap R[a_1, \ldots, a_m]$ and define

$$\mathcal{X}_m := \mathrm{Spec}\, R[a_1, \ldots, a_m]/\mathcal{I}_m.$$

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

$$R[a_1, a_2, ..., a_m]/\mathcal{I}_m \longrightarrow R[a_1, a_2, ..., a_{m+1}]/\mathcal{I}_{m+1}$$

so that one can define:

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

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

$\mathcal{X}(R')$ corresponds bijectively to automorphisms of order q of $R'[\![Z]\!]$ such that $\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots)$.
Moreover, in this context the **Oort-Sekiguchi conjecture** corresponds to extending a k-section of $\mathcal{X}$ to an R-section as in the diagram:

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

References

[Be] J. Bertin, *Obstructions locales au relevement de revetements galoisiens de courbes lisses, (Local obstructions to lifting Galois covers of smooth curves)* C. R. Acad. Sci., Paris, Ser. I, Math. 326, No.1 (1998), 55–58.

[Be-Me] J. Bertin, A. Mézard, *Déformations formelles des revêtements sauvagement ramifiés de courbe algébriques*, Invent. math. 141 (2000), 195–238.

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

[G-M1] B. Green, M. Matignon, *Liftings of Galois Covers of Smooth Curves*, Compositio Mathematica, Vol 113 no. 3 (1998), 239–274.

[G-M2] B. Green, M. Matignon, *Order p automorphisms of the open disc of a p-adic field,* J. of the Amer. Math. Soc., Vol 12 no.1 (January 1999), 269–303.

[G] B. Green, *Automorphisms of formal power series rings over a valuation ring,* To appear in the proceedings of the International Conference on Valuation Theory, Saskatoon, July 1999.

[Gr] M. Greenberg, *Rational points in henselioan discrete valuation rings,* Inst. haut. Étud. sci., Publ. math. No. 31 (1966), 563–568.

[H1] Y. Henrio, *Arbres de Hurwitz et automorphismes d'ordre p des disques et des couronnes p-adiques formels,* To appear in Compositio Mathematica.

[H2] Y. Henrio, *Automorphismes d'ordre p des couronnes p-adiques ouvertes,* C.R. Acad. Sci. Paris, t.329, Série I (1999), 47–50.

[K] K. Kato (with collaboration of T. Saito), *Vanishing cycles, ramification of valuations, and class field theory,* Duke Math. J. 55, 3 (1987), 629–659.

[M] M. Matignon, *p-Groupes abéliens de type $(p, ..., p)$ et disques ouverts p-adiques,* manuscripta math., 99 (1999), 93–109.

[N] S. Nakajima, *On abelian automorphism groups of algebraic curves,* J. London Math. Soc. (2) 36 (1987), 23–32.

[O1] F. Oort, *Lifting Algebraic Curves, Abelian Varieties, and their Endomorphisms to Characteristic Zero,* Proceedings of Symposia in Pure Mathematics, Vol 46 (1987).

[O2] F. Oort, *Some questions in algebraic geometry,* Utrecht Univ., Math. Dept. Preprint Series, June 1995.

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

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

[S-O] T. Sekiguchi, F. Oort, *On the deformations of Witt Groups to Tori*, Algebraic and Topological Theories – to the memory of Dr. Takehiko Miyata (1985), 283–298.

[S-S1] T. Sekiguchi, N. Suwa, *On the unified Kummer-Artin-Schreier-Witt theory*, (Preprint series), CHUO MATH NO.41, (1994).

[S-S2] T. Sekiguchi, N. Suwa *On the unified Kummer-Artin-Schreier-Witt Theory*, Mathématiques Pures de Bordeaux C.N.R.S., Prépublication 111 (1999), 1–90.

Department of Mathematics, University of Stellenbosch, 7602 Stellenbosch, South Africa