Liftings of Galois Covers of Smooth Curves

By

Barry Green and Michel Matignon

Abstract: Let (C, G) be a smooth irreducible projective curve of genus g over an algebraically closed field k of chararacteristic $p > 0$ and G be a finite group of automorphisms of C. It is well known that here, contrary to the characteristic 0 case, Hurwitz's bound $|G| \leq 84(g-1)$ doesn't hold in general; in such cases this gives an obstruction to obtaining a smooth galois lifting of (C, G) to characteristic 0.

We shall give new obstructions of local nature to the lifting problem, even in the case where G is abelian. In the case where the inertia groups are $p^a e$-cyclic with $a \leq 2$ and $(e,p) = 1$, we shall prove that smooth galois liftings exist over $W(k)[\sqrt[p^2]{1}]$.

1991 AMS Subject Classification. Primary 11G20, 14H30; Secondary 14D15, 14E22.

Key Words: Sekiguchi-Suwa theory; order p^2 automorphisms of p-adic discs; rigid analytic geometry.

Contents

The authors would like to thank the Mathematisches Forschungsinstitut Oberwolfach for partially supporting this research through a Research in Pairs fellowship. The first author would also like to thank the Deutsche Forschungsgemeinschaft for supporting this work while he was a member of the Mathematisches Institut, Universität Heidelberg.

0. Introduction

In this paper we consider the following question:

Situation: Let k be an algebraically closed field of characteristic $p > 0$, and C/k be a complete, non-singular, irreducible curve of genus $g = g(C)$. Let R be a complete discrete valuation ring dominating the ring of Witt vectors $W(k)$ and π be a uniformising parameter of R.

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

Background Results:

- If $(|G|, p) = 1$ the answer is yes for any R, by Grothendieck, SGA I.
- If $|G| > 84(g(C) - 1)$ 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 then became natural to ask for the following generalisation (see [O1] I.7 and [O2]):

Conjecture: *The answer is yes if G is a cyclic group.*

In this paper we prove two main theorems. In the first we give necessary conditions for the solvability of the lifting problem when the p-parts of the inertia groups aren't cyclic. Our second main theorem answers the conjecture positively, for G-galois covers whose inertia groups are $p^a e$-cyclic with $a \leq 2$ and $(e, p) = 1$. More precisely in section I, 5.7, we prove:

Theorem 1. *Let $f\colon C \longrightarrow C/G := D$ be a G-galois cover of proper smooth curves over k. Let $y \in C$, $x = f(y)$ and suppose that the p-part of the corresponding inertia group, I_p, is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$. Then a necessary condition for f to be lifted as a G-galois cover of smooth R-curves, for some extension R of $W(k)$, is that the minimal conductor of the p-cyclic extensions of $\hat{\mathcal{O}}_{C,y}^{I_p}$ in $\hat{\mathcal{O}}_{C,y}$ is congruent to -1 modulo p.*

As a corollary to the proof method for this theorem we present examples of galois covers with group $(\mathbb{Z}/p\mathbb{Z})^2$ which cannot be lifted over any extension R of $W(k)$. Our second theorem (III, 1.3)is:

Theorem 2. *Let $f\colon C \longrightarrow C/G := D$ 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.*

We have used rigid methods to study this question and these also enable us to reprove the result from [O–S–S] in this context. In this respect the crucial study is that of the existence of liftings of G-galois covers of formal power series rings $k[\![z]\!]/k[\![z]\!]^G = k[\![t]\!]$ over k in G-galois covers of the formal power series rings $R[\![Z]\!]/R[\![Z]\!]^G = R[\![T]\!]$ over R. This is the condition which ensures smoothness of the lifting of curves. In contrast, the methods used by Oort, Sekeguchi and Suwa are global in the sense that they use generalized Jacobians. In our context the results we have proved give more information than those stated in Theorems 1 and 2 above, but rather than embarking on explanations now, we invite the reader to go straight to the paper for these.

Now we sketch how one uses rigid geometry to solve the lifting problem, under the assumption that the automorphisms of the formal power series rings over k can be lifted:

Suppose $f\colon C \longrightarrow D = C/G$ 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 $r\colon \mathcal{D}^{\mathrm{an}} \longrightarrow D$ 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

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

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 one can glue this cover to $\tilde{f}' : \mathcal{V}' \longrightarrow \mathcal{U}'$ along the morphisms induced on the annuli $\mathcal{U}' - \mathcal{U}$.

We remark that in his thesis, [G], Garuti has proved that for any G such a lifting of $k[\![z]\!]/k[\![z]\!]^G = k[\![t]\!]$ in $\mathcal{A}/\mathcal{A}^G = R[\![T]\!]$ is always possible for suitable R dominating $W(k)$, where $\mathcal{A}$ has generic fibre a suitable open 1-dimensional rigid analytic space of genus not necessarily 0. This gives rise to liftings $\mathcal{C}' \longrightarrow \mathcal{D} = \mathcal{C}'/G$ of galois covers $C' \longrightarrow D = C'/G$, where C' is birational to C, with only cusps as singularities, and generic fibre $\mathcal{C}'_\eta \longrightarrow \mathcal{D}_\eta$ is a G-cover of smooth curves.

Hence the question is if over the open disc $\operatorname{Spec} R[\![T]\!]$, we have "genus 0", more precisely open discs, and so we begin our investigation by studying the geometry of automorphisms of open discs.

Contrary to prime to p-order automorphisms, the geometry of order p automorphisms of the open disc $\operatorname{Spec} R[\![Z]\!]$, is far from understood. 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.

Our main contribution concerns higher p-exponent, one first needs a presentation of p^2-cyclic extensions from which one can easily read the degree of the different; this is done via Artin-Schreier-Witt Theory in Lemma 5.1, Section II. The first challenge is then to lift the equations as a p^2-cyclic cover of the open disc and this can be done using Sekiguchi and Suwa's recent work *"On the unified Kummer-Artin-Schreier-Witt theory"*, [S-S 1], but in order to cover the disc by discs we need to minimize the degree of the generic different; this is done after developing this theory in an effective way: namely we explicitly describe the map ψ_2 from [S-S-1], and finally we give 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 the geometry of automorphism of order p of the open disc we refer to our forthcoming paper, [G-M].

We would like to thank Tsutomu Sekiguchi and Noriyuki Suwa for communicating their work *On the unified Kummer-Artin-Schreier-Witt theory* to us. Their approach inspired our own work on p^2-cyclic liftings in Section II.

I. Local obstructions to the lifting

Let k be an algebraically closed field of characteristic p and $W(k)$ be its associated Witt-ring. The aim of this section is to give obstructions for a given group of automorphisms G of $k[\![z]\!]$ to be lifted to the formal power series ring $R[\![Z]\!]$, where R is any complete discrete valuation ring dominating $W(k)$. We shall use the notation $\tilde{R}$ to denote the unique valuation ring in the algebraic closure which dominates R.

We begin by collecting and proving those facts on automorphisms of finite order of the disc $\operatorname{Spec} R[\![Z]\!]$ and their fixed points, which we need in order to show obstructions to the lifting problem.

1. Geometry of the disc.

Recall that by using the Weierstrass Preparation Theorem [B1], chap. 7, p. 38, we can describe the geometry of the R-scheme $X := \operatorname{Spec} R[\![Z]\!]$. Namely, the special fibre, $X \times_R k$, has only one closed point which corresponds to the ideal $(\pi, Z)R[\![Z]\!]$, and the closed points of the generic fibre, $X \times_R K$, correspond to the irreducible distinguished polynomials of $R[\![Z]\!]$. These polynomials have roots in the maximal ideal of $\tilde{R}$. This allows us to identify $X \times_R K$ with the open disc $\{z \in \tilde{R} \mid |z| < 1\}$ modulo galois action.

2. Automorphisms of finite order with fixed points.

Let σ be an R-automorphism of $R[\![Z]\!]$ of finite order – we shall always work with R-automorphisms and so drop the reference to R. Then it 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 disc X, which we call $\tilde{\sigma}$. For rational points $(Z - Z_0) \in X$ 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, $P \in X$ is a fixed point if and only if $P = \pi R[\![Z]\!]$, $P = (0)$ or $P \supset (\sigma(Z) - Z)$. In the sequel we shall refer to this last set when we speak about fixed points. Moreover, we use the terminology geometric fixed points to describe the points they define in the geometric generic fibre.

2.1. Existence of fixed points. *Let σ be an automorphism of $R[[Z]]$ of finite order which doesn't induce the identity residually (i.e., the inertia group at π, I_π, is not the full group $\langle\sigma\rangle$). Then σ has at least one fixed point.*

Proof. Using the writing above, suppose first that $a_1 \equiv 1 \bmod \pi R$. Then since σ doesn't induce the identity residually, one knows that there is an a_i $(i > 1)$ which is a unit. Let m be the first $i > 1$ such that a_i is a unit. Then by the Weierstrass Preparation Theorem the series

$$\sigma(Z) - Z = f_m(Z)u(Z)$$

where $f_m(Z)$ is a distinguished polynomial of degree m and the series $u(Z)$ is a unit in $R[[Z]]$. It follows that the points of X which contain $f_m(Z)$ are the fixed points for σ. Finally if $a_1 \not\equiv 1 \bmod \pi R$, we repeat the above argument with $m = 1$. (Note that in this case σ has only one fixed point which is rational.)

We shall need the following lemmas:

Lemma 2.2. ([C] Lemma 14 p. 245) *Let $e \in \mathbb{N}^\times$ and $f(Z) \in R[[Z]]$, such that $f(Z) \equiv Z \bmod (Z^2)$ and defines an R-automorphism of $R[[Z]]$ of order e. Then $e = 1$.*

We shall also use a weak form of Lemma 15 from [C].

Lemma 2.3. *Consider the series $f(Z) = a_0 + a_1 Z + \cdots + a_n Z^n + \cdots \in R[[Z]]$, $a_0 \in \pi R$, and for $e \in \mathbb{N}^\times$ let $f^e(Z) = b_0 + b_1 Z + \cdots$. Then one has $b_0 \equiv a_0(1 + a_1 + \cdots + a_1^{(e-1)}) \bmod a_0^2 R$ and $b_1 \equiv a_1^e \bmod a_0 R$.*

Proof. By induction on e: Check that

$$\begin{aligned} f^{(e+1)}(Z) &= a_0 + a_1 f(Z) + \cdots \\ &= a_0 + a_1(b_0 + b_1 Z + \cdots) + a_2(b_0 + b_1 Z + \cdots)^2 + \cdots \\ &= a_0 + a_1 b_0 + a_2 b_0^2 + \cdots + Z(a_1 b_1 + 2a_2 b_0 b_1 + \cdots) + \cdots \end{aligned}$$

From this one deduces that $a_0 + a_1 b_0 + a_2 b_0^2 + \cdots \equiv a_0 + a_1 b_0 \bmod a_0^2 R$, and $a_1 b_1 + 2a_2 b_0 b_1 + \cdots \equiv a_1 b_1 \bmod a_0 R$.

Corollary 2.4. *If σ is an automorphism of $R[[Z]]$ of order e, with $(e,p) = 1$, then σ has a rational fixed point.*

Proof. Suppose $a_0 \neq 0$, $\sigma(Z) = a_0 + a_1 Z + \cdots$ and that $\sigma^e(Z) = b_0 + b_1 Z + \cdots = Z$. Then by the Lemma above $1 + a_1 + \cdots + a_1^{(e-1)} \equiv 0 \bmod a_0 R$. Hence as $e \not\equiv 0 \bmod p$, it follows that $a_1 \not\equiv 1 \bmod \pi R$. Therefore the automorphism σ

doesn't induce the identity residually, and hence by 2.1 must have a rational fixed point.

Remark. The analysis in Coleman [C], section 5, is more precise: namely he proves that there are no automorphism of order p over $R = W(k)$, for $p > 3$.

2.5. Linearization. *Let e be an integer prime to p and $f(Z) \in R[\![Z]\!]$ a power series with $f(Z) \equiv sZ \bmod (Z^2)$, which defines an R-automorphism of $R[\![Z]\!]$ of order e. Then there exists $Z' \in ZR[\![Z]\!]$ such that $f(Z') = sZ'$.*

Proof. Observe that as that the order of f is e then s is an e-th root of unity. Consider the Lagrange-Hilbert resolvant:

$$Z' = Z + s^{-1} f(Z) + s^{-2} f^2(Z) + \ldots + s^{-(e-1)} f^{e-1}(Z).$$

Then $f(Z') = sZ'$, and moreover $Z' \equiv eZ \bmod (Z^2)$, with e a unit in R as $(e,p) = 1$.

The following example shows that not every automorphism of finite order is linearizable.

Example. Let ζ be a primitive p-th root of unity and $\sigma(Z) = \zeta Z(1+Z)^{-1}$, then $\sigma^p(Z) = Z$ and 0, $\zeta - 1$ are the fixed points.

3. Comparison of the different.

Let σ be an automorphism of $R[\![Z]\!]$ of finite order n. We denote the inertia group at π in $\langle\sigma\rangle$ by I_π and assume that it is the identity group 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 (see Lemma 2.2).

Claim 3.1. *Let $T = Z\sigma(Z)\cdots\sigma^{n-1}(Z) = \epsilon Z^n(1+\cdots)$ where $\epsilon = (-1)^{(n-1)}$. Then $R[\![Z]\!]^{\langle\sigma\rangle} = R[\![T]\!]$.*

Proof. From [B1], 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.

Claim 3.2. *Let d_η, resp. d_s, be the degrees of the generic, resp. special differents for the extension $R[\![Z]\!]/R[\![T]\!]$. Then $d_\eta = d_s$.*

Proof. Let $f(X) = \prod_{0\le i<n} (X - \sigma^i(Z))$ 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

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

and so the result follows by the Weierstrass Preparation Theorem. We remark that the same equality for the different holds for towers of such cyclic extensions, see also 3.4.

Claim 3.3. *Let* F *be the set of geometric fixed points of* σ *and suppose* m *is the first integer such that the coefficient* a_m *in* $\sigma(Z)-Z=(\zeta-1)Z+\cdots+\zeta a_i Z^{i+1}+\cdots$ *is a unit. Then* $|F|=m+1$.

Proof. First note that by assumption $I_\pi = \mathbf{1}$, the identity group, so the integer m exists. If $\zeta \not\equiv 1 \bmod \pi$, then σ has a unique fixed point. Suppose $\zeta \equiv 1 \bmod \pi$ (i.e. n is a p-power). Then $m>0$, and the geometric fixed points are given by the zeros of the distinguished polynomial $f_m(Z)$ of $\sigma(Z)-Z$. Let Z_0 be such a zero, then the derivative at Z_0

$$\sigma'(Z_0)=1+f'_m(Z_0)u(Z_0)$$

is a primitive n-th root of unity ($\mathrm{o}(\sigma)=n$) and so $f'_m(Z_0)\neq 0$. Hence the roots are distinct, thus giving $m+1$ geometric fixed points. Observe that if $n=p$ this corroborates the previous fact $d_\eta = d_s$.

Remark. One checks that the integer m appearing in 3.3 is the conductor of the residual extension $k[\![z]\!]/k[\![z]\!]^{\langle\sigma\rangle}=k[\![t]\!]$.

It is known that claim 3.2 has a converse in the germ of curves context which follows from a formula given by Kato [K], section 5. Namely, given a finite morphism of strict henselizations of local rings of R-curves at closed points one can express the difference between the degrees of the generic and special differents in terms of Milnor numbers at the closed point. As our context is that of completions of local rings, for the convenience of the reader we give an adapted proof in the special case we use.

3.4. 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* $B=R[\![Z]\!]$.

Proof. It follows from EGA IV, chapter 0, corollary to Proposition 17.3.4, that B is a free A-module say of rank r. Following [S], chapter III we consider $\det_A(B):=\bigwedge_A^r B$ and define

$$\mathrm{T}_{B/A}:\det_A(B)\otimes_A \det_A(B)\longrightarrow A \qquad (*)$$

to be the homomorphism induced by the symmetric bilinear form:

$$B \times B \longrightarrow A; \quad (x,y) \mapsto \mathrm{tr}_{B/A}(xy),$$

where $\mathrm{tr}_{B/A} : B \longrightarrow A$ is the trace map. Then $\mathrm{Im}\,\mathrm{T}_{B/A} = cA$ for some $c = \pi^n P(T)$ in A with $n \geq 0$ and $P(T)$ a distinguished polynomial. Tensoring $(*)$ by K we obtain

$$\mathrm{T}_{B_K/A_K} : \det_{A_K}(B_K) \otimes_{A_K} \det_{A_K}(B_K) \longrightarrow A_K.$$

It follows $d_\eta = \mathrm{Coker}\,\mathrm{T}_{B_K/A_K} = \deg P$. On the other hand setting $\mathrm{T}' = \pi^{-n}\mathrm{T}_{B/A}$, $\mathrm{mod}\,\pi$ this induces a homomorphism

$$\mathrm{T}'_0 : \det_{A_0}(B_0) \otimes_{A_0} \det_{A_0}(B_0) \longrightarrow A_0.$$

Moreover $\mathrm{Im}\,\mathrm{T}'_0 = (c/\pi^n)A_0 = t^{\deg P}A_0$ so $\dim_k \mathrm{Coker}\,\mathrm{T}'_0 = \deg P$.

Now consider $\tilde{\mathrm{T}}'_0$ to be the homomorphism defined as in $(*)$ from the extension $A_0 \subset \tilde{B}_0$:

$$\tilde{\mathrm{T}}'_0 : \det_{A_0}(\tilde{B}_0) \otimes_{A_0} \det_{A_0}(\tilde{B}_0) \longrightarrow A_0.$$

Then $\dim_k \mathrm{Coker}\,\tilde{\mathrm{T}}'_0 = d_s$ and it follows from [S], Chap. III, Proposition 5, that $\dim_k \mathrm{Coker}\, T'_0 = d_s + 2\delta_k(B)$. Collecting the previous equalities we obtain the desired equality.

If $d_\eta = d_s$, then $B_0 = \tilde{B}_0 = k[\![z]\!]$ and it follows from [B2], chapter 9, §2, No. 5, that $B = R[\![Z]\!]$.

4. Automorphisms of the disc without fixed points.

In this paragraph we want to show the reader that automorphisms of the open disc without fixed points appear quite naturally within the study of those which have a fixed point.

Let σ be an automorphism of $R[\![Z]\!]$ of finite order which has at least one rational fixed point in X. We are interested in the open discs in X with rational centre and radius in $|\tilde{R}|$ which are stabilized by σ.

If $(\mathrm{o}(\sigma), p) = 1$, such a disc necessarily contains the fixed point of σ by 2.4. So we shall concentrate on the case where $\mathrm{o}(\sigma) = p$ and has a rational fixed point, which we assume to be 0.

Let $a \in \pi R$, choose $r \in |\tilde{R}|$ and set $D(a, r^+) = \{z \in \tilde{R} \mid |z - a| < r\}$. There are two cases to look at; either the inertia group $I_\pi = \langle\sigma\rangle$, or $I_\pi = \mathbf{1}$.

a) Suppose that $I_\pi = \langle\sigma\rangle$. Then $\sigma(Z) = \zeta Z$, for ζ a primitive p-th root of unity. One checks that $D(a, r^+)$ is stabilized by σ iff $r > |(\zeta - 1)a|$, and moreover σ will have no fixed point iff $|a| > r$.

b) Next suppose $I_\pi = \mathbf{1}$. Then we have seen that $\sigma(Z) = \zeta Z(1+\cdots+a_m Z^m+\cdots)$ where ζ is a primitive p-th root of unity, $a_i \in \pi R$ for $i < m$, $a_m \in R^\times$ for some m, and further by Artin-Schreier theory $(m,p) = 1$. By the preparation theorem $\sigma(Z) - Z = f_m(Z)u(Z)$ where $f_m(Z)$ is a distinguished polynomial of degree $m+1$, and $u(Z)$ is a unit.

Let $F = (Z_i)_{1\le i\le m+1} \in \tilde{R}$ be the zeros of f_m. Then $D(a, r^+)$ is stabilized by σ iff $|\sigma(a) - a| = \prod_{Z_i \in F} |a - Z_i| < r$. Further σ has no fixed point in $D(a, r^+)$ iff $|a - Z_i| > r$ for all $Z_i \in F$. These last two conditions are satisfied as soon as r is smaller than but sufficiently close to $\min_i |a - Z_i|$.

For example if $\sigma(Z) = \zeta Z(1+Z)^{-1}$, then $F = \{0, \zeta - 1\}$ and the conditions above are:

$$\max\big(|\zeta - 1 - a|, |a|\big) > r > |a|.|\zeta - 1 - a|.$$

5. Obstructions to liftings of automorphisms. In this paragraph we shall give necessary conditions on the conductors of p-cyclic subextensions of abelian extensions $k[\![z]\!]$ of $k[\![t]\!]$, for the liftablity of automorphisms of $k[\![z]\!]$ to $R[\![Z]\!]$. In the sequel given a finite group G and a G-cover $k[\![z]\!]/k[\![z]\!]^G = k[\![t]\!]$, by a lifting of this cover over R we mean a G-cover $R[\![Z]\!]/R[\![Z]\!]^G = R[\![T]\!]$ such that specializing modulo πR one obtains $k[\![z]\!]/k[\![t]\!]$. We shall use the same notation for the automorhisms acting on $R[\![Z]\!]$ and those acting modulo πR on $k[\![z]\!]$.

Theorem 5.1. *Let G be an abelian group isomorphic to $\big(\mathbb{Z}/p\mathbb{Z}\big)^2$. Let G_i, $1 \le i \le p+1$, be the $p+1$ subgroups of order p. Assume that G is a group of automorphisms of $k[\![z]\!]$ and arrange the G_i in such a way that the extensions $k[\![z]\!]^{G_i}/k[\![z]\!]^G$ have conductors m_i, with $m_1 \le m_2 \le \ldots \le m_{p+1}$. Denote the conductor of the extension $k[\![z]\!]/k[\![z]\!]^{G_i}$ by m_i'. Then if there is a lifting of G to a group of automorphisms of $R[\![Z]\!]$ the following two cases can occur:*

1st Case: Suppose $m_1 < m_2$. Then $m_1 \equiv -1 \bmod p$, $m_1' = m_2 p - m_1(p-1)$, $m_i = m_2$, and $m_i' = m_1$, for $2 \le i \le p+1$.

2nd Case: Suppose $m_1 = m_2$. Then $m_i = m_1 \equiv -1 \bmod p$, and $m_i' = m_1$ for $1 \le i \le p+1$.

In each case the two covers $R[\![Z]\!]^{G_i}/R[\![Z]\!]^G$ for $i = 1,2.$ have $(p-1)\dfrac{m_1+1}{p}$ common geometric branch points. [1])

Conversely, if $m_1 \equiv -1 \bmod p$ and if one can lift $k[\![z]\!]^{G_i}/k[\![z]\!]^G$ for $i = 1,2$ in such a way that the corresponding covers have $(p-1)(m_1+1)/p$ common

[1]) Note that by geometric branch points we mean the set of points defined by the branch points in the geometric generic fibre.

geometric branch points, then the normalisation of the compositum of these two covers lifts $k[\![z]\!]/k[\![z]\!]^G$.

Proof. Let $G = \langle\sigma_1, \sigma_2\rangle$, with $\mathrm{o}(\sigma_i) = p$ and set $G_i = \langle\sigma_i\rangle$ for $i = 1, 2$. We let m'_i be the conductor of the extension $k[\![z]\!]/k[\![z]\!]^{G_i}$ and suppose that we can lift G as a group of automorphisms of $R[\![Z]\!]$. Then for each i, $m'_i + 1$ is the number of geometric branch points of $R[\![Z]\!]/R[\![Z]\!]^{G_i}$.

Setting $k[\![t]\!] := k[\![z]\!]^G$, for each i the extension $k(\!(z)\!)^{\langle\sigma_i\rangle}/k(\!(t)\!)$ is defined by an Artin-Schreier equation

$$x_i^p - x_i = f_i(\frac{1}{t}).$$

It is possible to choose t (and so x_i) such that

$$f_1(\frac{1}{t}) = \frac{1}{t^{m_1}}, \quad (m_1, p) = 1$$
$$f_2(\frac{1}{t}) = \frac{c_{m_2}}{t^{m_2}} + \frac{c_{m_2-1}}{t^{m_2-1}} + \cdots + \frac{c_1}{t}$$

where for $1 \le l \le m_2$, $c_l = 0$ if $p|l$, $(m_2, p) = 1$ and we assume $m_1 \le m_2$.

1st Case: Suppose $m_1 < m_2$. Then $m_1 \equiv -1 \bmod p$, $m'_1 = m_2p - m_1(p-1)$, and $m_i = m_2$, respectively $m'_i = m_1$, for $2 \le i \le p+1$.

We begin by expressing the conductor m'_1 of the extension $k(\!(z)\!)/k(\!(z)\!)^{G_1}$ in terms of m_1 and m_2. One has $k(\!(z)\!) = k(\!(z)\!)^{G_1}[x_2]$ and as $z_1 := x_1^{-1/m_1} \in k(\!(z)\!)^{G_1}$ is a uniformizing parameter

$$\frac{1}{t} = z_1^{-p}(1 - z_1^{m_1(p-1)})^{1/m_1}.$$

Therefore

$$\begin{aligned} x_2^p - x_2 &= \sum_{1\le i\le m_2} \frac{c_i}{z_1^{pi}} \big(1 - z_1^{m_1(p-1)}\big)^{i/m_1} \qquad \text{with } (i, p) = 1 \\ &= \sum_{1\le i\le m_2} \frac{c_i}{z_1^{pi}} - \sum_{1\le i\le m_2} c_i \frac{i}{m_1} \big(\frac{1}{z_1^{pi-m_1(p-1)}} + \text{smaller terms}\big). \end{aligned}$$

By assumption $m_1 < m_2$, so it follows that the final expression on the right is equivalent (after an Artin-Schreier translation) to $\dfrac{a}{z_1^{pm_2-m_1(p-1)}}$ + smaller terms. Hence we obtain $m'_1 = pm_2 - (p-1)m_1$.

Let d be the number of common geometric branch points in $R[\![Z]\!]^{G_i}/R[\![Z]\!]^G = R[\![T]\!]$ for $i = 1, 2$. Now the degree of the generic different for $R[\![Z]\!]/R[\![Z]\!]^{G_1}$ is $(m_2 + 1 - d)(p-1)p$ (the points of $R[\![Z]\!]^{G_1}$ corresponding to the d set are completely decomposed.) It follows from the equality of the degrees of the generic and special differents (Claim 3.2) that

$$(m_2 + 1 - d)(p-1)p = (m'_1 + 1)(p-1).$$

This together with the identity for m_1' gives

$$(p-1)(m_1+1) = pd, \quad \text{i.e. } m_1 \equiv -1 \bmod p.$$

Now we remark that the p-cyclic extensions of $k((z))^G$ inside $k((z))$ are generated by the elements $w_1x_1 + w_2x_2$, for $(w_1, w_2) \in \mathbb{F}_p^2 \setminus \{(0,0)\}$. Moreover, one can choose an Artin-Schreier generator, say x_2 or $x_1 + w_2x_2$ for each $w_2 \in \mathbb{F}_p$. As

$$(x_1 + w_2x_2)^p - (x_1 + w_2x_2) = \frac{1}{t^{m_1}} + w_2 \sum_{1 \le i \le m_2} \frac{c_i}{t^i},$$

it follows that the set of conductors of these $p+1$ cyclic extensions is

$$m_1,\, m_2,\, m_2, \ldots, m_2$$

provided $m_1 < m_2$.

The degree of the different of the extension $k((z))/k((z))^G$ is

$$\begin{aligned} d_s &= (m_1+1)(p-1)p + (m_1'+1)(p-1) \\ &= (m_i+1)(p-1)p + (m_i'+1)(p-1) \quad \text{for } i = 2, \ldots, p+1. \end{aligned}$$

Since $m_1' = pm_2 - (p-1)m_1$ and $m_i = m_2$, $i = 2, \ldots, p+1$, it follows $m_i' = m_1$. This finishes the proof of the first case.

2nd Case: Suppose $m_1 = m_2$. Then $m_i = m_1 \equiv -1 \bmod p$, and $m_i' = m_1$ for $1 \le i \le p+1$.

We first observe that in this case $m_1 = m_i$ for all $1 = 2, \ldots, p+1$, for otherwise we can argue as in case 1, so obtaining $m_2 \neq m_1$. To simplify the notation we set $m = m_i$ for all i. The equations for the extensions admit the writing

$$\begin{aligned} x_1^p - x_1 &= \frac{1}{t^m} \\ x_2^p - x_2 &= \frac{u^p}{t^m} + \frac{a}{t^l} + \cdots \end{aligned}$$

where $u, a \in k$, $l < m$ and $(l,p) = 1$. First observe that u^p is distinct from u, for otherwise a $\mathbb{F}_p$-linear combination of x_1 and x_2 would generate a p-cyclic sub-extension of $k((z))$ over $k((t))$ having conductor strictly less than m. This contradicts the observation at the beginning of this case. Setting $z_1 = x_1^{-1/m}$, the first equation gives $t^{-1} = z_1^{-p}(1 - z_1^{m(p-1)})^{1/m}$. The second equation becomes

$$x_2^p - x_2 = u^p(z_1^{-mp} - z_1^{-m}) + \frac{a}{z_1^{lp}}(1 - \frac{l}{m} z_1^{m(p-1)} + \cdots) + \cdots$$

where the dots indicate terms having increasing z_1 powers. By making the usual Artin-Schreier translation the right side of the equation above becomes

$$\frac{u-u^p}{z_1^m}+\frac{a}{z^l}-\frac{al}{m}z_1^{m(p-1)-lp}+\cdots.$$

Observe that $m(p-1)-lp>-l>-m$, so the conductor m_1' is m. Thus $m_i=m_i'=m$ for $i=1,\ldots,p+1$.

Comparing the degrees of the generic and special differents for the covers $R[\![Z]\!]^{G_i}/R[\![T]\!]$ and $k[\![z]\!]^{G_i}/k[\![t]\!]$ we obtain

$$d_\eta=(m+1-d)(p-1)p=(m+1)(p-1)=d_s,$$

where d is the number of common geometric branch points in $R[\![Z]\!]^{G_i}/R[\![T]\!]$ for 2 different values of i. It follows that

$$(p-1)(m+1)=dp,\quad \text{i.e. } m\equiv -1 \bmod p.$$

This finishes the second case, and also shows that for both cases the number of common geometric branch points in $R[\![Z]\!]^{G_i}/R[\![T]\!]$, for $i=1,2$, is $d=(p-1)(m_1+1)/p$.

For the converse, suppose $m_1\equiv -1 \bmod p$ and that one can lift $k[\![z]\!]^{G_i}/k[\![z]\!]^G$ to G/G_i-covers $R[\![Z_i]\!]/R[\![T]\!]$ for $i=1,2$ in such a way that these have $(p-1)(m_1+1)/p$ common geometric branch points. We examine the normalisation of their compositum. The degree of the generic different of the normalisation of the compositum $\big(R[\![Z_1]\!]\otimes_R R[\![Z_2]\!]\big)\tilde{}$ is

$$d_\eta=(m_1+m_2+2-(p-1)\frac{m_1+1}{p})(p-1)p.$$

The specialisation of the compositum generically gives the cover $k[\![z]\!]/k[\![z]\!]^G$ whose degree of different is

$$d_s=(m_1+1)(p-1)p+(m_1'+1)(p-1).$$

The direct part of the theorem shows that $m_1'=pm_2-(p-1)m_1$ in both cases so $d_\eta=d_s$, therefore applying criterion 3.4 from this section, we conclude that $\big(R[\![Z_1]\!]\otimes_R R[\![Z_2]\!]\big)\tilde{}\simeq R[\![Z]\!]$, $R[\![Z]\!]^{G_i}\simeq R[\![Z_i]\!]$, $R[\![Z]\!]^G\simeq R[\![T]\!]$ and the cover $R[\![Z]\!]/R[\![Z]\!]^G$ lifts $k[\![z]\!]/k[\![z]\!]^G$.

Examples. Below we give two examples of covers with group $\big(\mathbb{Z}/p\mathbb{Z}\big)^2$ where the theorem above is applied. The first is an example of a cover with group $\big(\mathbb{Z}/2\mathbb{Z}\big)^2$ for which the conditions of the theorem are satisfied and one is able to lift the cover. The second is for a cover which cannot be lifted over any R dominating $W(k)$.

5.2. Suppose $\mathrm{char}(k) = 2$ and set $G = \left(\mathbb{Z}/2\mathbb{Z}\right)^2$. Let $u \in k$ with $u^2 \neq u$ and consider the covers of $k(\!(t)\!)$ defined by

$$x_1^2 - x_1 = \frac{1}{t} \quad \text{and} \quad x_2^2 - x_2 = \frac{u^2}{t}.$$

These covers are lifted to covers over $R = W(k)$ by the equations:

$$\frac{(-2X_1+1)^2-1}{4} = \frac{1}{T} \quad \text{and} \quad \frac{(-2X_2+1)^2-1}{4} = \frac{U^2}{T}$$

where $U \in R$ lifts u. The equation for the compositum of these two covers is $X_2^2 - X_2 = U^2(X_1^2 - X_1)$ and setting $Z := X_2 - UX_1$, this becomes

$$Z^2 + (2UX_1 - 1)Z = (U - U^2)X_1. \tag{$*$}$$

Remark that $\mathrm{Fr}(R[T, X_1, Z]) = \mathrm{Fr}(R[Z]) = K(Z)$, i.e., the projective line $\mathbb{P}^1_K$.
From the equation $X_1^2 - X_1 = \dfrac{1}{T}$ we see that

$$|T| < 1 \iff |X_1| > 1$$

and from $(*)$ that

$$|X_1| \leq 1 \ \Rightarrow\ |Z| \leq 1$$

Now assume $|X_1| > 1$ and $|Z| \leq 1$, then $|X_1| = |Z^2 - Z + 2UX_1Z|$ and so $|X_1| = |2UX_1Z|$, i.e. $|Z| = \dfrac{1}{|2U|}$ which is a contradiction. Hence

$$|T| < 1 \iff |Z| > 1.$$

The group G is realized as the group of automorphisms of the disc $|Z| > 1$, i.e., of $R[\![Z^{-1}]\!]$, by

$$\sigma_1(Z) = (4 - U)\frac{Z + U}{2Z - 1 + U}$$
$$\sigma_2(Z) = (1 - U)\frac{Z - 1}{2Z - 1 + U}.$$

One checks that each of these automorphisms has order 2. Notice that this cover gives rise to a global G-lifting over $\mathbb{P}^1_R$.

5.3. Consider the covers of $k(\!(t)\!)$ defined by the equations

$$x_1^p - x_1 = \frac{1}{t^{m_1}}, \quad \text{with } m_1 \not\equiv 0, -1 \bmod p$$

and

$$x_2^p - x_2 = \frac{c_{m_2}}{t^{m_2}} + \cdots + \frac{c_1}{t}, \quad \text{with } (m_2, p) = 1,$$

$c_{m_2} \neq 0$ and $c_{m_2} \notin \mathbb{F}_p$ if $m_1 = m_2$. Then if $m_2 \geq m_1$ the compositum of these covers cannot be lifted over any R dominating $W(k)$. Note, we need the condition $c_{m_2} \notin \mathbb{F}_p$ if $m_1 = m_2$ to ensure that no other subextension of $k((t))$ in the compositum has smaller conductor than m_1. We know that $x_1 + wx_2$, $w \in \mathbb{F}_p$, are Artin-Schreier generators for these extensions and now the above condition guarantees there is no cancellation which would give smaller conductor.

5.4. Observation. Suppose we can lift a G-cover $k[\![z]\!]/k[\![z]\!]^G$ to a G-cover $R[\![Z]\!]/R[\![Z]\!]^G$ with $G = \big(\mathbb{Z}/p\mathbb{Z}\big)^2 \times \mathbb{Z}/\ell\mathbb{Z}$ and $(p, \ell) = 1$. We first assume that ℓ is prime. Then considering the subgroup $\big(\mathbb{Z}/p\mathbb{Z}\big)^2 \subset G$ and the corresponding p-cyclic subcovers on the one side and the quotient group $G/\big(\mathbb{Z}/\ell\mathbb{Z}\big)$ and the corresponding p-cyclic subcovers on the other, one can apply the congruence identity of Theorem 5.1, namely "$m_1 \equiv -1 \bmod p$", to deduce that $\ell \equiv 1 \bmod p$. It follows for general ℓ that for any prime $q|\ell$, $q \equiv 1 \bmod p$.

The geometry of fixed points of automorphisms of order p of the open disc $\operatorname{Spec} R[\![Z]\!]$ and the constraint to realise the converse part of Theorem 5.1 leads us to the following:

5.5. Question. Assume $p \geq 2$; what are the abelian non-cyclic automorphism groups of $k[\![z]\!]$ that we can lift to automorphism groups of $R[\![Z]\!]$? For example, if $G = \big(\mathbb{Z}/p\mathbb{Z}\big)^2$ then there do exist such automorphism groups which can be lifted if $p = 2$ (see 5.2) and $p = 3$ (see [G-M]).

5.6. Local to Global Obstructions. In the literature the method used to show obstructions to smooth galois liftings of curves is of global nature, by using "Hurwitz" bounds for the number of automorphisms in characteristic 0. Now using the local obstruction we can give new families of covers which are not liftable.

Indeed, consider any finite p-group G which occurs as the galois group of an extension $k[\![z]\!]/k[\![t]\!]$ and cannot be lifted over R. From Harbater's theorem, [H] 2.7, see also [Ka] 2.1.4, one can extend this to a G-galois cover of the projective line for which G is the inertia group at ∞. The extension $k[\![z]\!]/k[\![t]\!]$ is that induced by the cover at ∞, and moreover the cover can be chosen étale outside ∞. Such covers cannot be lifted to characteristic 0.

If G is an abelian group, it is known that the bounds for the number of automorphisms obtained using the Hurwitz formula are the same in characteristic 0 and p, [N]. We remark that the equations of example 5.3 are those of a $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$ galois cover of $\mathbb{P}^1_k$ which cannot be lifted over any $R \supset W(k)$.

Now suppose $f\colon C \longrightarrow C/G := D$ is a G-galois cover of proper smooth curves over k. Let $y \in C$, $x = f(y)$ and suppose that the p-part of the corresponding inertia group, which we denote by I_p, is isomorphic to $\big(\mathbb{Z}/p\mathbb{Z}\big)^2$. Assume that it is possible to lift f as a G-galois cover $\mathcal{C}/\mathcal{D}$ of smooth R-curves, for some extension R of $W(k)$. Then, this lifting induces an I_p-galois cover $\hat{\mathcal{O}}_{\mathcal{C},y} \,/\, \hat{\mathcal{O}}^{I_p}_{\mathcal{C},y}$ which specializes to $\hat{\mathcal{O}}_{C,y} \,/\, \hat{\mathcal{O}}^{I_p}_{C,y} \bmod \pi R$ and so Theorem 5.1 implies that the minimal conductor of the p-cyclic subextensions of $\hat{\mathcal{O}}_{C,y} \,/\, \hat{\mathcal{O}}^{I_p}_{C,y}$ is congruent to -1 modulo p. We have proved Theorem 1 from the introduction, namely:

Theorem 5.7. *Let $f\colon C \longrightarrow C/G := D$ be a G-galois cover of proper smooth curves over k. Let $y \in C$, $x = f(y)$ and suppose that the p-part of corresponding inertia group, I_p, is isomorphic to $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$. Then a necessary condition for f to be lifted as a G-galois cover of smooth R-curves, for some extension R of $W(k)$, is that the minimal conductor of the p-cyclic extensions of $\hat{\mathcal{O}}^{I_p}_{C,y}$ in $\hat{\mathcal{O}}_{C,y}$, is congruent to -1 modulo p.*

6. Ramification in p^n-cyclic covers of the disc – the Hasse-Arf Theorem.

Let $k[\![z]\!]/k[\![t]\!]$ be a G-galois extension with $G = \langle\sigma\rangle$ cyclic of order p^n. Assume that G can be lifted as a G galois cover of the disc $X \longrightarrow X/G$. Let F_l be the geometric fixed points of σ^{p^l} and $N_l := |F_l|$, $0 \le l < n$. The p-cyclic cover $X/\langle\sigma^{p^{l+1}}\rangle \longrightarrow X/\langle\sigma^{p^l}\rangle$ is unramified over the image of $F_{l+1} - F_l$; this means that σ^{p^l} defines a partition of $F_{l+1} - F_l$ in orbits of length p, hence $p|(N_{l+1} - N_l)$. Note that the conductor for this p-cyclic extension is $N_l - 1$, so $N_l > 0$.

This congruence above is the classical Hasse-Arf congruences for p^n-cyclic covers (see [S], p. 84) and following Serre's notation one has $N_0 = 1 + i_0, \ldots, N_l = 1 + i_0 + pi_1 + \cdots + p^l i_l$. The fact that at each stage $N_{l+1} - N_l \ne 0$ (which gives the full Hasse-Arf Theorem) follows from the non-triviality of the conductors.

We remark that the method of thickening $\operatorname{Spec} k[\![z]\!]$ in $\operatorname{Spec} R[\![Z]\!]$ was recently successfully exploited by Lubin, [L], in order to give a new proof of Sen's Theorem on formal power series (this is an extension of Hasse-Arf congruences). In fact he only needs to lift the series $\overline{\sigma}(z) \in k[\![z]\!]$ in $\sigma(Z)$ such that $\sigma(Z) - Z$ has only simple zeros (but may have infinite order). For automorphism $\overline{\sigma}$ of finite order this is clearly a less stringent condition than what we intend to do, i.e., to lift in an automorphism σ of finite order.

II. Local lifting in the $p^a e$-cyclic case with $a \le 2$

In this section we begin by recalling certain results from Oort-Sekiguchi-Suwa, [O-S-S] and Sekiguchi-Suwa, [S-S 1]. In [O-S-S] the pe-cyclic case, $(e,p) = 1$, is studied and in [S-S 1] the generic p^n-cyclic case. Our aim here is to treat the local lifting of G galois $p^a e$-cyclic covers with $a \leq 2$. Here we follow the Sekiguchi-Suwa exposition from [S-S 1].

1. Kummer theory.

Let ℓ be an integer with $\ell \geq 2$ and K be a field containing μ_ℓ, the group of ℓ-th roots of unity ($\mathrm{char}(K) \not| \ell$). Let X a K-scheme, then one has the following exact sequence of sheaves of groups on the étale site on X (Kummer exact sequence):

$$1 \to \boldsymbol{\mu}_{\ell,K} \to \mathbb{G}_{m,K} \xrightarrow{\theta_\ell} \mathbb{G}_{m,K} \to 1 \qquad \theta_\ell : t \mapsto t^\ell \tag{1}$$

and a long exact cohomology sequence

$$\mathbb{G}_{m,K}(X) \to H^1(X_{et}, \boldsymbol{\mu}_{\ell,K}) \to H^1(X_{et}, \mathbb{G}_{m,K}) \to H^1(X_{et}, \mathbb{G}_{m,K}).$$

Here $H^1(X_{et}, \boldsymbol{\mu}_{\ell,K})$ is identified with the set the set of isomorphy classes of $\mathbb{Z}/\ell\mathbb{Z}$-torsors over X. Now let X be the spectrum of a local K-algebra B, then as $H^1(\mathrm{Spec}\, B, \mathbb{G}_{m,K}) = 0$ (Hilbert theorem 90) it follows that the map

$$\mathbb{G}_m(\mathrm{Spec}\, B) \to H^1(\mathrm{Spec}\, B, \boldsymbol{\mu}_\ell)$$

is surjective. This means that for any ℓ-cyclic étale extension C of B, there exists a morphism $f : \mathrm{Spec}\, B \to \mathbb{G}_{m,K}$ and $\mathrm{Spec}\, C$ is given by the fibre product:

$$\begin{array}{ccc} \mathrm{Spec}\, C & \longrightarrow & \mathbb{G}_{m,K} \\ \Big\downarrow & & \Big\downarrow{\scriptstyle \theta_\ell} \\ \mathrm{Spec}\, B & \longrightarrow & \mathbb{G}_{m,K} \end{array} \tag{2}$$

2. Artin-Schreier-Witt theory.

Let k be a field of characteristic $p > 0$ and $W_{n,k}$ be the Witt-group scheme of dimension n (the truncated Witt-vectors). Let X be a k-scheme. This time one has the following exact sequence (for the étale site):

$$W_{n,k}(X) \to H^1(X_{et}, \mathbb{Z}/p^n\mathbb{Z}) \to H^1(X_{et}, W_{n,k}) \to H^1(X_{et}, W_{n,k}) \tag{3}$$

In particular, if X is affine, then $H^1(X, W_{n,k}) = 0$. Therefore, we get the surjectivity of the map

$$W_{n,k}(X) \to H^1(X_{et}, \mathbb{Z}/p^n\mathbb{Z}).$$

We shall use the following facts: $W_{n,k}$ is the extension of $\mathbb{G}_{a,k}$ by $W_{n-1,k}$ and one has the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p^n\mathbb{Z} & \to & \mathbb{Z}/p^{n-1}\mathbb{Z} & \to & 0 \\ & & \cap & & \cap & & \cap & & \\ 0 & \to & \mathbb{G}_{a,k} & \to & W_{n,k} & \to & W_{n-1,k} & \to & 0 \end{array} \tag{4}$$

3. Sekiguchi-Suwa theory.

Assertion 1. ([S-S 1] Theorem 7.1.) There exists a smooth group scheme $\mathcal{W}_n$ over the discrete valuation ring $R := \mathbb{Z}_{(p)}[\mu_{p^n}]$, containing the constant group scheme $(\mathbb{Z}/p^n\mathbb{Z})_R$, such that the exact sequence

$$0 \to (\mathbb{Z}/p^n\mathbb{Z})_R \to \mathcal{W}_n \xrightarrow{\psi_n} \mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R \to 0 \tag{5}$$

has the Artin-Schreier-Witt exact sequence as special fibre and an exact sequence of Kummer type

$$1 \to \boldsymbol{\mu}_{p^n} \to \mathbb{G}_m^n \to \mathbb{G}_m^n \to 1$$

as the generic fibre. Moreover, for each n with $n \geq 2$, there exists a commutative diagram consisting of horizontal exact sequences

$$\begin{array}{ccccccccc} 0 & \to & (\mathbb{Z}/p\mathbb{Z})_R & \to & (\mathbb{Z}/p^n\mathbb{Z})_R & \to & (\mathbb{Z}/p^{n-1}\mathbb{Z})_R & \to & 0 \\ & & \cap & & \cap & & \cap & & \\ 0 & \to & \mathcal{W}_{1,R} & \to & \mathcal{W}_{n,R} & \to & \mathcal{W}_{n-1,R} & \to & 0 \end{array} \tag{6}$$

which gives a deformation of (4) to a commutative diagram consisting of exact sequences of multiplicative groups

$$\begin{array}{ccccccccc} 1 & \to & \boldsymbol{\mu}_p & \to & \boldsymbol{\mu}_{p^n} & \to & \boldsymbol{\mu}_{p^{n-1}} & \to & 1 \\ & & \cap & & \cap & & \cap & & \\ 1 & \to & \mathbb{G}_m & \to & (\mathbb{G}_m)^n & \to & (\mathbb{G}_m)^{n-1} & \to & 1 \end{array} \tag{7}$$

Now this exact sequence is universal for étale p^n-cyclic coverings of local rings dominating R. Namely one has the following:

Assertion 2. ([S-S 1], Theorem 3.8.) Let B be a local R-algebra which is flat over R. Then

$$H^1(\operatorname{Spec} B, \mathcal{W}_n) = 0$$

i.e. the canonical map

$$(\mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R)(B) \to H^1(\operatorname{Spec} B, (\boldsymbol{\mu}_{p^n})_R)$$

is surjective.

Moreover, if C is a flat local R-algebra which is an unramified p^n-cyclic covering of B then there exists an R-morphism

$$f : \operatorname{Spec} B \longrightarrow \mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R,$$

and the covering

$$\operatorname{Spec} C \longrightarrow \operatorname{Spec} B$$

is given by the fibre product:

$$\begin{array}{ccc} \operatorname{Spec} C & \longrightarrow & \mathcal{W}_n \\ \big\downarrow & & \big\downarrow{\scriptstyle \psi_n} \\ \operatorname{Spec} B & \xrightarrow{f} & \mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R \end{array}$$

We shall apply this last theorem to the case where $B = R[[T]]_{(\pi)}$ (here π is the uniformizing parameter of R); this solves the local lifting for p^n-cyclic groups generically. This lifting is therefore of the same nature as Garuti's, but in [G] the method is valid for general groups, (see the introduction).

In order to smoothen the singularities of [G], we need to give the map ψ_n below explicitly:

$$\psi_n : \mathcal{W}_n \longrightarrow \mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R.$$

We shall do this in the p^2-cyclic case, i.e. $n = 2$. Following [S-S 1], Theorem 7.1, one can take:

$$\mathcal{W}_2 = \operatorname{Spec} R[X_1, X_2, (\lambda X_1 + 1)^{-1}, (\lambda X_2 + F_1(X_1))^{-1}]$$

where

$$F_1(X_1) = 1 + \mu X_1 + \frac{1}{2!}\mu^2 X_1^2 + \cdots + \frac{1}{(p-1)!}\mu^{p-1}X_1^{p-1} =: \operatorname{Exp}_p(\mu X_1)$$

is the Artin-Hasse exponential truncated at degree p,

$$\mu = \pi - \pi^2/2 + \cdots + (-1)^p \pi^{p-1}/(p-1)$$

and $\pi = \zeta_{(2)} - 1$. Here $\zeta_{(2)}$ is a primitive p^2-th root of unity.

As explained in [S-S 1], proof of Theorem 8.4, the group scheme $\mathcal{V}_2 := \mathcal{W}_2/(\mathbb{Z}/p^2\mathbb{Z})_R$ is given by a polynomial $G_1(X_1)$ such that:

$$\mathcal{V}_2 = \operatorname{Spec} R[X_1, X_2, (\lambda^p X_1 + 1)^{-1}, (\lambda^p X_2 + G_1(X_1))^{-1}]$$

and G_1 satisfies the congruence equation:

$$G_1(\psi_1(X_1)) \equiv F_1(X_1)^p (\lambda X_1 + 1)^{-1} \bmod \lambda^p.$$

Here $\psi_1(X_1) = ((\lambda X_1 + 1)^p - 1)/\lambda^p$ and the isogeny ψ_2 is then

$\psi_2(X_1, X_2) = (\psi_1(X_1), X_2')$ with

$$X_2' = (1/\lambda^p)[(\lambda X_2 + F_1(X_1))^p - (\lambda X_1 + 1)G_1(\psi_1(X_1))](\lambda X_1 + 1)^{-1}.$$

In Lemma 5.2 we shall prove that for F_1 as above, the polynomial $G_1(Z) = \mathrm{Exp}_p(\mu^p Z)$ works and then

$$X_2' = (1/\lambda^p)[(\lambda X_2 + F_1(X_1))^p - (\lambda X_1 + 1)\mathrm{Exp}_p(\mu^p(\psi_1(X_1))](\lambda X_1 + 1)^{-1}.$$

4. Local lifting of p-cyclic covers.

Let $\zeta_{(1)}$ be a primitive p-th root of unity and set $\lambda := \zeta_{(1)} - 1$. Let R be a discrete valuation ring of characteristic 0, with uniformizing parameter π, and algebraically closed residue field k of characteristic p as before, and assume that $\zeta_{(1)} \in R$.

Theorem 4.1. [Compare [O–S–S], Theorem 2.2.] *The equation*

$$((\lambda X_1 + 1)^p - 1)/\lambda^p = T^{-m_1} \tag{$*$}$$

defines a p-cyclic cover $\mathcal{C}$ of $\mathbb{P}^1_R$ which after normalisation is étale outside the disc $|T| < 1$ (i.e., outside $\{x \in \mathbb{P}^1_K \mid |T(x)| < 1\}$). The special fiber is smooth and induces the extension of $k[\![t]\!]$ defined by the equation

$$x_1^p - x_1 = t^{-m_1} \tag{$**$}$$

In this way we cover all p-cyclic extensions of $k[\![t]\!]$. Moreover the set $\{a \in \mathcal{C}_\eta : |T(a)| < 1\}$ is an open disc and X_1^{-1/m_1} is a parameter.

Proof. By the criterion 3.4, section I, to prove the smoothness of the lifting over $\mathbb{P}^1_R$ determined by $(*)$, we must show that the degrees of generic and special differents are equal. From the Artin-Schreier equation $(**)$ it follows immediately that the special different is $d_s = (m_1 + 1)(p - 1)$.

The degree of the generic different of the extension of $R[\![T]\!]$ defined by $(*)$ is determined by the roots of $T^{m_1} + \lambda^p = 0$ and $T = 0$. Hence we obtain $d_\eta = (m_1 + 1)(p - 1) = d_s$. Note, the Artin-Schreier equations $(**)$ for $(p, m_1) = 1$ determine all p-cyclic extensions of $k(\!(t)\!)$.

It remains to show that X_1^{-1/m_1} is a parameter for the disc

$$\{a \in \mathcal{C}_\eta \,:\, |T(a)| < 1\}.$$

From the equation

$$X_1^p + \frac{p}{\lambda} X_1^{p-1} + \cdots + \frac{p}{\lambda^{p-1}} X_1 = T^{-m_1}$$

it follows that $\mathrm{supp}\,(X_1^{-1})_0 \subset \mathrm{supp}\,(T)_0$ and that X_1^{-1} is integral over $R[\![T]\!]$. As the cover $\mathcal{C}/\mathbb{P}^1_R$ is smooth, if $x \in \mathbb{P}^1_K$ corresponds to $T = 0$ and $\overline{x}$ its specialisation to $\left(\mathbb{P}^1_R\right)_k$, then $\widehat{\mathcal{O}}_{\mathbb{P}^1_R,\overline{x}} \simeq R[\![T]\!]$. This point is completely ramified in $\mathcal{C}$ and the disc above $\operatorname{Spec} R[\![T]\!]$ is of the form $\widehat{\mathcal{O}}_{\mathcal{C},\overline{y}} \simeq R[\![Z]\!]$ ($Z = 0$ at x), where residually $z = x_1^{-1/m_1}$ is a uniformizing parameter for $k(\!(t)\!)[x_1]$. We get $(X_1^{-1/m_1})_0 = (Z)_0$ and applying the Weierstrass Preparation Theorem we see that $X^{-1/m_1} = ZU$, for some unit in $R[\![Z]\!]$. This completes the proof.

5. Local lifting of p^2-cyclic covers.

In the following section we give explicit equations for p^2-cyclic extensions of $k(\!(t)\!)$ from which one can immediately read the different. We call them Artin-Schreier-Witt, representants of the extension and we use them to parametrize all p^2-cyclic covers of $k(\!(t)\!)$.

Lemma 5.1. *Let $a_j \in k$ and $p_{j,p-i} \in k[x]$, $0 \le j < m_1$, $0 < i < p$, polynomials of respective degrees $d_{j,p-i}$ and assume that $(m_1, p) = 1$. The equations*

$$x_1^p - x_1 = t^{-m_1}$$

and

$$x_2^p - x_2 = c(x_1^p, -x_1) + \sum_{0 \le s < m_1(p-1)} a_s t^{-s} + \sum_{0 \le j < m_1} t^{-jp} \sum_{0<i<p} (x_1^p - x_1)^i p_{j,p-i}(x_1^p - x_1)^p$$

define a p^2-cyclic extension of $k((t))$ whose degree of different is

$$(m_1 + 1)(p - 1)p + (m_2 + 1)(p - 1),$$

where

$$m_2 := \max_{\substack{0 \le j < m_1 \\ 0 < i < p}} \left(p^2 m_1, p(jp + (i + p d_{j,p-i}) m_1)\right) - (p-1)m_1$$

and $c(x, y) = ((x + y)^p - x^p + (-y)^p)/p$. Moreover, as the semigroup $p\mathbb{N} + m_1\mathbb{N}$ covers the integers greater than $(m_1 - 1)(p - 1)$, it follows that every p^2-cyclic extension of $k((t))$ has such a representation.

Proof. Because $(m_1, p) = 1$ it follows that $z := x_1^{-1/m_1}$ is a uniformizing parameter of $k((t))[x_1]$. We need to calculate the conductor of the extension $k((t))[x_1, x_2]/k((t))[x_1]$. One can easily express $1/t = z^{-p}(1 - z^{m_1(p-1)})^{-1/m_1}$ (up to a multiplicative constant), and then

$$c(x_1^p, -x_1) = -z^{-p^2 m_1 + (p-1)m_1} + \cdots$$

gives a bigger contribution in the z-valuation than any t^{-j}, $0 < j < m_1(p - 1)$. The other terms can be arranged as polynomials in t^{-1} and restricting our attention to the non p-powers, the term of highest degree in z^{-1} comes from only one polynomial

$$t^{-jp}(x_1^p - x_1)^i (p_{j,p-i}(x_1^p - x_1))^p.$$

After the standard transformation to eliminate p-powers, the non p-power of highest order in z^{-1} gives the conductor for the extension as claimed.

We need to justify that the expressions on the right of the second equation give Artin-Schreier-Witt representants for all p^2-cyclic extensions. This follows as writing in terms of t^{-1}, each monomial t^{-l}, with $l \geq m_1(p-1)$ and prime to p, does occur in expressions of the type given. The monomials occuring as p-powers can be removed by making a transformation to the variable x_2 for the extension, so give no new covers. This completes the proof of the lemma.

Remark. Note that $x_2 - \sum_{0\leq j<m_1} t^{-j} \sum_{0<i<p} (x_1)^i p_{j,p-i}(x_1^p - x_1)$ is an Artin-Schreier representant for the p-cyclic extension $k(\!(t)\!)[x_1, x_2]/k(\!(t)\!)[x_1]$.

Notations. In the sequel $\zeta_{(2)}$ is a primitive p^2-root of unity, $\pi := \zeta_{(2)} - 1$ is a uniformizing parameter in R and $\lambda := \zeta_{(2)}^p - 1$, a uniformizing parameter for the intermediate p-cyclic extension. Let $\mu = \mathrm{Log}_p(1+\pi)$, where for $F(X) \in R[\![X]\!]$ we denote the truncation by terms of degree bigger than $p-1$ by $F_p(X)$. The following congruence identities will be used several times in the lemmas that follow:

i) One has $\mu/\pi \equiv 1 \bmod \pi$, $p/\lambda^{p-1} \equiv -1 \bmod \pi$ and $\lambda/\mu^p \equiv 1 \bmod \pi$. Further from these we often use the identity $p\mu^p/\mu^{p^2} \equiv -1 \bmod \pi$.

ii) We shall also need the binomial congruence identity $\binom{p}{i} \equiv \frac{p(-1)^{i-1}}{i} \bmod p^2$ for $1 \leq i \leq p$.

In the lemmas below, Lemma 5.3 will be an amelioration of Lemma 5.2; this explains why in the proof of 5.2 we prove estimates which are better then necessary.

Lemma 5.2. *Let* $Y := ((\lambda X + 1)^p - 1)/\lambda^p$. *Then*

$$\mathrm{Exp}_p(\mu X)^p - (\lambda X + 1)\,\mathrm{Exp}_p(\mu^p Y) = 0 \bmod \pi^{p^2}.$$

Proof. The idea is to prove that the expression on the left of the congruence satisfies a linear differential equation of first order $\bmod p\mu^p$. This enables us to handle monomials of degree prime to p, and then a direct calculation handles the other monomials. One can easily see the non-triviality of estimates by looking at the coefficient of X which is $p\mu - \lambda - p\mu^p/\lambda^{p-1}$.

Sublemma. $h_1 := p\mu - \lambda - p\mu^p/\lambda^{p-1} \equiv 0 \bmod \pi^{p^2+1}$.

Proof. As $\binom{p}{i} \equiv \frac{p(-1)^{i-1}}{i} \bmod p^2$, $1 \leq i \leq p$, consequently

$$\lambda = (1+\pi)^p - 1 \equiv \pi^p + p\mu \bmod p^2.$$

Now

$$h_1 \equiv -\pi^p - p\mu^p/\lambda^{p-1} = -p/\lambda^{p-1}((\lambda^{p-1}/p)\pi^p + \mu^p) \bmod p^2.$$

From the identity $(\lambda+1)^p - 1 = 0$ it follows that

$$\lambda^{p-1}/p = -\sum_{1\le i\le p-1} \frac{\binom{p}{i}}{p}\,\lambda^{i-1} \equiv -\sum_{1\le i\le p-1} \frac{(-1)^{i-1}}{i}\,(\pi^p + p\mu)^{i-1} \bmod p\pi$$

and so

$$(\lambda^{p-1}/p)\pi^p \equiv \sum_{1\le i\le p-1} \frac{(-1)^i}{i}\,(\pi^p)^i \bmod p\pi^{p+1}.$$

Remarking that $\lambda^{p-1}/p \equiv -1 \bmod \pi$ we obtain

$$h_1 \equiv \sum_{1\le i\le p-1} \frac{(-1)^i}{i}\,(\pi^p)^i - \sum_{1\le i\le p-1} \Big(\frac{(-1)^i}{i}\,(\pi)^i\Big)^p \bmod p\pi^{p+1} \equiv 0 \bmod \pi^{p^2+1}.$$

Now we return to lemmas 5.2 and 5.3:

We define $f := \mathrm{Exp}_p(\mu X)^p$, $g := (\lambda X + 1)\mathrm{Exp}_p(\mu^p Y)$ and set

$$h := f - g = \sum_{1\le i\le p(p-1)+1} h_i X^i.$$

First claim: $f' = p\mu f + p\pi^p X^{p-1} \bmod p\pi^{p+1}$. This is left to the reader.

Second claim: $g' = p\mu g - \mu^{p^2}(X^p - X)^{p-1} \bmod p\pi^{p+1}$. This is a straightforward calculation using the previous sublemma.

Now we remark that if $C(X,Y) := ((X+Y)^p - X^p - Y^p)/p$ then

$$\begin{aligned} C(X^p, -X)' &= (X^p - X)^{p-1}(pX^{p-1} - 1) - pX^{p^2-1} + X^{p-1} \\ &\equiv -(X^p - X)^{p-1} + X^{p-1} \bmod p. \end{aligned}$$

From these observations it follows that

$$h' = p\mu h + p\pi^p C(X^p, -X)' \bmod p\pi^{p+1}, \qquad (*)$$

which here will only be used in the weak form:

$$ih_i = p\mu h_{i-1} + p\pi^p r_{i-1}, \quad r_{i-1} \in R. \qquad (**)$$

Using $(**)$ we first note that $v_p(i) \le 1$ for $i \le p(p-1)+1$; then an induction argument shows that $ih_i = 0 \bmod p\pi^p$, which is Lemma 5.2 for monomials of h of degree prime to p.

Now one can have a look at the other monomials. In fact there is no problem for them because one can easily locate them in f and g :

For those in $f - \sum_{0\le i\le p-1} ((\mu X)^i/i!)^p$:

To see them we remark that developing $(1+X_1+X_2+...X_{p-1})^p$, where the X_i are commuting indeterminates, gives a coefficient in $1^{i_0}X_1^{i_1}\dots X_{p-1}^{i_{p-1}}$ divisible by p iff this is not a p power (viewed $\bmod p$). Now inside one can replace X_i by $(\mu X)^i$; this shows that the coefficient of X^{jp} in

$$f - \sum_{0\le i\le p-1} ((\mu X)^i/i!)^p$$

is a multiple of $p\mu^{i_1+2i_2+\dots+(p-1)i_{p-1}} = p\mu^{jp}$.

For those in $g - \sum_{0\le i\le p-1} (\mu X)^{pi}/i!$:

One has to look at the coefficients of X^{pj} and X^{pj-1} in Y^i . An easy calculation shows that the coefficients of V^{pj} and V^{pj-1} in $((1+V)^p-1)^i$ are divisible at least by p^{i-j+1} for $i>j$. It follows that the coefficient of X^{pj} in

$$g - \sum_{0\le i\le p-1} (\mu X)^{pi}/i!$$

coming from $(\mu^p Y)^i/i!$ is divisible by $p^{i-j+1}\mu^{pi}\lambda^{pj}/\lambda^{pi}$. This shows that the contribution of $g - \sum_{0\le i\le p-1} (\mu X)^{pi}/i!$ is what we expect. Lemma 5.2 is proved.

Lemma 5.3. *One has*

$$\big(\mathrm{Exp}_p(\mu X)^p - (\lambda X+1)\,\mathrm{Exp}_p(\mu^p Y)\big)/(p\mu^p) \;\equiv\; C(X^p,-X) \bmod \pi,$$

where $C(X^p,-X) = \big((X^p-X)^p - (X^{p^2}-X^p)\big)/p$.

Proof. Consider the expression $H := h + \mu^{p^2}C(X^p,-X)$. Then $(*)$ shows that $H' \equiv p\mu h \bmod p\pi^{p+1}$. Now we remark that $C(X^p,-X)$ has no monomials which are p-powers. Hence the result follows as in lemma 2 if we can perform the estimates for p-powers in h .

Following the estimates in the preceding proof we note that the only p-power which can occur with a non-trivial coefficient $\bmod \pi^{p^2+1}$ is X^p.

We first work with f.

The idea is that this coefficient is “close” to that of $\mathrm{Exp}(p\mu X)$. In fact in this way you add only one contribution which is that of $(\mu X)^p/p!$ times powers of 1 ;

so this is $p(\mu X)^p/p!$. Hence the coefficient of X^p in f is $(p\mu)^p/p! - p\mu^p/p!$ and so the coefficient of X^p in $f - \sum_{0\le i<p} ((\mu X)^i/i!)^p$ is

$$(p\mu)^p/p! - p\mu^p/p! - \mu^p \equiv (-1/(p-1)! - 1)\mu^p \bmod \pi^{p^2+1}.$$

Now we work with g and compute the contribution of X^p in

$$g - \sum_{0\le i\le p-1} (\mu X)^{pi}/i! \;=\; (\lambda X + 1)\mathrm{Exp}_p(\mu^p Y) \;-\; \sum_{0\le i\le p-1} (\mu X)^{pi}/i!. \qquad (*)$$

By using the expansion

$$\mu^p Y = (\mu/\lambda)^p\big((\lambda X+1)^p - 1\big) = (\mu/\lambda)^p \sum_{1\le k\le p} \binom{p}{k} (\lambda X)^k$$

and the binomial congruence identity $\binom{p}{k} \equiv \dfrac{(-1)^{k-1}p}{k} \bmod p^2$, for $k \ne p$, we see that $\bmod \pi^{p^2+1}$ the coefficient of X^p in $\mathrm{Exp}_p(\mu^p Y)$ is that of X^p in

$$\sum_{1\le i\le p-1} \frac{\mu^{pi}}{i!\lambda^{pi}} \Big((\lambda X)^p \;+ \sum_{1\le k\le p-1} \frac{(-1)^{k-1}p}{k}(\lambda X)^k\Big)^i.$$

Now $\bmod \pi^{p^2+1}$ the coefficient of X^p in $\mathrm{Exp}_p(\mu^p Y) - \mu^p X^p$ is that of X^p in

$$\lambda^p \sum_{1\le i\le p-1} \frac{\mu^{pi}p^i}{i!\lambda^{pi}} \Big(\sum_{1\le k\le p-1} \frac{(-1)^{k-1}}{k} X^k\Big)^i.$$

This is the same as the coefficient of X^p in

$$\lambda^p \Big(\sum_{1\le i\le p-1} \frac{\mu^{pi}p^i}{i!\lambda^{pi}} \big(\mathrm{Log}(1+X)\big)^i \;-\; \frac{\mu^p p}{\lambda^p}\frac{(-1)^{p-1}}{p} X^p\Big).$$

Now this is the same as the coefficient of X^p in

$$\lambda^p \Big(\mathrm{Exp}\big(\frac{\mu^p p}{\lambda^p}\mathrm{Log}(1+X)\big) \;-\; \frac{\mu^p p}{\lambda^p}\frac{(-1)^{p-1}}{p} X^p \;-\; \frac{\mu^{p^2}}{p!\lambda^{p^2}} p^p X^p\Big). \qquad (**)$$

Observing that $\dfrac{\mu^p}{\lambda^p} p = \dfrac{\mu^p}{\lambda}\dfrac{p}{\lambda^{p-1}} \equiv -1 \bmod \pi$, and substituting in $(**)$, $\bmod \pi^{p^2+1}$ we obtain

$$\begin{aligned} &\lambda^p \Big(\mathrm{Exp}\big(-\mathrm{Log}(1+X)\big) \;+\; \frac{(-1)^{p-1}}{p} X^p \;-\; \frac{(-1)^p}{p!} X^p\Big) \\ &= \lambda^p \Big(\frac{1}{1+X} \;+\; \frac{(-1)^{p-1}}{p} X^p \;-\; \frac{(-1)^p}{p!} X^p\Big). \end{aligned}$$

Therefore the coefficient of X^p here is

$$\lambda^p(-1)^p(1-\frac{1}{p}-\frac{1}{p!}).$$

Finally in order to accommodate the contribution to the coefficient of X^p in $(1+\lambda X)\mathrm{Exp}_p(\mu^p Y) - \sum_{0\le i\le p-1}(\mu X)^{pi}/i!$ coming from the factor $(1+\lambda X)$, we compute the coefficient of $(\lambda X)^{p-1}$ in $\mathrm{Exp}_p(\mu Y)$. One checks, in the same way as before, that $\bmod \pi^{p^2+1}$ this is that of $\dfrac{1}{1+X}$, i.e. $(-1)^{p-1}$. In conclusion we deduce that $\bmod \pi^{p^2+1}$ the coefficient of X^p in $f-g$ is

$$\lambda^p(\frac{1}{p!}+\frac{1}{p})+(p\mu^p+\lambda^p)(1-\frac{1}{p}-\frac{1}{p!}-1)\equiv 0 \bmod \pi^{p^2+1},$$

finishing the proof of Lemma 5.3.

Remark: Lemma 5.4 below is a deformation of lemma 5.3 and will enable us to find all p^2-cyclic extensions residually.

Lemma 5.4. *Let $Y := ((\lambda X_1+1)^p-1)/\lambda^p = T^{-m_1}$ with $(p,m_1)=1$, and suppose $P_{j,i}(Y)\in R[Y]$, $0\le j<m_1$, $0<i<p$, are polynomials of degree $d_{j,i}$. We assume that the $P_{j,i}$ which are non-zero are primitive (i.e. have leading coefficient an R-unit). We write*

$$\mathrm{Exp}_p(\mu^p Y)\Big(1+\sum_{\substack{0\le j<m_1\\0<i<p}} T^{-j}\mu^i(p-1)!P_{j,i}(Y)\Big)^p \;=\; G(T^{-1})+\mu^{p^2}H(T^{-1}),$$

where G and H are polynomials in T^{-1} defined by

$$G(T^{-1}) := \mathrm{Exp}_p(\mu^p Y) + \sum_{\substack{0\le j<m_1\\(i_1,i_2)\in\mathcal{T}}} \frac{(\mu^p Y)^{i_1}}{i_1!}\big(\mu^{i_2}T^{-j}(p-i_2)!P_{j,i_2}(Y)\big)^p$$
$$+\Big(1+\sum_{\substack{0\le j<m_1\\0<i<p}} T^{-j}\mu^i(p-i)!P_{j,i}(Y)\Big)^p - 1 - \sum_{\substack{0\le j<m_1\\0<i<p}}\big(T^{-j}\mu^i(p-i)!P_{j,i}(Y)\big)^p$$

with $\mathcal{T}=\{(i_1,i_2)\,:\,0\le i_1<p,\ 0<i_2<p,\ i_1+i_2<p\}$, and

$$\mu^{p^2}H(T^{-1}) := \big(\mathrm{Exp}_p(\mu^p Y)-1\big)\Big(\big(1+\sum_{\substack{0\le j<m_1\\0<i<p}}T^{-j}\mu^i(p-i)!P_{j,i}(Y)\big)^p - 1$$
$$-\sum_{\substack{0\le j<m_1\\0<i<p}}\big(T^{-j}\mu^i(p-i)!P_{j,i}(Y)\big)^p\Big)$$
$$+\sum_{\substack{0\le j<p\\(i_1,i_2)\in\mathcal{S}}}\frac{(\mu^p Y)^{i_1}}{i_1!}\big(\mu^{i_2}T^{-j}(p-i_2)!P_{j,i_2}(Y)\big)^p$$

with $\mathcal{S} = \{(i_1, i_2) \,:\, 0 \le i_1 < p,\ 0 < i_2 < p,\ i_1 + i_2 \ge p\}$. *Let*

$$d := \max_{\substack{0 \le j < m_1 \\ 0 < i < p}} \big(jp + (i + pd_{j,p-i})m_1\big).$$

Then

$$\deg_{T^{-1}} G = \begin{cases} m_1(p-1) & \text{if all } P_{j,i} = 0 \\ d - m_1 & \text{otherwise} \end{cases}$$

and

$$\big[\mathrm{Exp}_p(\mu X_1)\big(1 + \sum_{\substack{0 \le j < m_1 \\ 0 < i < p}} T^{-j} \mu^i P_{j,i}(Y)\big)\big]^p - (1 + \lambda X_1) G(T^{-1}) = p\mu^p A,$$

where

$$A \equiv C(X_1^p, -X_1) - \sum_{\substack{0 \le j < m_1 \\ 0 < i < p}} T^{-jp} (X_1^p - X_1)^i P_{j,p-i}(X_1^p - X_1)^p \bmod \mu.$$

Proof. We first remark that Lemma 5.2 corresponds to the case where all $P_{j,i} = 0$.

Next, examining the terms in

$$\mathrm{Exp}_p(\mu^p Y)(1 + \sum_{\substack{0 \le j < m_1 \\ 0 < i < p}} T^{-j} \mu^i (p-i)! P_{j,i}(Y))^p$$

we remark that the “monomials”

$$(\mu^p Y)^i \big(\mu^{p-i} T^{-j} P_{j,p-i}(Y)\big)^p$$

are all of distinct degree in T^{-1} and the maximum degree attained is d. Suppose $d = j_0 p + (i_0 + pd_{j_0,p-i_0}) m_1$ for some $i_0 > 0$ and j_0. Then the "monomial"

$$(\mu^p Y)^{i_0 - 1} \big(\mu^{p-i_0} T^{j_0} P_{j_0,p-i_0}(Y)\big)^p$$

lies in $G(T^{-1})$ and gives the degree of $G(T^{-1})$, namely $d - m_1$. It is an exercise to see that the mixed terms in $G(T^{-1})$ don't contribute to the degree.

To prove the congruence identity, we deform lemma 5.3 by multiplying the congruence there by

$$(1 + \sum_{\substack{0 \le j < m_1 \\ 0 < i < p}} T^{-j} \mu^i (p-i)! P_{j,i}(Y))^p.$$

Doing this we obtain

$$\mathrm{Exp}_p(\mu X_1)^p (1 + \sum_{\substack{0 \le j < m_1 \\ 0 < i < p}} T^{-j} \mu^i (p-i)! P_{j,i}(Y))^p - (\lambda X_1 + 1)\big(G(T^{-1}) + \mu^{p^2} H(T^{-1})\big)$$
$$\equiv p\mu^p C(X_1^p, -X_1) \bmod \mu^{p^2+1}.$$

Simplifying this gives

$$\begin{aligned}&\mathrm{Exp}_p(\mu X_1)^p(1+\sum_{\substack{0\le j<m_1\\0<i<p}} T^{-j}\mu^i(p-i)!P_{j,i}(Y))^p-(\lambda X_1+1)G(T^{-1})\\&\equiv\ \mu^{p^2}(\lambda X_1+1)H(T^{-1})+p\mu^pC(X_1^p,-X_1)\bmod \mu^{p^2+1}.\end{aligned}$$

Dividing by $p\mu^p$ and using the identity $p\mu^p/\mu^{p^2}\equiv -1\bmod\mu$ we get

$$\begin{aligned}&\big(\mathrm{Exp}_p(\mu X_1)^p(1+\sum_{\substack{0\le j<m_1\\0<i<p}} T^{-j}\mu^i(p-i)!P_{j,i}(Y))^p-(\lambda X_1+1)G(T^{-1})\big)/(p\mu^p)\\&\equiv\ -H(T^{-1})+C(X_1^p,-X_1)\bmod\mu.\end{aligned}$$

Finally, examining the term of $H(T^{-1}) \mod\mu$ we obtain the desired residue of $A \bmod \mu$.

Theorem 5.5. *We keep the notations from the previous lemma and let* $A_s\in R$, $0<s<m_1(p-1):=r$ *be given. Then the equations*

$$((\lambda X_1+1)^p-1)/\lambda^p=T^{-m_1}$$

and

$$\begin{aligned}&\big[\lambda X_2+\mathrm{Exp}_p(\mu X_1)\big(1+\sum_{\substack{0\le j<m_1\\0<i<p}} T^{-j}\mu^i(p-i)!P_{j,i}(T^{-m_1})\big)\big]^p\\&=\big(G(T^{-1})+p\mu^p\sum_{0<s<r}A_sT^{-s}\big)(\lambda X_1+1)\end{aligned}$$

define a p^2*-cyclic cover,* $\mathcal{C}$, *of* $\mathbb{P}^1_R$ *which after normalisation is étale outside the disc* $|T|<1$. *The special fiber is smooth and induces the extension of* $k[\![t]\!]$ *defined by the equations*

$$\begin{aligned}x_1^p-x_1&=t^{-m_1}\\x_2^p-x_2&=c(x_1^p,-x_1)+\sum_{0<s<r}a_st^{-s}\\&\quad-\sum_{\substack{0\le j<m_1\\0<i<p}} t^{-jp}(x_1^p-x_1)^ip_{j,p-i}(x_1^p-x_1)^p\end{aligned}$$

where the polynomials $p_{j,p-i}$ *and coefficients* a_s *are the residues of* $P_{j,p-i}$ *and* A_s, *respectively. In this way we cover all* p^2 *-cyclic extensions of* $k[\![t]\!]$.

Proof. We know from 4.1 that $Z_1:=X_1^{-1/m_1}$ is a parameter for the open disc defined by the first equation. On the other hand by lemma 5.4 the T^{-1} polynomial

$$F(T^{-1})=G(T^{-1})+p\mu^p\sum_{0<s<r}A_sT^{-s}$$

has T^{-1}-degree $D := m_1(p-1)$ if all the $P_{i,j} = 0$ and $d - m_1$ otherwise. Now $T^D F(T^{-1}) \in R[T]$ is a primitive polynomial of degree D and we can expand it as a series in $R[\![Z_1]\!]$. Using the Weierstrass Preparation Theorem this series can be expressed as a distinguished polynomial $f_{pD}(Z_1)$ multiplied by a unit from $R[\![Z_1]\!]$. As $\deg_{Z_1} f_{pD} = pD$, it follows that f_{pD} has at most pD roots in the disc $|Z_1| < 1$. This consideration yields a bound for the degree of the generic different. Namely

$$d_\eta \leq (m_1+1)(p^2-1) + (p-1)pD.$$

From Lemma 5.1 it follows that $d_\eta \leq d_s$ and the Theorem now follows from the criterion 3.4, section I. Moreover Lemma 5.1 tells us that in this way we lift all p^2-cyclic extensions.

Corollary 5.6. *We keep the notations from the previous theorem. Let*

$$Y_2 := X_2 + \frac{1}{\lambda} \sum_{\substack{0 \leq j < p \\ (i_1,i_2) \in \mathcal{S}}} \frac{(\mu X_1)^{i_1}}{i_1!} \mu^{i_2} T^{-j} (p-i_2)! P_{j,i_2}(T^{-m_1}).$$

Let m_2 be as defined in Lemma 5.1. Then Y_2^{-1} is integral over $R[\![Z_1]\!]$, moreover Y_2^{-1/m_2} is a parameter for the open disc of $\mathcal{C}_\eta$ defined by $|Z_1| < 1$.

Proof. We shall examine the case where at least one of the $P_{i,j} \neq 0$, and remark that the other case works in the same way. First note that the transformation of the variable above is such that the residual image of Y_2 is an Artin-Schreier representant for the p-cyclic extension $k(\!(t)\!)[x_1,x_2]/k(\!(t)\!)[x_1]$. One has

$$\lambda X_2 + \mathrm{Exp}_p(\mu X_1)\big(1 + \sum_{\substack{0 \leq j < m_1 \\ 0 < i < p}} T^{-j} \mu^i (p-i)! P_{j,i}(T^{-m_1})\big) = \lambda Y_2 + A,$$

where

$$A := \mathrm{Exp}_p(\mu X_1) + \sum_{\substack{0 \leq j < p \\ (i_1,i_2) \in \mathcal{T}}} \frac{(\mu X_1)^{i_1}}{i_1!} \mu^{i_2} T^{-j} (p-i_2)! P_{j,i_2}(T^{-m_1}).$$

Then Y_2 satisfies the equation

$$Y_2^p + \frac{p}{\lambda} A Y_2^{p-1} + \cdots + \frac{p}{\lambda^{p-1}} A^{p-1} Y_2 = B \qquad (*)$$

where

$$B = \frac{1}{\lambda^p}\Big(-A^p + \big(G(T^{-1}) + p\mu^p \sum_{0<s<r} A_s T^{-s}\big)(1+\lambda X_1)\Big).$$

We know from 5.5 that $B \in R[\![Z_1]\!]_{(Z_1)}$, where $Z_1 = X_1^{-1/m_1}$. The way of truncating

$$\mathrm{Exp}_p(\mu X_1)\big(1 + \sum_{\substack{0 \leq j < m_1 \\ 0 < i < p}} T^{-j} \mu^i (p-i)! P_{j,i}(T^{-m_1})\big)$$

mimics that of truncating

$$\mathrm{Exp}_p(\mu^p Y)\Big(1+\sum_{\substack{0\le j<m_1\\0<i<p}} T^{-j}\mu^i(p-i)!P_{j,i}(Y)\Big)^p$$

in 5.4. It follows that

$$B=\frac{U}{Z_1^{p(d-m_1)+m_1}}$$

for some $U\in R[\![Z_1]\!]$ and as $m_2=p(d-m_1)+m_1$, also that $U\in R[\![Z_1]\!]^\times$.

Multiplying $(*)$ by $\dfrac{Z_1^{p(d-m_1)+m_1}}{Y_2^p}U^{-1}$ one gets an integral equation for Y_2^{-1} over $R[\![Z_1]\!]$. Since the defining equation of X_2 in 5.5 shows that $\mathrm{supp}\,(Y_2)_\infty\subset\mathrm{supp}(T)_0$, the result follows from the Weierstrass Preparation Theorem.

6. Local lifting of $p^a e$-cylic covers with $a\le 2$.

6.1. The $a=1$ case: Let $k[\![z]\!]/k[\![t]\!]$ be a pe-cyclic cover, $(e,p)=1$, and suppose σ is a generator. One can assume, after possibly changing the uniformizing parameter, that $k[\![z]\!]^{\langle\sigma^e\rangle}/k[\![t]\!]$ is defined by the equation $x_1^p-x_1=t^{-m_1}$ for some m_1 with $(p,m_1)=1$.

Let $\mathbb{P}^1_R=\mathrm{Proj}\,R[T_0,T_1]$, the projective line over R, which we assume contains the p-th roots of unity. We assume that t is a parameter of $\mathbb{P}^1_R\times k$ at $\infty=[0,1]$ and set $T=T_0/T_1$. Let $\mathcal{X}_0\longrightarrow\mathbb{P}^1_R$ be the morphism of smooth R-curves defined by the the equation $Z^e=T$. This morphism is ramified at $T=0$ and $T=\infty$.

Let $\mathcal{X}_1/R$ be the smooth R-curve obtained from theorem 4.1 and $\mathcal{X}_{1k}$ its special fibre, which is an étale cover of the affine line $t\neq 0$.

Claim: *The normalisation $(\mathcal{X}_0\times_R\mathcal{X}_1)\tilde{}$ is a smooth R-curve and the morphism $(\mathcal{X}_0\times_R\mathcal{X}_1)\tilde{}\longrightarrow\mathbb{P}^1_R$ is a $\mathbb{Z}/pe\mathbb{Z}$ cover which lifts $k[\![z]\!]/k[\![t]\!]$.*

Proof. We first remark that $\mathcal{X}_{0k}\times\mathcal{X}_{1k}$ is smooth outside the point ∞ as $\mathcal{X}_{1k}\longrightarrow\mathbb{P}^1_k$ is étale outside ∞. In order to see the smoothness over R above ∞ we shall apply the criterion 3.4 from section I.

Because $(p,e)=1$, the branch locus of $(\mathcal{X}_0\times_R\mathcal{X}_1)\tilde{}\longrightarrow\mathbb{P}^1_R$ consists of a point totally ramified (for $T=0$) and m_1e geometric points with ramification of order p. This yields the degree of the generic different above $|T|<1$:

$$d_\eta=pe-1+m_1e(p-1)$$

which is easily seen to be equal to that of the special different; this shows the smoothness of $(\mathcal{X}_0\times_R\mathcal{X}_1)\tilde{}$.

6.2. The $a = 2$ case: We use the same notation as above, but now R contains the p^2-roots of unity and $k[\![z]\!]^{\langle\sigma^e\rangle}/k[\![t]\!]$ is defined by the two equations

$$\begin{aligned} x_1^p - x_1 &= t^{-m_1} \\ x_2^p - x_2 &= c(x_1^p, -x_1) + f(t^{-1}). \end{aligned}$$

Theorem 5.5 gives a p-cyclic cover $\mathcal{X}_2/R$ of $\mathcal{X}_1/R$ which defines a p^2-cyclic cover of $\mathbb{P}^1_R$, lifts the extension $k[\![z]\!]^{\langle\sigma^e\rangle}/k[\![t]\!]$, and is totally ramified at $T = 0$. As previously one knows that $\mathcal{X}_{0k} \times_k \mathcal{X}_{2k}$ is smooth outside ∞. Now look more precisely at the branch locus for the p-cyclic cover

$$(\mathcal{X}_0 \times_R \mathcal{X}_2)\tilde{} \longrightarrow (\mathcal{X}_0 \times_R \mathcal{X}_1)\tilde{}$$

above $|T| \leq 1$. Now we are in the same situation as previously, so this relative generic different has degree equal to that of the special one; using the criterion we conclude the smoothness of $(\mathcal{X}_0 \times_R \mathcal{X}_2)\tilde{}$ and that $(\mathcal{X}_0 \times_R \mathcal{X}_2)\tilde{} \longrightarrow \mathbb{P}^1_R$ lifts the $p^2 e$-cyclic cover $k[\![z]\!]/k[\![t]\!]$.

III. Global lifting

The main ingredient of this section is a prolongation lemma which enables us to extend certain finite morphisms over an open annulus to the open disc. This result is adapted from a lemma in the unpublished manuscript, [M-Y].

1. Prolongations of automorphisms to the disc.

Let R denote a complete discrete valuation ring with fraction field K, uniformizing parameter π and residue field k of characteristic p. Let $\tilde{R}$ be its integral closure in the algebraic closure $\tilde{K}$ which is endowed with the unique prolongation of the valuation. Denote the completion of $\tilde{K}$ with respect to this valuation by L. Let $X := \operatorname{Spec} R[\![T]\!]$, the open disc and set $X_\varpi := \operatorname{Spec} R[\![T]\!]\langle\frac{\varpi}{T}\rangle$, for $\varpi \in \pi R$ where

$$R[\![T]\!]\langle\frac{\varpi}{T}\rangle = \{f = \sum_{n\geq 0} a_n T^n + \sum_{n>0} \frac{a_{-n}\varpi^n}{T^n} \mid a_i \in R \text{ and } a_{-n} \to 0\}.$$

We shall denote the image of such an f in $k[\![t]\!]$ by $\overline{f}$, where t denotes the reduction of T with respect to the Gauss valuation. Then the generic fibre of $\operatorname{Spec} R[\![T]\!]\langle\frac{\varpi}{T}\rangle$ identifies with the semi-open annulus $\{z \in \tilde{R} \mid |\varpi| \leq |z| < 1\}$ of thickness $|\varpi|$ modulo the Galois action.

Prolongation Lemma 1.1. *Let* $P(X) = X^n + A_{n-1}(T)X^{n-1} + \cdots + A_0(T) \in R[\![T]\!][X]$ *and* $Q(X) = X^n + A'_{n-1}(T, \frac{\varpi}{T})X^{n-1} + \cdots + A'_0(T, \frac{\varpi}{T}) \in R[\![T]\!]\langle\frac{\varpi}{T}\rangle[X]$, *such that* $\overline{P}(X) = \overline{Q}(X) \in k[\![t]\!][X]$ *are separable Eisenstein polynomials in* t. *Let* $Z \in \Omega$ *(*Ω *an algebraically closed field containing* $R[\![T]\!]$*) such that* $P(Z) = 0$. *Then*

1) $R[\![T]\!][Z] = R[\![Z]\!]$. *Moreover* $T = D(Z)u(Z)$ *where* $D(Z) \in R[Z]$ *is a distinguished polynomial of degree* n *and* $u(Z)$ *is a unit in* $R[\![Z]\!]$.

2) After a finite extension R'/R *and taking an annulus of smaller thickness* $|\varpi'|$, *the map* $Z \mapsto T(Z)$ *defines a finite morphism*

$$\operatorname{Spec} R'[\![Z]\!]\langle\frac{\omega}{Z}\rangle \longrightarrow \operatorname{Spec} R'[\![T]\!]\langle\frac{\varpi'}{T}\rangle$$

for some $\omega \in R'$ *with* $|\omega|^n = |\varpi'|$. *Moreover* Q *has a root* Z' *in* $R'[\![Z]\!]\langle\frac{\omega}{Z}\rangle$, *i.e. the morphisms defined by* P *and* Q *are isomorphic over the semi-open annulus* $|\varpi'| \leq |T| < 1$.

Proof. 1) One has $A_0(T) = (\alpha - T)u_0(T)$ for some $\alpha \in \pi R$ and $u_0(T)$ a unit in $R[\![T]\!]$, so after changing coordinates for the disc one can assume that $A_0(T) = -T$. Then

$$\begin{aligned} T &= Z^n + A_{n-1}(T)Z^{n-1} + \cdots + A_1(T)Z \\ &= Z^n + P_0(Z) + TZ\,H_0(T,Z) \end{aligned} \tag{$*$}$$

where $P_0(Z) = \sum_{i=1}^{n-1} A_i(0)Z^i \in \pi Z R[Z]$ and $H_0(T,Z) \in R[\![T]\!][Z]$. Iterating T in $(*)$ one expresses T as an element of $R[\![Z]\!]$, so $R[\![T]\!][Z] = R[\![Z]\!]$. One has the writing

$$T = \prod_{i=1}^{n} (Z - \alpha_i)\, u(Z),$$

with $\alpha_1 = 0$, $\alpha_i \in \tilde{R}$, $|\alpha_i| < 1$ and $u(Z) \in R[\![Z]\!]^\times$.

2) Let $\varpi' \in \tilde{R}$, $|\varpi'| < 1$, be chosen such that $|\varpi'| > \max_i |\alpha_i|^n$. Then for $z \in \tilde{R}$, $|z| < 1$,

$$|T(z)| = |\varpi'| \iff |z| = |\varpi'^{1/n}| = |\omega|$$

and so for some R' the injection $R'[\![T]\!] \hookrightarrow R'[\![Z]\!]$ induces a finite morphism

$$\operatorname{Spec} R'[\![Z]\!]\langle\frac{\omega}{Z}\rangle \longrightarrow \operatorname{Spec} R'[\![T]\!]\langle\frac{\varpi}{T}\rangle.$$

Now we can see $Q(X)$ as a polynomial in $A\langle\frac{\omega}{Z}\rangle[X]$, where $A := R'[\![Z]\!]$. For the rest of the proof we denote the X derivative of $Q(X)$ by $Q'(X)$. We want to show that if $|\varpi'|$ is sufficiently near to 1, then $Q(X)$ has a root $Z' \in A\langle\frac{\omega}{Z}\rangle$.

In order to prove this we use Newton's method, but must overcome some technical difficulty as $A\langle\frac{\omega}{Z}\rangle$ isn't a field and moreover is endowed with a norm $\|\,.\,\|$ (the spectral norm on $|\omega| \le |z| < 1$) which isn't multiplicative. As usual we build a sequence $Z_i \in A\langle\frac{\omega}{Z}\rangle$ such that

$$Z_{i+1} = Z_i - \frac{Q(Z_i)}{Q'(Z_i)}$$

and prove that it converges. First we shall work in the affinoid algebras $L\langle\frac{Z}{\rho}, \frac{\omega}{Z}\rangle$ for ρ near to 1, and take the limit as $\rho \to 1$.

We have

$$Q(Z) = Q(Z) - P(Z) = \sum_{0\le i<n} \big(A_i'(T, \frac{\varpi}{T}) - A_i(T)\big)Z^i,$$

hence $\|Q(Z)\| < 1$ by the hypothesis ($\overline{P} = \overline{Q}$ in $k[\![\overline{T}]\!][X]$); moreover $\overline{Q}'(\overline{Z}) \neq 0$, hence $\|Q'(Z)\| = 1$. Changing ω we can assume that $Q'(Z)$ has no zeros in the semi-open annulus $\{z \in \tilde{R} \,|\, |\omega| \le |z| < 1\}$. Hence $Q'(Z) \in L\langle\frac{Z}{\rho}, \frac{\omega}{Z}\rangle^{\times}$ and $\|\frac{Q(Z)}{Q'(Z)^2}\| < h < 1$ (with h independent of ρ).

Set $Z_1 = Z - \frac{Q(Z)}{Q'(Z)} \in L\langle\frac{Z}{\rho}, \frac{\omega}{Z}\rangle$, then using the Taylor expansion one has

$$Q(Z_1) = Q(Z) - \frac{Q(Z)}{Q'(Z)}Q'(Z) + \big(\frac{Q(Z)}{Q'(Z)}\big)^2 r(Z)$$

where $\|r(Z)\| \le 1$ (remark that $r(X) \in A\langle\omega/Z\rangle[X]$) and consequently $\|\frac{Q(Z_1)}{Q(Z)}\| \le h.$

Next we show that $Q'(Z_1) \in L\langle\frac{Z}{\rho}, \frac{\omega}{Z}\rangle^{\times}$.

One has $-Q'(Z) + Q'(Z_1) = (Z - Z_1)E$ for some $E \in L\langle\frac{Z}{\rho}, \frac{\omega}{Z}\rangle$, $\|E\| \le 1$. Therefore

$$\frac{Q'(Z_1)}{Q'(Z)} = 1 + \frac{Q(Z)}{Q'(Z)^2}E$$

is invertible and so $Q'(Z_1) \in L\langle\frac{Z}{\rho}, \frac{\omega}{Z}\rangle^{\times}$. Now $\|\frac{Q'(Z_1)}{Q'(Z)}\| = \|\frac{Q'(Z)}{Q'(Z_1)}\| = 1$ and $\|\frac{Q(Z_1)}{Q'(Z_1)^2}\| \le h\,\|\frac{Q(Z)}{Q'(Z_1)^2}\| \le h^2$. It follows $\|\frac{Q(Z_2)}{Q(Z_1)}\| \le h^2$.

Recurrently this process works in the same way and in the limit yields $Z' = \lim Z_i \in L\langle\frac{Z}{\rho}, \frac{\omega}{Z}\rangle$ independently of ρ, such that $Q(Z') = 0$. Moreover $\|Z'\| = \|Z\| = 1$ and so $Z' \in A\langle\frac{\omega}{Z}\rangle$.

Theorem 1.2. *Let* $\omega \in R$ *and* $\mathcal{A}_\omega := \{z \in \tilde{R} \mid |\omega| \leq |z| < 1\}$ *which modulo the galois action identifies with the generic fibre of* $\operatorname{Spec} R[\![Z]\!]\langle \frac{\omega}{Z} \rangle$. *Let* G *be a* $p^a e$*-cyclic group of automorphisms of* $\mathcal{A}_\omega$ *with* $a \leq 2$. *We assume that the inertia at* πR *is the identity. Then after enlarging* R *and diminishing the thickness,* G *can be extended to a group of automorphisms of the open disc* $\operatorname{Spec} R[\![Z']\!]$ *and* $\mathcal{A}_\omega$ *is identified with* $\{z' \in \tilde{R} \mid |\omega| \leq |z'| < 1\}$.

Proof. This is a consequence of the Prolongation Lemma and paragraph 6, Section II, where we lift automorphisms of $k[\![z']\!]$ of order $p^a e$ with $a \leq 2$ to automorphisms of $R[\![Z']\!]$.

The Global Lifting Theorem 1.3. *Let* $f : C \longrightarrow C/G := D$ *be a* G*-galois cover of proper smooth irreducible curves over* k. *Assume that the inertia groups are* $p^a e$*-cyclic with* $a \leq 2$. *Then* f *can be lifted over* $R = W(k)[\zeta_{(2)}]$ *as a* G*-cover of smooth* R*-curves.*

Proof. 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 $\mathcal{D}^{\text{an}}$ the generic fibre endowed with rigid analytic structure and let $r: \mathcal{D}^{\text{an}} \longrightarrow D$ be the reduction map. Let $U \subset D = C/G$ be the étale locus, and $\mathcal{U} \subset \mathcal{D}^{\text{an}}$, be the affinoid defined by $\mathcal{U} = r^{-1}(U)$. Then by Grothendieck, up to isomorphism one can lift in a unique diagram

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

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 discs in a G-galois way.

We write $D = U \amalg \operatorname{Branch} f$, where $\operatorname{Branch} f$ is the branch locus. For $x \in \operatorname{Branch} f$, choose $y \in f^{-1}(x)$ and let I_y be the inertia group at y. Let Γ be a representative system of $G \bmod I_y$, then $f^{-1}(x) = \amalg_{\gamma \in \Gamma}\{\gamma y\}$. The G-cover $\tilde{f}: \mathcal{V} \longrightarrow \mathcal{U}$ extends to a G-cover $\tilde{f}_{\pi'}: \mathcal{V}_{\pi'} \longrightarrow \mathcal{U}_{\pi'}$, where $\mathcal{U}_{\pi'} = \mathcal{U} \amalg \mathcal{A}_x$ and $\mathcal{A}_x := \{z \in r^{-1}(x) \mid |\pi'| \leq |z| < 1\}$. Moreover the germ of prolongation is unique up to isomorphism, see [Ra], Proposition 3.4.1. Let

$$\tilde{f}_y: \mathcal{A}_y \longrightarrow \mathcal{A}_x$$

be the corresponding I_y-cover for the $y \in f^{-1}(x)$, then using Lemma 1.1 again we observe that deminishing the thickness of $\mathcal{A}_x$ it follows that $\mathcal{A}_y$ is a semi-open annulus; so the conditions of Theorem 1.2 are satisfied. Following Raynaud, [Ra] 4.1, one can define the G-cover obtained from $\mathcal{A}_y$ via induction from I_y to G. Then

$$\tilde{f}_{\pi'}(\mathcal{A}_x) \simeq \operatorname{Ind}_{I_y}^{G} \mathcal{A}_y.$$

Now one can apply the previous theorem in order to extend $\tilde{f}_y$ to an I_y-morphism of open discs:

$$\begin{array}{ccc} B_y & \longrightarrow & B_x \\ \uparrow & & \uparrow \\ \mathcal{A}_y & \longrightarrow & \mathcal{A}_x \end{array}$$

We can then glue the morphism $\mathrm{Ind}_{I_y}^G B_y \longrightarrow B_x$ to $\tilde{f}_{\pi'}$ along $\tilde{f}_y$ for each $x \in \mathrm{Branch}\, f$. This gives a lifting of f as an analytic cover of $\mathcal{D}^{\mathrm{an}}$, which via rigid GAGA can be algebraized to a G-cover of smooth R-curves lifting f.

IV. References

[B1] N. Bourbaki *Algèbre Commutative*, Hermann, Paris 1961.

[B2] N. Bourbaki *Algèbre Commutative*, Chapitres 8 et 9, Masson, Paris 1983.

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

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

[G-M] B. Green, M. Matignon, *Order p automorphisms of the open disc over a p-adic field*, In preparation, 1996.

[H] D. Harbater, *Moduli of p-covers of curves*, Comm. in Algebra, 8, n° 12 (1980), 1095–1122.

[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.

[Ka] N. Katz, *Local-to-Global Extensions of Representations of Fundamental Groups*, Ann. Inst. Fourier, Grenoble 36 (1986), 69–106.

[L] J. Lubin, *Sen's theorem on iteration of power series*, Proc. AMS 123, 1 (1995), 63–66.

[M-Y] M. Matignon, T. Youssefi, *Prolongement de morphismes de fibres formelles et cycles evanescents*, Prepint, April 1992.

[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., 4e série, t. 22 (1989), 345–375.

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

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

[S-S 1] T. Sekiguchi, N. Suwa, *On the unified Kummer-Artin-Schreier-Witt theory*, (Preprint series), CHUO MATH NO.41, (1994).

[S-S 2] T. Sekiguchi, N. Suwa *Théories de Kummer-Artin-Schreier-Witt*, C. R. Acad. Sci. Paris, t. 319, Série I (1994), 105–110.

[S] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

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