Parametrizing Cyclic Automorphisms of Power Series Rings

Dirk Basson

Thesis presented for the degree of Master of Science at
Stellenbosch University

Supervisor: Professor B.W. Green

December 2010

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the owner of the copyright thereof (unless to the extent explicitly otherwise stated) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: November 19, 2010

Abstract

In the work of Green and Matignon it was shown that the Oort-Sekiguchi conjecture is equivalent to a local question of lifting automorphisms of power series rings. The Oort-Sekiguchi conjecture asks when an algebraic curve in characteristic p can be lifted to a relative curve in characteristic 0, while keeping the same automorphism group. The local formulation asks when an automorphism of a power series ring over a field k of characteristic p can be lifted to an automorphism of a power series ring over a discrete valuation ring with residue field k of the same order as the original automorphism.

This thesis looks at the local formulation and surveys many of the results for this case. At the end it presents a new theorem giving a Hensel's Lemma type sufficient condition under which lifting is possible.

Opsomming

Green en Matignon het bewys dat die Oort-Sekiguchi vermoede ekwivalent is aan ‘n lokale vraag oor of outomorfismes van magsreeksringe gelig kan word. Die Oort-Sekiguchi vermoede vra of ‘n algebraïese kromme in karakteristiek p gelig kan word na ‘n relatiewe kromme in karakteristiek 0, terwyl dit dieselfde outomorfisme groep behou. Die lokale vraag vra wanneer ‘n outomorfisme van ‘n magsreeksring oor ‘n liggaam k van karakteristiek p gelig kan word na ‘n outomorfisme van ‘n magsreeksring oor ‘n diskrete waarderingsring met residuliggaam k, terwyl dit dieselfde orde behou as die aanvanklike outomorfisme.

Hierdie tesis fokus op die lokale vraag en bied ‘n opsomming van baie bekende resultate vir hierdie geval. Aan die einde word ‘n nuwe stelling aangebied wat voorwaardes stel waaronder hierdie vraag positief beantwoord kan word.

Acknowledgements

Firstly I would like to thank the members of staff of the Mathematics division of the Department Mathematical Sciences at Stellenbosch University for their support and friendly company. In particular, I wish to mention the following:

- Professor Breuer and Doctor Keet, the Number Theory Seminar group, who played a large part in my growth in this area;
- Doctors Bartlett and Janelidze, who organized the post-graduate activities which were a lot of fun and helped in my development as a mathematician;
- Professor Green, my supervisor, for all his time, patience and support throughout the period 2009-2010.

Then I wish to thank the Wilhelm Frank Scholarship Fund for financial support during 2009 and 2010. It was an indespensible part of my studies.

Dankie aan my ouers vir alles wat hulle sover vir my gedoen het. Dankie vir al die ondersteuning en geleenthede wat aan my gebied is. Dankie ook aan my verloofde, Remerta, vir alles wat sy doen om my lewe beter te maak en my deur hierdie tydperk te help.

Contents

Conventions

We make the following conventions throughout the text, except when explicitly required otherwise.

- A – commutative ring with unity
- R – discrete valuation ring of mixed characteristic
- K – quotient field of R
- π – uniformizing parameter for R
- K^{alg} – algebraic closure of K
- R^{alg} – integral closure of R in K^{alg}
- $\tilde{\pi}$ – the maximal ideal of R^{alg} (not principal)
- k – residue field of R
- $W(k)$ – the ring of Witt vectors of k
- p – the characteristic of k
- $A[\![X]\!]$ – ring of formal power series over A generated by X
- D – the p-adic open unit disc $\mathrm{Spec}(R[\![Z]\!])$
- $\mathbb{Z}_p$ – the ring of p-adic integers

- When there is referred to "characteristic p", $p > 0$ is meant. For characteristic 0 we shall use "characteristic 0". In the one instance where we wish to keep the possibility to have both, we write $\mathrm{char}(k)$.

In this thesis we shall often start with an algebraically closed field k of characteristic p, and let R be some discrete valuation ring, dominating the Witt vectors $W(k)$. Usually, R will be finite over $W(k)$, obtained by adjoining a p^n-th root of unity $\zeta_{(n)}$ to $W(k)$, i.e. $R = W(k)(\zeta_{(n)})$. There are some other cases where the extension is obtained in a different way, but these are usually clear from the context.

Introduction

The book [H-K-T] starts one of its chapters with the saying *the larger its automorphism group, the richer its geometry* in reference to all branches of geometry, but especially to the geometry of algebraic curves. Though we will not deal with the size of automorphism groups in this thesis, the automorphism group still has an important effect on the geometry of algebraic curves.

We will mainly be interested in the comparison between the automorphism groups of two curves: one over a field k of characteristic p and one over a discrete valuation ring with residue field k. The main question when studying this situation is the lifting problem.

Problem. *Given a smooth projective algebraic curve C over a field k of characteristic p with automorphism group G, when is it possible to find a proper smooth curve $\mathcal{C}$ over a discrete valuation ring with residue field k such that $\mathcal{C}$ has special fibre C and also has automorphism group G and the action of the automorphism group is compatible with the reduction map between these curves?*

One may adjust the problem slightly, not asking for the full automorphism group to be lifted, but asking which of its subgroups can be lifted. It turns out that an automorphism group in characteristic p can be much larger than an automorphism group in characteristic 0 (Theorem 1.3.1). This kills all hope of a general lifting. However, we still have hope of lifting certain classes of automorphism groups. In particular, we wish to be able to solve the lifting problem for all cyclic groups G.

In chapter 1, we give a brief overview of reduction and lifting in a rather elementary setting. This serves to help the non-specialist (in the areas of arithmetic geometry and algebraic number theory) to get a feeling for the type of problems we are interested in. In section 1.3 we state the Oort-Sekiguchi conjecture as an example of a lifting problem. This conjecture is the main focus of this thesis. We also state a result which reduces the problem to the local problem of lifting automorphisms of power series rings. For the remainder of the thesis we shall concentrate exclusively on the local formulation of the Oort-Sekiguchi conjecture.

In chapter 2, we discuss some elementary results on the automorphisms of power series rings. We start off by classifying an automorphism σ by the image of a generator of the power series ring under σ. In section 2.3 we focus on finite order automorphisms and develop some properties which are specific to this case. In section 2.2 we try to get nice representatives for conjugacy classes of automorphisms. This turns out to be especially effective when working with power series rings over a field of characteristic zero.

Chapter 3 is a little more demanding. We start by considering the p-adic open unit disc $\mathrm{Spec}(R[\![Z]\!])$ where R is a discrete valuation ring. An automorphism of $R[\![Z]\!]$ induces an automorphism of this disc and this induced automorphism has certain fixed points which carry a lot of information about the automorphism. There are also a few nice results on how these fixed points are arranged on the disc. In section 3.3 we decribe the technique by Green and Matignon which has been the most effective in studying the lifting problem. In it we consider a power series ring $R[\![Z]\!]$ and its fixed ring under some automorphism. In the resulting ring extension we compare the special different to the generic different to give conditions under which lifting is possible.

In chapter 4 we show that equations may be determined, whose solution would form the coefficients of an order $q = p^n$ automorphism. In this way the solutions to these equations are in one-to-one correspondence with the

order q automorphisms. We may define a scheme by the spectrum of some polynomial ring (in infinitely many variables) modulo these equations. This scheme can be thought of as the moduli space of order q automorphisms. In section 4.2 novel results, due to the author, are presented. These equations are studied and their properties help us to give a criterion under which the lifting problem can be solved. This criterion is similar to the criterion in Hensel's lemma, where you need a solution modulo p to lift to a solution in $\mathbb{Q}_p$. Our criterion needs a solution modulo a higher power of the uniformizing parameter.

The work in sections 2.2 and 4.2 is the author's own original work. The results in 2.2 are in an earlier paper by Muckenhoupt [Mu], but the methods are slightly different from the author's. The author gave, as far as possible, his own proofs of known theorems and results.

Chapter 1

Reduction and Lifting

1.1 Reduction

Suppose that R is a commutative ring with unity and suppose that $I \subset R$ is an ideal of R. Then there is a natural surjective map $\rho_I : R \to R/I$ called the *reduction map* modulo the ideal I. For example, in elementary number theory where one works primarily with $R = \mathbb{Z}$, all the ideals are of the form $n\mathbb{Z}$ for some integer n. One then speaks simply of reduction modulo n.

As an especially important example, we mention the case where R is a local ring, with maximal ideal $\mathfrak{m}$. Then the reduction map $\rho_{\mathfrak{m}} : R \to R/\mathfrak{m} = k$ has the field k as its codomain. One may note that reduction modulo some power $\mathfrak{m}^r$ of $\mathfrak{m}$ is also possible. In this case the codomain is a ring, finite over k which contains nilpotent elements.

The reduction modulo any maximal ideal (i.e. even when R is not local) essentially comes from the map for R local which is described above. This is achieved by composing the localization map $\iota : R \to R_{\mathfrak{m}}$ with the reduction map $\rho_{\mathfrak{m}}$ on $R_{\mathfrak{m}}$. Here, $R_{\mathfrak{m}}$ refers to the localization of R at the prime ideal $\mathfrak{m}$. We remark that here we used the classical result that $R/\mathfrak{m} \cong R_{\mathfrak{m}}/R_{\mathfrak{m}}\mathfrak{m}$.

The utility of reduction is twofold. Firstly it is possible to disprove the existence of solutions to some equations. Secondly, if this is not possible, it is

at least possible to eliminate solutions with certain properties under reduction. As an example of the former, suppose that we are given a polynomial equation with integer coefficients, say $x^2 + y^2 = 1703$. This is an equality of integers and therefore the left and right hand sides must leave the same remainder under reduction modulo 4. However the quantities x^2 and y^2 can only leave a remainder of either 0 or 1, while 1703 gives 3 under reduction. It is clear that this cannot happen and there are no solutions. As an example of the latter consider the equation $x^2 + y^2 = 1702$. Since the right hand side now leaves a remainder of 2 when divided by 4, we can no longer conclude that there are no solutions as above. We can, however, conclude that if such a pair (x, y) exists then x and y must both be odd numbers.

The philosophy can be stated in modern terms as follows. Suppose that there is a ring homomorphism $f : R \to S$. This induces a ring homomorphism $F : R[x_1, x_2, \ldots, x_m] \to S[x_1, x_2, \ldots, x_m]$ defined by $F(r) = f(r)$ when $r \in R$ and $F(x_i) = x_i$ for each $i = 1, 2, \ldots, m$ and extended uniquely to $R[x_1, x_2, \ldots, x_m]$ to be a homomorphism. Suppose further that there is some tuple $(a_1, a_2, \ldots, a_m) \in R^m$ satisfying a polynomial equation $g(a_1, a_2, \ldots, a_m) = 0$ where g is defined over R. Then

$$F(g)\big(f(a_1), f(a_2), \ldots, f(a_m)\big) = f\big(g(a_1, a_2, \ldots, a_m)\big) = f(0) = 0$$

since f and F are ring homomorphisms. In particular, this holds when f is a reduction map.

Therefore, the image of a solution to a polynomial equation is again a solution to that polynomial, but viewed over the codomain. When f is a reduction map, the codomain is often a finite field, which is beneficial from a computational point of view. In a finite field, one may easily find all the solutions by performing a brute force search. Then we know that it is only necessary to consider elements $r \in R$ which reduce to one of these solution in the finite field.

Here is another example, which is more technical of nature, but illustrates that reduction is also an important process in the algebraic geometric setting.

We assume for the rest of this section that the reader is familiar with the language of schemes. The reader unfamiliar with the language of schemes may skip to the next section. Suppose that S is a Dedekind scheme. This means that S is normal, locally Noetherian and of dimension at most 1. Suppose further that $\mathfrak{p} \in S$ and denote the residue field of the local ring $\mathcal{O}_{S,\mathfrak{p}}$ by $k_{\mathfrak{p}}$.

Now, let $C \to S$ be a curve over S. For our purposes, this means that C is proper over S and that its fibres are equidimensional of dimension one. It is then possible to form the fibre product $C_{k_{\mathfrak{p}}} = C \times_S \mathrm{Spec}(k_{\mathfrak{p}})$ called the reduction modulo $\mathfrak{p}$. This turns out to be an algebraic curve over the field $k_{\mathfrak{p}}$ (or, at worst a finite connected union of algebraic curves).

Example. Let E_K be an elliptic curve over the fraction field K of a discrete valuation ring R. It is then often possible to define a scheme E over $\mathrm{Spec}(R)$ which has the generic fibre E_K. Let E_k denote the closed fibre of this scheme. Then E_k is a cubic curve over the residue field k. Suppose that this curve is non-singular.

Let m be an integer which is relatively prime to the characteristic of k. Then the map

$$E_K(K)[m] \to E_k(k)$$

defined on the m-torsion points of E_K is injective (see [Si], VII.3). One may thus obtain information about the torsion on the elliptic curve over K by considering the reduction of the elliptic curve modulo π. As is usual with our theme that reduction imposes restrictions on what may happen over K, we see that the m-torsion of the elliptic curve E_K must be a subgroup of the group of rational points on E_k.

1.2 Lifting

Lifting can be described as an inverse procedure to reduction. Suppose that $f : R \to k$ is a surjective map as in the previous section. We defined what it means to reduce a set of elements in R to k. Lifting is the procedure, given a set of elements in k, to find a corresponding set of elements in R that reduces to that set. Usually the original set will have some property, and the lifting will be required to have the same property.

For example, let $P(x) = x^2 + 1$ a polynomial defined over the integers. We may take the reduction of this polynomial modulo some prime number p. If $p \equiv 1 \pmod 4$, then the polynomial has a root in $\mathbb{F}_p$. This gives an element $\bar{x}$ with the property that $\bar{x}^2 + 1 = 0$. However, we know that there is no integer x for which $x^2 + 1 = 0$. Hence we cannot lift this element to $\mathbb{Z}$ while keeping this property.

Usually, we prefer to lift to the complete local ring $\mathbb{Z}_p$ rather than to $\mathbb{Z}$. We shall see shortly (Hensel's Lemma) that whenever $p \equiv 1 \pmod 4$, the roots of $P(x)$ lift from $\mathbb{F}_p$ to $\mathbb{Z}_p$ (for $p \neq 2$). So, it is possible to lift a solution to the equation $x^2 + 1 = 0$ to the ring $\mathbb{Z}_p$. The problem of determining whether solutions to each $\mathbb{Z}_p$ imply a solution in $\mathbb{Z}$ is another fundamental problem in number theory, called the *local-to-global problem*.

As we have seen, the existence of a lifting might depend on the ring chosen to lift to. Luckily, there is a canonical ring of characteristic 0 associated to any field k of characteristic p, called the *ring of Witt vectors* of k. We shall usually consider lifting to this ring, or a finite extension thereof.

We shall not describe the construction of the Witt vectors here[1], but merely recall the property that makes it suitable for us. If k is a field of characteristic p, then the ring of Witt vectors $W(k)$ is a complete discrete valuation ring of characteristic zero with residue field k. We shall often make the assumption that k is algebraically closed. In that case we have the extra benefit that every finite extension of $W(k)$ is also a complete discrete valua-

[1] One may consult [Se] for a quick introduction to Witt vectors.

tion ring with residue field k.

Theorem 1.2.1 (Hensel's Lemma)**.** *Let R be a complete discrete valuation ring and suppose that $f(X) \in R[X]$. Suppose further that there is an element $a_0 \in R$ such that*

$$v(f(a_0)) > 2v(f'(a_0))$$

where v is the valuation associated to R and f' is the formal derivative of f. Then there exists an element $a \in R$ such that $f(a) = 0$ and $v(a - a_0) \geq v(f(a_0)) - 2v(f'(a_0))$.

Proof. [La2] II.2. □

In particular, when $f(a_0)$ reduces to 0 in k and $f'(a_0)$ does not reduce to 0 in k, there exists a root $a \in R$ of f such that a and a_0 reduce to the same element of k. This can be restated as follows. Let $\bar{f}$ be the polynomial obtained by reducing each coefficient of f modulo the maximal ideal of R. If $\bar{f}$ has a simple root in k, then this root lifts to a root of f in R.

Theorem 1.2.2 ([Gr])**.** *Assume that R is a complete discrete valuation ring and that K is its field of fractions. Let $f_1, f_2, \ldots, f_r$ be a system of r polynomials in n variables, denoted collectively by Z. Then there are constants $N \geq 1, c \geq 1, s \geq 0$ depending on the ideal of $R[Z]$ generated by $f_1, f_2, \ldots, f_r$ such that for every $\nu \geq N$ and any X in R^n such that*

$$f_i(X) \equiv 0 \pmod{\pi^\nu} \quad \text{for every } i = 1, 2, \ldots, r$$

there exists $Y \in R^n$ such that $f_i(Y) = 0$ for every $i = 1, 2, \ldots, r$ and

$$Y \equiv X \pmod{\pi^{\lfloor \nu/c \rfloor - s}}.$$

□

This theorem can be summarized to say that if a solution to a finite set of polynomial equations can be lifted sufficiently far (modulo a high enough

power of π), then it can be lifted to the ring R. In particular, if a solution can be found modulo π^n for every positive integer n, then a solution exists in R.

As in the previous section we wish to translate the process of lifting to the language of schemes. This will illustrate the geometric significance of lifting. Suppose that X_k is a curve over $\mathrm{Spec}(k)$. Lifting is the procedure of finding a (complete) discrete valuation ring R with residue field k and an R-scheme X which has special fibre X_k. There are often other conditions to be met, e.g. if X_k is a smooth k-curve, we need to find a smooth R-curve X which has special fibre X_k.

We may also lift relative properties. Given a morphism of k-schemes $f_k : X_k \to Y_k$, is it possible to find R and a morphism $f : X \to Y$ of R-schemes which induces the morphism f_k on the special fibre? If f_k has some property P, can we find f which also has property P?

1.3 The Oort-Sekiguchi Conjecture

As an example of a lifting problem we present the Oort-Sekiguchi Conjecture. This conjecture provides the motivation for most of the material in this thesis. This conjecture is not concerned with lifting solutions to polynomial equations, but rather to lift certain automorphism groups. We will, however, reinterpret this conjecture in terms of equations in section 4.1.

Let k be an algebraically closed field of characteristic p and let $W(k)$ be its ring of Witt vectors. Let R be a complete discrete valuation ring dominating $W(k)$. (Usually we will take R to be a finite extension of $W(k)$.) Let $\mathcal{C}$ be a smooth curve over R (an integral scheme proper over $\mathrm{Spec}(R)$ with one-dimensional fibres over the points of $\mathrm{Spec}(R)$). Then the fibre C of $\mathcal{C}$ over the closed point of $\mathrm{Spec}(R)$ is an algebraic curve over k, while the generic fibre is an algebraic curve over K, the field of fractions of R. We wish to compare the automorphism groups of these two curves. In particular, suppose that

we are given a curve C over k and a subgroup G of its automorphism group. We ask when it is possible to lift this curve to a curve $\mathcal{C}$ over R such that the generic fibre $\mathcal{C}_K$ has automorphism group that contains G. We assume that the curve C is smooth over k. We then require $\mathcal{C}$ to be a smooth curve over R. Note that this smoothness condition implies that the (arithmetic) genus of $\mathcal{C}$ over R is the same as the genus of C over k. Hence, this equality of genera is a necessary condition for smoothness.

Another way to formulate this is in terms of G-galois covers. Given a curve C and a group G that acts on it, define the map $\bar{\phi} : C \to C/G$, where C/G is the quotient of C by G. We wish to lift $\bar{\phi}$ to a morphism of R-curves $\phi : \mathcal{C} \to \mathcal{C}/G$. Furthermore, the action of G on $\mathcal{C}$ should, in the special fibre, be the same action as that of G on C in the initial setup.

It is almost immediately clear that such a lifting does not exist in general. In characteristic zero, a theorem of Hurwitz states that the automorphism group is bounded by $84(g-1)$, where g is the genus of the curve. On the other hand, it is known that there exist curves in characteristic p with automorphism groups larger than this. We state the theorem here for reference and give an example of a curve over a field of characteristic p with automorphism group larger than this.

Theorem 1.3.1 (Hurwitz)**.** *Suppose that C is a projective algebraic curve of genus $g \geq 2$ over an algebraically closed field k of characteristic* $\mathrm{char}(k)$ *and denote the automorphism group of C by G. Suppose that G is finite. If* $\mathrm{char}(k) = 0$ *or if* $\mathrm{char}(k) = p$ *does not divide the order of G, then G has order at most* $84(g-1)$.

Proof. Consider the quotient map $\phi : C \to C/G$. It has degree $d = |G|$. Suppose further that the quotient curve C/G has genus g'. Since this is a galois cover, the ramification at P is the same as the ramification at $\sigma(P)$ for any point P and any $\sigma \in G$. Furthermore, k is algebraically closed, and hence there can be no inertia. We obtain the formula $e_P h_P = d$, where h_P is the cardinality of the set $\{\sigma(P) | \sigma \in G\}$.

The Riemann-Hurwitz formula then states that

$$2(g-1) \geq 2d(g'-1) + \sum (e_i - 1),$$

where the sum runs over all the ramified points of ϕ. Equality occurs when the ramification is tame for each $i = 1, 2, \ldots, n$. In characteristic zero ramification is always tame, while in characteristic p it is tame when p does not divide the ramification index e_i. But p does not divide d, and $e_i h_i = d$. So, under the conditions we can only have tame ramification.

If two points P_i and P_j are in the same orbit under the action of G, i.e. if $\sigma(P_i) = P_j$ for some $\sigma \in G$, then they have the same ramification indices, i.e. $e_i = e_j$. So we divide the points into their orbit classes: h_i points with ramification index e_i, for $i = 1, 2, \ldots, r$. We may further suppose that $2 \leq e_1 \leq e_2 \leq \cdots \leq e_r$. Bearing in mind that $e_i h_i = d$ for every i, the Riemann-Hurwitz formula becomes

$$2(g-1) = 2d(g'-1) + rd - \sum h_i = 2d(g'-1) + rd - \sum \frac{d}{e_i},$$

or

$$d = 2(g-1)\big(2g' - 2 + r - \sum \frac{1}{e_i}\big)^{-1}.$$

So we wish to minimize $2g' - 2 + r - \sum \frac{1}{e_i}$, while keeping it positive. It suffices to prove that this minimum is $1/42$. This is done by cases.

Case 1: $g' \geq 2$. Clearly $r \geq \sum \frac{1}{e_i}$, since $\frac{1}{e_i} \leq 1$. Hence $2g' - 2 + r - \sum \frac{1}{e_i} \geq 2g' - 2 \geq 2$.

Case 2: $g' = 1$. Here $2g' - 2 + r - \sum \frac{1}{e_i} = \sum (1 - \frac{1}{e_i})$, and since this must be positive we must have $r \geq 1$ and $\sum (1 - \frac{1}{e_i}) \geq 1 - \frac{1}{e_1} \geq \frac{1}{2}$.

Case 3: $g' = 0$. In this case $2g' - 2 + r - \sum \frac{1}{e_i} = (r-2) - \sum \frac{1}{e_i}$, so clearly $r \geq 3$.

Subcase 1: $r \geq 5$. Then $(r-2) - \sum \frac{1}{e_i} \geq (5-2) - \sum \frac{1}{2} = \frac{1}{2}$.

Subcase 2: $r = 4$. Then $(r-2) - \sum \frac{1}{e_2} \geq (4-2) - 3 \times \frac{1}{2} - \frac{1}{3} = \frac{1}{6}$.

Subcase 3(a): $r = 3$ and $e_1 \geq 3$. Then $(r-2) - \sum \frac{1}{e_2} \geq 1 - 2 \times \frac{1}{3} - \frac{1}{4} = \frac{1}{12}$.

Subcase 3(b): $r = 3$ and $e_1 = 2$. Then $(r-2) - \sum \frac{1}{e_2} \geq 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{7} = \frac{1}{42}$. $\square$

Remark. The assumption that G is finite is not strictly necessary. This can be proven independently using Weierstrass points. It does, however, keep the proof at a reasonable length. The result is also true in characteristic p, when $p > 2g + 1$, where wild ramification cannot occur ([Sa], Theorem 14.3.13).

Example. In this example, we exhibit an algebraic curve in characteristic p, which does not satisfy this bound. The Hermitian curve is the compactification of the curve defined by the equation

$$y^q + y = x^{q+1}$$

over the finite field $\mathbb{F}_{q^2}$. This curve has genus $g = \frac{q(q-1)}{2}$, since this plane model is nonsingular and of degree $q + 1$.

To estimate the size of its automorphism group, we mention a few elements in this group.

Firstly, for every $(d, e) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ such that $e^q + e = d^{q+1}$, we have an automorphism σ defined by $\sigma(x) = x + d$ and $\sigma(y) = y + d^q x + e$. One may check that indeed $\sigma(y)^q + \sigma(y) = \sigma(x)^{q+1}$. These automorphisms form a subgroup of order q^3 of the full group of automorphisms.

A second family of automorphism is given by $\tau(x) = cx$, $\tau(y) = c^{q+1}y$, for any non-zero element $c \in \mathbb{F}_{q^2}$. This clearly forms a subgroup of order $q^2 - 1$ of the full group of automorphisms.

Lastly, there is an involution μ defined by $\mu(x) = x/y$ and $\mu(y) = 1/y$.

We may describe these automorphisms as elements of the projective linear group $\mathrm{PGL}_3(\mathbb{F}_{q^2})$. The action of $\mathrm{PGL}_3(\mathbb{F}_{q^2})$ on the projective plane may be given by matrix multiplication of the element of $\mathrm{PGL}_3(\mathbb{F}_{q^2})$ with the projective coordinates (X, Y, Z), where, of course, $x = X/Z$ and $y = Y/Z$. The automorphisms σ, τ and μ can then be described as the matrices

$$\begin{pmatrix} 1 & 0 & d \\ d^q & 1 & e \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} c & 0 & 0 \\ 0 & c^q & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

One can show that these matrices generate the projective unitary group

$\mathrm{PGU}_3(\mathbb{F}_{q^2})$ which has order $q^3(q^3+1)(q^2-1)$. This is clearly greater than $84(g-1)$. For large p, it is in the order of $16g^4$.

For a full proof that the automorphism group of the Hermitian curve is isomorphic to $\mathrm{PGU}_3(\mathbb{F}_{q^2})$, one may consult [H-K-T], Chapter 11.

Theorem 1.3.2 ([Na]). *Suppose that C is an algebraic curve of genus g over a field k of characteristic p and suppose that the automorphism group G of C is abelian. Then*

- $|G| \leq 4g+2$ *if $p=2$, and*
- $|G| \leq 4g+4$ *otherwise.*

□

The theorem by Nakajima lets us believe that we should concentrate on the case where G is abelian. However, Green and Matignon [G-M1] showed that there are abelian groups which cannot be lifted. Most notably, for $p>2$, there are realizations of the group $(\mathbb{Z}/p\mathbb{Z})^2$ which cannot be lifted. Hence, we turn our attention toward the simplest case, when G is cyclic.

Grothendieck [SGA1] solved the problem in the case where $\left|G\right|$ is not divisible by p. This method also implies that if the conjecture is known to be true for cyclic groups of order p^n it would also be true for cyclic groups of order ap^n where a is relatively prime to p. We shall give proofs to the "local versions" (to be described below) of both these statements in Section 2.3. Thus it remains to consider the case where the order of G is a power of p.

Conjecture 1 (Oort-Sekiguchi). *Let C be a smooth projective curve over the field k and suppose that the automorphism group of C contains a cyclic group G of order p^r. Then there exists a smooth curve $\mathcal{C}$ over R with special fibre C such that its automorphism group contains G and that the actions of G on C and on $\mathcal{C}$ are compatible.*

For $\left|G\right| = p^n$ with $n \leq 2$, it is known that the conjecture is true. The case $n=1$ is originally due to [O-O-S] and new methods due to [G-M1] obtained

its validity for $n = 1, 2$. A key ingredient in [G-M1] is a local-global principle. This states that if the conjecture were known to be true in the local setting, it would follow in the global setting as described above. Locally, the conjecture can be stated as follows:

Conjecture 2 (Local Oort-Sekiguchi)**.** *Let k be an algebraically closed field of characteristic p and suppose that $\bar{\sigma}$ is an automorphism of $k[\![z]\!]$ of order p^n. Then there exists a local ring R finite over the Witt vectors $W(k)$ and an automorphism σ of $R[\![Z]\!]$ of order p^n such that the reduction of σ modulo π equals $\tilde{\sigma}$.*

Remark. In the Local Oort-Sekiguchi Conjecture we mention the reduction of an automorphism modulo π. This will be defined in section 2.1.

Theorem 1.3.3 ([G-M1])**.** *The Local Oort-Sekiguchi conjecture implies the Oort-Sekiguchi conjecture.* □

Grothendieck showed that a smooth lifting always exists on the étale locus of the map between the curve and its quotient by its automorphism group. The idea is that if we are always able to lift this map locally at the ramified points, then we will be able to lift the map globally by glueing the maps from the étale locus and the hypothesized local maps. To do this, we need a certain overlap of the open sets on which these maps are defined. This is exactly what [G-M1] proved. This *prolongation lemma* extends the domain of definition of the hypothesized local map. They then show that it can be done in a way which is consistent with the map on the étale locus.

In the rest of this thesis we shall be concerned only with the local phrasing of this question. Hence, from here on we shall work with power series rings over fields of characteristic p and power series rings over complete discrete valuation rings. This is the topic of the next chapter.

Chapter 2

Automorphisms of Power Series Rings

2.1 Some Elementary Results

Automorphisms of power series rings over fields.
We shall start out by describing some of the elementary results for automorphisms of power series ring over fields. These results put some restrictions on what $\sigma(Z)$ may look like if σ is an automorphism.

Suppose that $E[\![Z]\!]$ is a power series ring over a field E. We wish to investigate the automorphisms of $E[\![Z]\!]$. We shall only consider such automorphisms which fix E. Consequently it is enough to specify $\sigma(Z)$ to define a homomorphism $\sigma : E[\![Z]\!] \to E[\![Z]\!]$. Clearly $\sigma(Z)$ is an element of $E[\![Z]\!]$, so we may write

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

It is clear that the image of Z cannot be a unit in $E[\![Z]\!]$, otherwise σ could not be an automorphism. Indeed, if $\sigma(Z) = f$, then $\sigma^{-1}(1/f) = 1/Z$, and the image of an element of $E[\![Z]\!]$ under an automorphism σ^{-1} falls outside $E[\![Z]\!]$. We conclude that $a_0 = 0$.

To obtain surjectivity of σ we need $a_1 \neq 0$. Indeed, if $a_1 = 0$ then the image of σ would contain only power series with zero coefficient for Z.

Automorphisms over power series rings over discrete valuation rings.

In exactly the same way as for power series rings over fields, we conclude that the image of Z under an automorphism σ cannot be a unit in $R[\![Z]\!]$. Hence $a_0 \in \pi R$.

Similarly we may use the surjectivity of σ to obtain that $a_1 \in R^\times$. Indeed, if $a_1 \in \pi R$, then Z does not lie in the image of σ. The only power series that lie in the image of σ are those whose coefficient of Z is in the maximal ideal πR.

In section 3.1 we will see that we may restrict our attention further to those automorphisms for which $a_0 = 0$.

Comparison between automorphisms of $R[\![Z]\!]$ and automorphisms of $k[\![Z]\!]$.

Before we start, we remind the reader that R is a discrete valuation ring and that k is its residue field. Recall that we have a canonical reduction map $r : R \to k$, and that this may be extended to a map $\rho : R[\![Z]\!] \to k[\![z]\!]$ by setting $\rho(Z) = z$ and $\rho(x) = r(x)$ for $x \in R$. The map ρ is the unique homomorphism for which this holds.

Given an automorphism $\sigma : R[\![Z]\!] \to R[\![Z]\!]$ we would like to define a reduction of σ modulo π. Assuming existence and well-definedness for the moment, we shall denote this automorphism by $\bar{\sigma} : k[\![z]\!] \to k[\![z]\!]$. Ideally if we define $\sigma(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots$, we would like $\bar{\sigma}$ to be defined by the equation $\bar{\sigma}(z) = \bar{a}_0 + \bar{a}_1 z + \bar{a}_2 z^2 + \cdots$, where each $\bar{a}_i$ is the reduction of a_i modulo π. It is not hard to show that this indeed does the trick. If two elements in $R[\![Z]\!]$ reduce to the same element in $k[\![z]\!]$, they differ by a multiple of π. Since $\bar{\sigma}(\pi) = 0$, we conclude that $\bar{\sigma}$ sends these elements in $R[\![Z]\!]$ to the same element of $k[\![z]\!]$. Thus $\bar{\sigma}$ is well-defined on $k[\![z]\!]$.

We shall denote this homomorphism between automorphism groups by $\Psi : \mathrm{Aut}_R(R[\![Z]\!]) \to \mathrm{Aut}_k(k[\![z]\!])$.

Let us compare the criterion we set for automorphisms of $k[\![z]\!]$ and $R[\![Z]\!]$. In the case of $k[\![z]\!]$ we had the conditions that $a_0 = 0$ and $a_1 \neq 0$, while in the case of $R[\![Z]\!]$ we had the conditions $a_0 \in \pi R$ and $a_1 \in R^\times$. It is clear that under reduction the conditions for σ to be an automorphism of $R[\![Z]\!]$ become exactly the conditions for $\bar{\sigma}$ to be an automorphism of $k[\![z]\!]$.

2.2 Conjugacy Classes of Automorphisms of Power Series Rings

In this section we explore the conjugates of the elements in the automorphism group of the power series ring $A[\![Z]\!]$ for some commutative rings A. In particular we are interested in finding (at least) one element in any conjugacy class which has a particularly nice form. The use of this idea stems from the fact that an element in any group has the same order as any of its conjugates.

We shall assume that all the automorphisms in this section are of the form $\sigma(Z) = Z(a_1 + a_2Z + a_3Z^2 + \cdots)$ and $\tau(Z) = Z(b_1 + b_2Z + b_3Z^2 + \cdots)$. This is not a severe restriction. In fact, in section 2.3 we state a theorem that all the automorphisms we are interested in, take this form. We are interested in the conjugates of σ, i.e. in the automorphisms of the form $\tau \circ \sigma \circ \tau^{-1}$. Hence a good starting point is to compute $\tau^{-1}(Z)$ explicitly in terms of $b_1, b_2, \ldots$ as a power series in Z.

Set $\tau^{-1}(Z) = Z(c_1 + c_2Z + c_3Z^2 + \cdots)$. Then we may compute $\tau \circ \tau^{-1}(Z) = g_1Z + g_2Z^2 + g_3Z^3 + \cdots$ where each g_n is a polynomial in the variables $b_1, \ldots, b_n, c_1, \ldots, c_n$. When we compose the formulas for τ and τ^{-1} we obtain

$$\begin{aligned}
\tau \circ \tau^{-1}(Z) &= \tau(c_1 Z + c_2 Z^2 + c_3 Z^3 + \cdots) \\
&= c_1 \tau(Z) + c_2 \tau(Z)^2 + c_3 \tau(Z)^3 + \cdots \\
&= c_1(b_1 Z + b_2 Z^2 + \cdots) + c_2(b_1 Z + b_2 Z^2 + \cdots)^2 + \cdots \\
&= b_1 c_1 Z + (b_1^2 c_2 + b_2 c_1) Z^2 + (b_1^3 c_3 + 2 b_1 b_2 c_2 + b_3 c_1) z^3 + \cdots .
\end{aligned}$$

We thus get explicit formulas for the polynomials g_i:

$$\begin{aligned}
g_1 &= b_1 c_1 \\
g_2 &= b_1^2 c_2 + b_2 c_1 \\
g_3 &= b_1^3 c_3 + 2 b_1 b_2 c_2 + b_3 c_1.
\end{aligned}$$

etc. But τ and τ^{-1} are inverses, which means that $\tau \circ \tau^{-1}(Z) = Z$. Hence we must have $g_1 = 1$ and $g_i = 0$ for $i \geq 2$. We may thus rewrite the equations above as

$$\begin{aligned}
b_1 c_1 &= 1 \\
b_1^2 c_2 + b_2 c_1 &= 0 \\
b_1^3 c_3 + 2 b_1 b_2 c_2 + b_3 c_1 &= 0.
\end{aligned}$$

We may then systematically solve for the c_i from these equations. The first few such calculations yield

$$\begin{aligned}
c_1 &= b_1^{-1} \\
c_2 &= -b_1^{-3}(b_2) \\
c_3 &= -b_1^{-5}(b_1 b_3 - 2 b_2^2).
\end{aligned}$$

Before we continue we set out to prove a few structural results about the polynomials g_i.

Lemma 2.2.1. *The n-th coefficient g_n of Z^n in the composite $\tau \circ \tau^{-1}(Z)$ can be expressed as*

$$g_n = \sum_{t=1}^{n} c_t \sum_{i_1+i_2+\cdots+i_t=n} b_{i_1} b_{i_2} \cdots b_{i_t}.$$

Remark. Composing the other way ($\tau^{-1} \circ \tau$) yields the same equations, but with the b_i and the c_i interchanged. However, once we solve for the c_i in terms of the b_i there is no difference.

Proof. We are looking for the coefficient of Z^n in the expansion of

$$\tau \circ \tau^{-1}(Z) = c_1(b_1 Z + b_2 Z^2 + \cdots) + c_2(b_1 Z + b_2 Z^2 + \cdots)^2 + \cdots .$$

It is clear that the contribution from the first term is $c_1 b_n$ and that the last term to contribute is the n-th term $c_n(b_1 Z + b_2 Z^2 + \cdots)^n$, whose contribution is $c_n b_1^n$. Consider the t-th term $c_t(b_1 Z + \cdots)^t$. To obtain the contribution to the coefficient of Z^n, think of multiplying out this power. One has to take one term (e.g. $b_r Z^r$) from each of the t factors. Let the indices of these terms be denoted by $i_1, i_2, \ldots, i_t$ (so the factors in the product are $b_{i_1} Z^{i_1}, \ldots, b_{i_t} Z^{i_t}$). Note that the coefficient b_i is always paired with Z^i, so to get the total degree of Z in any product we may sum the indices of the b_i. The degree is required to be n, so we need $i_1 + i_2 + \cdots + i_t = n$. Summing over all such products, we obtain the result. □

Corollary. *We can attach weights to the variables b_i and c_i in various ways to make the g_n homogeneous polynomials in the variables b_i, c_i:*

- *If $w(c_i) = i$ and $w(b_i) = -1$ then g_n has degree 0,*
- *if $w(c_i) = 1$ and $w(b_i) = 0$ then g_n has degree 1, and*
- *if $w(c_i) = 0$ and $w(b_i) = i$ then g_n has degree n.* □

Remark. We may also form new weightings by taking linear combinations of these. For example, if C is any integer, then the weight function $w(c_i) = C$ and $w(b_i) = i$ makes g_n homogeneous of weight $n + C$.

We may now list more equations for the c_j in terms of the b_i obtained with the help of a computer.

$$\begin{aligned} c_1 &= b_1^{-1} \\ c_2 &= -b_1^{-3}(b_2) \\ c_3 &= -b_1^{-5}(b_1b_3 - 2b_2^2) \\ c_4 &= -b_1^{-7}(5b_2^3 - 5b_1b_2b_3 + b_1^2b_4) \\ c_5 &= -b_1^{-9}(5a_2^4 + 21b_1b_2^2b_3 - 6b_1^2b_2b_4 - 3b_1^2b_3^2 + b_1^3b_5). \end{aligned} \tag{2.1}$$

Lemma 2.2.2. *Assign the weights $w(b_i) = i$ (and hence $w(b_1^{-1}) = -1$). The equation for $c_n, n \geq 1$ is a homogeneous polynomial of weight -1 in $\mathbb{Z}[b_1, b_2, \ldots, b_n][b_1^{-1}]$. Furthermore, in this expression for $c_n, n \geq 3$, the variables b_n and b_{n-1} occur only once, namely in the terms*

$$-b_1^{-n-1}b_n \quad \text{and} \quad -b_1^{-n-2}b_{n-1}(n - 1 - 2b_2),$$

respectively.

Proof. Recall the formula $c_nb_1^n + \cdots + c_1b_n = g_n = 0$. We use this equation to solve for c_n. It is thus clear that b_1 is the only variable that gets inverted. The statement about the weight of the c_j can be proved by induction. It is clear for $c_1 = b_1^{-1}$. So if $w(c_j) = -1$ for $j = 1, 2, \ldots, n-1$ and $w(c_n) = C$, then the expression for g_n is homogeneous of weight $n - 1$, except possibly for the term $c_nb_1^n$, which is of weight $n + C$. But we must solve for c_n from this equation. We are forced to conclude that this term has the same weight as the others and that $w(c_n) = -1$.

From the equation $c_nb_1^n + \cdots + c_1b_n = 0$, it is clear that

$$c_n = -b_1^{-n}(c_1b_n + \cdots)$$

where the terms not listed do not contain the variable b_n. Since $c_1 = b_1^{-1}$, we see that b_n only occurs in the term $-b_1^{-n-1}b_n$. Concerning the statement about b_{n-1}, we shall need to compute the coefficients of c_{n-1} and c_2 in the expression for g_n. It is not hard to see that the following expression is correct:

$$g_n = c_1 b_n + c_2 \binom{2}{1} b_{n-1} b_1 + \cdots + c_{n-1} \binom{n-1}{1} b_1^{n-2} b_2 + c_n b_1^n. \tag{2.2}$$

To compute the coefficient of b_{n-1} we must remember that this variable also occurs in the expression for c_{n-1}. From what we just proved we know that $c_{n-1} = -b_1^{-n} b_{n-1} + \cdots$ where none of the other terms contain a b_{n-1}. Hence

$$\begin{aligned} c_n &= -b_1^{-n}(c_1 b_n + 2c_2 b_{n-1} b_1 + \cdots + (n-1)c_{n-1} b_1^{n-2}) \\ &= -b_1^{-n}(2(-b_1^{-3}(b_2))b_{n-1} b_1 + (n-1)(-b_1^{-n} b_{n-1} + \cdots) b_1^{n-2} + \cdots) \\ &= -b_1^{-n-2}(-2b_2 b_{n-1} + (n-1)b_{n-1} + \cdots) \\ &= -b_1^{n-2}(b_{n-1}(n-1-2b_2)) + \cdots \end{aligned}$$

as required. □

Remark. In the final expression 2.2 we listed for g_n it is only coincidental that each c_i has only one term multiplied by some constant. In general, for $3 \leq t \leq n-2$, we will need more terms.

Let us finally turn to the reason why we wish to study these equations, namely to find "nice" conjugates of certain automorphisms. Start with an automorphism σ defined by $\sigma(Z) = a_1 Z + a_2 Z^2 + \cdots$. We wish to determine the conjugate $\tau \circ \sigma \circ \tau^{-1}$ in terms of the a_i and the b_i. Do this, first note that τ is defined in terms of the b_i, σ is defined in terms of the a_i and τ^{-1} is defined in terms of the c_i. However, we already have equations in which the c_i are expressed in terms of the b_i. Hence $\tau\sigma\tau^{-1}$ can be expressed in terms of the a_i and b_i alone.

$$\begin{aligned}
\tau\sigma\tau^{-1}(Z) &= \tau\sigma(c_1Z + c_2Z^2 + c_3Z^3 + \cdots) \\
&= \tau(c_1\sigma(Z) + c_2\sigma(Z)^2 + c_3\sigma(Z)^3 + \cdots) \\
&= \tau\big(c_1(a_1Z + a_2Z^2 + \cdots) + c_2(a_1Z + a_2Z^2 + \cdots)^2 + \cdots\big) \\
&= \big(c_1(a_1\tau(Z) + a_2\tau(Z)^2 + \cdots) + c_2(a_1\tau(Z) + a_2\tau(Z)^2 + \cdots) + \cdots\big) \\
&= \Big(c_1\big(a_1(b_1Z + b_2Z^2 + \cdots) + a_2(b_1Z + \cdots) + \cdots\big) + c_2\big(\cdots\big)^2 + \cdots\Big) \\
&= a_1b_1c_1Z + (a_1b_2c_1 + a_1^2b_1^2c_2 + a_2b_1^2c_1)Z^2 + \cdots
\end{aligned}$$

Remark. For computational purposes we mention the following. Let $f(Z) = \sigma(Z)$ and $g(Z) = \tau(Z)$ be the formal power series obtained by applying the automorphisms σ and τ to Z. Then we may determine $\sigma \circ \tau(Z)$ as $g(f(Z))$, where the latter expression is composition of formal power series. Note that the order is reversed.

After we substitute the formulas 2.1 for the c_i, this becomes

$$\begin{aligned}
\tau\sigma\tau^{-1}(Z) &= a_1Z + b_1^{-1}\big(b_1^2a_2 - b_2(a_1^2 - a_1)\big)Z^2 + \\
&\qquad b_1^{-2}\big(2b_2^2(a_1^3 - a_1^2) - b_1b_3(a_1^3 - a_1) - 2b_1^2b_2(a_1 - 1) + b_1^4a_3\big)Z^3 + \cdots .
\end{aligned}$$

For convenience, let us call the coefficient of Z^n in $\tau\sigma\tau^{-1}(Z)$, f_n.

Lemma 2.2.3. *If we assign the weights $w(a_i) = 0$ and $w(b_i) = i$, then f_n is a homogeneous polynomial of weight $n - 1$.*

Proof. By Lemma 2.2.2, each c_i is a homogeneous polynomial of weight -1 under these hypotheses. From the equation

$$\tau\sigma\tau^{-1}(Z) = \Big(c_1\big(a_1(b_1Z + b_2Z^2 + \cdots) + a_2(b_1Z + \cdots)^2 + \cdots\big) + c_2\big(\cdots\big)^2 + \cdots\Big),$$

we see that it suffices to prove that the coefficient of Z^n in

$$a_1(b_1Z + b_2Z^2 + \cdots) + a_2(b_1Z + b_2Z^2 \cdots)^2 + \cdots$$

is homogeneous of weight n. But the a_i all have weight 0, so it suffices to prove that the coefficient of Z^n in $(b_1Z + b_2Z^2 + \cdots)^r$ is homogeneous of

degree n for any positive integer r. This is clear, since multiplying out this power gives various terms of the form

$$b_{i_1} Z^{i_1} b_{i_2} Z^{i_2} \cdots b_{i_r} Z^{i_r}.$$

Such a term contains Z to the power n if and only if $i_1 + i_2 + \cdots + i_r = n$, whence the coefficient is homogeneous of degree n. The statement follows by the fact that the sum of homogeneous polynomials of the same degree is again homogeneous of that degree. □

Lemma 2.2.4. *The coefficient of b_n in f_n is $b_1^{-1}(a_1 - a_1^n)$.*

Proof. The variable b_n only occurs in the variable b_n itself and in the equations for c_r for $r \geq n$. In the term containing Z^n as a factor, the only contributions can thus come from b_n and c_n. Consider, once again, the expansion

$$\tau\sigma\tau^{-1}(Z) = \Big(c_1\big(a_1(b_1Z+b_2Z^2+\cdots)+a_2(b_1Z+\cdots)^2+\cdots\big)+c_2\big(\cdots\big)^2+\cdots\Big).$$

The only contribution from b_n must come from the first term $c_1(a_1(b_1Z + b_2Z^2 + \cdots + b_nZ^n + \cdots))$. This is because in any power $(b_1Z + b_2Z^2 + \cdots)^r$, $r \geq 2$, any term containing a b_n will necessarily have Z to a power strictly greater than n. We thus have the contribution $c_1a_1b_n = a_1b_1^{-1}b_n$ in this case.

To determine which terms contain c_n, we write

$$\tau\sigma\tau^{-1} = c_1\tau\sigma(Z) + c_2\tau\sigma(Z)^2 + \cdots .$$

The term containing c_n must be

$$c_n\tau\sigma(Z)^n = c_n(a_1(b_1Z + b_2Z^2 + \cdots) + a_2(b_1Z + \cdots)^2 + \cdots)^n.$$

The only way to get a factor Z^n in this case is from the linear term a_1b_1Z (raised to the power n). The contribution in this case is then $c_na_1^nb_1^n$. By Lemma 2.2.2, c_n contains the variable b_n only in the term $-b_1^{-n-1}b_n$, so the contribution to the coefficient of Z^n is $-b_1^{-n-1}b_na_1^nb_1^n = -a_1^nb_1^{-1}b_n$.

Thus the coefficient of b_n in f_n is indeed $b_1^{-1}(a_1 - a_1^n)$. □

Corollary. *If A is a field in which a_1 has infinite order, then any automorphism defined by $\sigma(Z) = a_1 Z + \cdots$ is conjugate to an automorphism σ' defined by $\sigma'(Z) = a_1 Z$.*

Proof. Since the coefficient of b_2 in f_2 is $b_1^{-1}(a_1 - a_1^2)$, we can solve for b_2 in $f_2 = 0$ under the hypotheses. Then we can solve for b_3 in $f_3 = 0$, since the coefficient of b_3 there is $b_1^{-1}(a_1 - a_1^3)$. This process can be continued indefinitely, and we never run into trouble, because a_1 has infinite order, so we never have $a_1 - a_1^n = 0$. □

Different methods by Eakin and Sathaye treat certain cases where a_1 has finite order. In the following theorem, the circle group is the group of automorphisms of the form $\sigma(Z) = \zeta Z$, where ζ is a root of unity in R.

Theorem 2.2.5 ([E-S])**.** *Let A be an integral domain containing the rational numbers, $\mathbb{Q}$, and suppose that G is a torsion subgroup of the group of automorphisms $Aut_A A[\![X]\!]$. Then G is conjugate to a subgroup of the circle group in $Aut_A A[\![X]\!]$.* □

2.3 Finite Order Automorphisms

So far we have not used the assumption that σ has finite order. This is quite a strong assumption as we shall see in some of the lemmas and theorems below. In this section we shall make the assumption that σ has finite order throughout.

We start with two preliminary lemmas. Both are easily obtained by induction.

Lemma 2.3.1. *If $\sigma(Z) \equiv a_0 Z \pmod{Z^2}$, then $\sigma^t(Z) \equiv a_0^t Z \pmod{Z^2}$.*

Proof. If $\sigma^{t-1}(Z) \equiv a_0^{t-1} Z \pmod{Z^2}$, then

$$\begin{aligned} \sigma^t(Z) &\equiv \sigma(a_0^{t-1} Z) \pmod{Z^2} \\ &\equiv a_0^t Z \pmod{Z^2}. \end{aligned}$$

□

Lemma 2.3.2. *If* $\sigma(Z) \equiv Z + cZ^m \pmod{Z^{m+1}}$, *then* $\sigma^t(Z) \equiv Z + ctZ^m \pmod{Z^{m+1}}$.

Proof. If $\sigma^{t-1}(Z) \equiv Z + (t-1)cZ^m \pmod{Z^{m+1}}$, then

$$\begin{aligned} \sigma^t(Z) &\equiv \sigma(Z + (t-1)cZ^m) \pmod{Z^{m+1}} \\ &\equiv (Z + cZ^m) + (t-1)c(Z + cZ^m)^m \pmod{Z^{m+1}} \\ &\equiv Z + tcZ^m \pmod{Z^{m+1}}. \end{aligned}$$

□

Let us now state a few facts about finite order automorphisms in $\mathrm{Aut}_R R[\![Z]\!]$, where again R is a discrete valuation ring. Note that some of the results in the lemma below may require us to replace R with a finite extension of itself. This has to do with the *fixed points* of an automorphism, which we would like to be contained in R. This is described in Chapter 3.

Denote the identity automorphism of $R[\![Z]\!]$ by $\mathbf{1}$ and the identity automorphism of $k[\![z]\!]$ by $\bar{\mathbf{1}}$.

Lemma 2.3.3 ([G-M1],[G])**.** *Suppose that* σ *is an automorphism in* $Aut_R R[\![Z]\!]$ *of finite order* n. *The following hold over some finite extension of* R.

(a) *If* $\sigma(Z) \equiv Z \pmod{Z^2}$, *then* $\sigma = \mathbf{1}$.

(b) *If* $\Psi(\sigma) \neq \bar{\mathbf{1}}$, *then we may write*

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

where ζ *is a primitive* n*-th root of unity.*

(c) *Call an automorphism* σ linearizable *if there exists an automorphism* $\tau \in Aut_R R[\![Z]\!]$ *such that* $\tau \circ \sigma \circ \tau^{-1}(Z) = a_0 Z$ *for some* $a_0 \in R^\times$. *If* n *is relatively prime to the characteristic* p *of* $k = R/(\pi)$, *then* σ *is linearizable.*

(d) *If $n = p^r$ for some positive integer r and $\Psi(\sigma) \neq \bar{\mathbf{1}}$, then σ is not linearizable.*

(e) *Suppose that $\bar{\sigma}$ is an automorphism of $k[\![z]\!]$ of order n, prime to p. Then we can lift $\bar{\sigma}$ to an automorphism σ of $R[\![Z]\!]$ of order n.*

(f) *Suppose that $\bar{\sigma} \in Aut_k k[\![z]\!]$ has order $n = ep^r$ where e is prime to p. Suppose further that we are always able to lift automorphisms of order p^r. Then we may lift $\bar{\sigma}$ to an automorphism σ of $R[\![Z]\!]$ of order n.*

Remark. As we mentioned in section 1.3, (e) essentially solves the lifting problem for automorphisms of order prime to the characteristic, while (f) reduces all the other cases to the problem of lifting order p^r automorphisms.

Proof. (a) Choose m and c so that $\sigma(Z) \equiv Z + cZ^m \pmod{Z^{m+1}}$ where $c \neq 0$. Then $\sigma^n(Z) \equiv Z + ncZ^m \pmod{Z^{m+1}}$ by lemma 2.3.2. Since $nc \neq 0$, we conclude that σ cannot have order n.

(b) This will be proved in section 3.1 with the help of fixed points.

(c) If $n \geq 2$, then $\Psi(\sigma) \neq \bar{\mathbf{1}}$ so we may write $\sigma(Z) = \zeta Z(1 + a_1 Z + a_2 Z^2 + \cdots)$, where ζ is a primitive n-th root of unity. Construct an endomorphism

$$\tau(Z) = Z + \zeta^{-1}\sigma(Z) + \zeta^{-2}\sigma^2(Z) + \cdots + \zeta^{-n+1}\sigma^{n-1}(Z)$$

of $R[\![Z]\!]$. It is clear that $\sigma(\tau(Z)) = \zeta\tau(Z)$ which would imply that $\tau^{-1}\sigma\tau(Z) = \zeta Z$ if we knew that τ was actually an automorphism. One may easily compute that $\tau(Z) \equiv nZ \pmod{Z^2}$ and n is invertible in R, since it is not divisible by p. Hence τ is indeed an automorphism.

It is important to note that the same proof also works when working over k rather than R. We shall use this fact in (e).

(d) If σ was linearizable, we would have $\tau\sigma\tau^{-1} = \zeta Z$ for some primitive p^r-th root of unity ζ. But then, under reduction modulo π, we obtain that $\Psi(\tau)\Psi(\sigma)\Psi(\tau)^{-1} = \Psi(\tau\sigma\tau^{-1})$ is the identity. This implies that $\Psi(\sigma)$ is also the identity. Contradiction.

(e) By (c), we may find $\bar{\tau}$ such that $\bar{\tau}\bar{\sigma}\bar{\tau}^{-1}(z) = \bar{\zeta}z$ where $\bar{\zeta}$ is a primitive n-th root of unity in k. We may lift this conjugate to $\omega(Z) = \zeta Z$, where ζ is a primitive n-th root of unity in R. We may also lift $\bar{\tau}$ in any way and determine σ as $\tau^{-1}\omega\tau(Z)$. Since Ψ is a homomorphism and since $\Psi(\omega) = \bar{\tau}\bar{\sigma}\bar{\tau}^{-1}$, we have that $\Psi(\sigma) = \Psi(\tau^{-1})\Psi(\omega)\Psi(\tau) = \bar{\tau}^{-1}(\bar{\tau}\bar{\sigma}\bar{\tau}^{-1})\bar{\tau} = \bar{\sigma}$.

(f) Suppose that $\bar{\sigma}$ has order $n = ep^r$, where e is prime to p. Then the automorphism $\bar{\sigma}^{p^r}$ has order e, and hence can be linearized. Choose $\bar{\tau}$ so that $\bar{\tau}\bar{\sigma}^{p^r}\bar{\tau}^{-1}(z) = \bar{\zeta}_e z$, where $\bar{\zeta}_e$ is a primitive e-th root of unity in k. Write $\bar{\alpha} = \bar{\tau}\bar{\sigma}^{p^r}\bar{\tau}^{-1}$ for this automorphism.

Set $t = z\bar{\alpha}(z)\cdots\bar{\alpha}^{e-1}(z) = (\bar{\zeta}_e^{(e-1)/2}z)^e$. It is well known that the fixed ring of $k[\![z]\!]$ under the action of $\bar{\alpha}$ is $k[\![t]\!] = k[\![z]\!]^{\langle\bar{\alpha}\rangle}$. Hence, the automorphism $\bar{\sigma}|_{k[\![t]\!]}$ ($\bar{\sigma}$ restricted to the subring $k[\![t]\!]$) has order p^r. By our assumption, we may lift this to an order p^r automorphism σ of $R[\![Z]\!]$. We may also set

$$\begin{aligned}\bar{\sigma}(t) &= t(1 + \bar{a}_1 t + \cdots)\\ \sigma(T) &= \zeta_{p^r} T(1 + a_1 T + \cdots),\end{aligned}$$

where ζ_{p^r} is a primitive p^r-th root of unity in R. Let ζ_e be a primitive e-th root of unity in R, lifting the root of unity $\bar{\zeta}_e$ from k to R. Setting $X = \zeta_e^{(e-1)/2}Z$ (so that $T = X^e$) and $x = \bar{\zeta}_e^{(e-1)/2}z$ (so that $t = x^e$), we rewrite this as

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

so that

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

In the same way, we would like to extend $\sigma(X^e) = \zeta_{p^r} X^e(1+a_1X^e+\cdots)$ on $R[\![T]\!]$ to the automorphism $\sigma(X) = \zeta_{ep^r} X(1 + a_1X^e + \cdots)^{1/e}$ on $R[\![X]\!] = R[\![Z]\!]$. If this is possible, it is clear that $\Psi(\sigma) = \bar{\sigma}$. We only need to show that σ has order ep^r.

To show this, we first compute $\sigma(T)$ by iteration. Recall that $\sigma(T) = \zeta_{p^r} T(1+a_1T+\cdots)$ as an automorphism of $R[\![T]\!]$ and has order p^r. Set $B := 1 + a_1T + \cdots$.

$$\begin{aligned}
\sigma(T) &= \zeta_{p^r} TB \\
\sigma^2(T) &= \zeta_{p^r}^2 TB\sigma(B) \\
\sigma^3(T) &= \zeta_{p^r}^3 TB\sigma(B)\sigma^2(B) \\
&\vdots \\
\sigma^{p^r}(T) &= \zeta_{p^r}^{p^r} TB\sigma(B)\cdots\sigma^{p^r-1}(B) \\
&= T\big(B\sigma(B)\cdots\sigma^{p^r-1}(B)\big).
\end{aligned}$$

Since σ has order p^r over $R[\![T]\!]$, we conclude that $B\sigma(B)\cdots\sigma^{p^r-1}(B) = 1$. Now we compute $\sigma^{ep^r}(Z)$ in the same way.

$$\begin{aligned}
\sigma(Z) &= \zeta_{ep^r} ZB^{1/e} \\
\sigma^2(Z) &= \zeta_{ep^r}^2 ZB^{1/e}\sigma(B^{1/e}) \\
&\vdots \\
\sigma^{ep^r}(Z) &= \zeta_{ep^r}^{ep^r} ZB^{1/e}\sigma(B^{1/e})\cdots\sigma^{ep^r-1}(B^{1/e}) \\
&= Z\big(B\sigma(B)\cdots\sigma^{ep^r-1}(B)\big)^{1/e}.
\end{aligned}$$

We claim that this last expression is equal to Z, implying that σ has order $n = ep^r$. Recall that we have just shown that $B\sigma(B)\cdots\sigma^{p^r-1}(B) = 1$. Hence also $\sigma^{tp^r}\big(B\sigma(B)\cdots\sigma^{p^r-1}(B)\big) = \sigma^{tp^r}(1) = 1$, for $t = 1, 2, \ldots, e-1$. This implies that

$$\begin{aligned}
B\sigma(B)\cdots\sigma^{ep^r-1}(B) &= \big(B\sigma(B)\cdots\sigma^{p^r-1}(B)\big) \times \cdots \times \\
&\qquad \big(\sigma^{(e-1)p^r} B\sigma^{(e-1)p^r+1}(B)\cdots\sigma^{ep^r-1}(B)\big) \\
&= \big(B\sigma(B)\cdots\sigma^{p^r-1}(B)\big)^e.
\end{aligned}$$

□

The local Oort-Sekiguchi conjecture asks for a lifting of an order q automorphism of $k[\![z]\!]$ to an order q automorphism of $R[\![Z]\!]$. Green proved that it is enough to lift this automorphism to a finite order automorphism, rather than one of exact order q.

Theorem 2.3.4 ([G])**.** *Suppose that $\bar{\sigma}$ is an order p^r automorphism of $k[\![z]\!]$. Then the following conditions are equivalent:*

(i) There exists $\sigma \in Aut_R R[\![Z]\!]$ such that $\Psi(\sigma) = \bar{\sigma}$ and σ has finite order.

(ii) There exists $\tau \in Aut_R R[\![Z]\!]$ such that $\Psi(\tau) = \bar{\sigma}$ and τ has order p^r.

Proof. The fact that (ii) implies (i) is obvious. So suppose that the automorphism σ described in (i) has order ep^m, where p does not divide e. First we get rid of the e and show that $r \leq m$. Let k and l be integers such that $ke + lp^r = 1$ and set $\omega = \sigma^{ke}$ so that $\omega^{p^m} = \mathbf{1}$. We also have $\Psi(\omega) = \Psi(\sigma^{ke}) = \bar{\sigma}^{1-lp^r} = \bar{\sigma}$, since $\bar{\sigma}$ has order p^r. Hence ω is an automorphism of order p^m that reduces to $\bar{\sigma}$. This also shows that $r \leq m$, since otherwise $\bar{\sigma}^{p^m} = \bar{\mathbf{1}}$, contradicting the fact that $\bar{\sigma}$ has order p^r.

Next, we wish to show how to construct an automorphism τ from ω such that τ has exact order p^r and reduces to $\bar{\sigma}$. Denote by

$$R[\![T]\!] = R[\![Z]\!]^{\langle\omega\rangle} \text{ and } R[\![T_r]\!] = R[\![Z]\!]^{\langle\omega^{p^r}\rangle}$$

the fixed subrings of $R[\![Z]\!]$ under the groups generated by ω and ω^{p^r}, respectively. We know that

$$T = \prod_{i=1}^{p^m} \omega^i(Z) \text{ and } \qquad T_r = \prod_{j=1}^{p^{m-r}} \omega^{jp^r}(Z).$$

We would now like to see what happens to T and T_r under the reduction map $\rho : R[\![Z]\!] \to k[\![z]\!]$. We know that $\Psi(\omega) = \bar{\sigma}$ and hence has order p^r.

Hence $\Psi(\omega^{jp^r})$ is the identity for every j and hence $\rho(T_r) = z^{p^{m-r}}$.

$$\begin{aligned}
\rho(T) &= \prod_{i=1}^{p^m} \Psi\big(\omega^i(Z)\big) \\
&= \prod_{j=0}^{p^{m-r}-1} \Big(\prod_{i=1}^{p^r} \bar{\sigma}^{jp^r+i}(z)\Big) \\
&= \prod_{j=0}^{p^{m-r}-1} \Big(\prod_{i=1}^{p^r} \bar{\sigma}^{i}(z)\Big), \quad \text{since } \bar{\sigma} \text{ has order } p^r \\
&= \Big(\prod_{i=1}^{p^r} \bar{\sigma}^{i}(z)\Big)^{p^{m-r}} \\
&= \prod_{i=1}^{p^r} \bar{\sigma}^{i}(z^{p^{m-r}}).
\end{aligned}$$

Hence, we get the following diagram of ring extensions, both over R and over k after reducing modulo π.

$$\begin{array}{ccc}
R[\![Z]\!] & \longrightarrow & k[\![z]\!] \\
\big| & & \big| \\
R[\![T_r]\!] & \longrightarrow & k[\![t_r]\!] = k[\![z^{p^{m-r}}]\!] \\
\big| & & \big| \\
R[\![T]\!] & \longrightarrow & k[\![t]\!]
\end{array}$$

We are especially interested in the extension $k[\![z]\!]$ over $k[\![t_r]\!] = k[\![z^{p^{m-r}}]\!]$. This extension is of degree p^{m-r} in characteristic p. Hence it is purely insep-

arable. If we set

$$\bar{\sigma}(z) = z(1 + a_1 z + \cdots)$$

then we may compute $\bar{\sigma}(t_r)$, which defines the restriction of $\bar{\sigma}$ to $k[\![t_r]\!]$, by

$$\begin{aligned}
\bar{\sigma}(t_r) &= \bar{\sigma}(z^{p^{m-r}}) \\
&= \bar{\sigma}(z)^{p^{m-r}} \\
&= z^{p^{m-r}}(1 + a_1 z + a_2 z^2 + \cdots)^{p^{m-r}} \\
&= z^{p^{m-r}}(1 + a_1 z^{p^{m-r}} + a_2 z^{2p^{m-r}} + \cdots) \\
&= t_r(1 + a_1 t_r + a_2 t_r^2 + \cdots),
\end{aligned}$$

which is exactly $\bar{\sigma}$, but with z replaced by t_r. So, the restriction $\omega|_{R[\![T_r]\!]}$ of ω to $R[\![T_r]\!]$ has order p^r and reduces to $\bar{\sigma}|_{k[\![t_r]\!]}$ (the restriction of $\bar{\sigma}$ to $k[\![t_r]\!]$) modulo π. But this reduction is exactly $\bar{\sigma}$, just with z replaced by t_r.

Hence, the restriction $\omega|_{R[\![T_r]\!]}$ is a suitable candidate to satisfy the properties of (a). □

Chapter 3

The Geometry of Automorphisms of Power Series Rings over a DVR

3.1 The Fixed Points of an Automorphism

In this section we would like to view the power series ring $R[\![Z]\!]$ in a geometric way. In this way we may obtain some information about the automorphsims, e.g. the number of *fixed points* of an automorphism. Firstly we would like to describe the *p-adic open disc* $D = \mathrm{Spec}(R[\![Z]\!])$. We will use the Weierstrass Preparation Theorem throughout this section, so we state it here for reference.

Theorem 3.1.1 (Weierstrass Preparation Theorem)**.** *Suppose that* $f = a_0 + a_1 Z + a_2 Z^2 + \cdots$ *is an element of the power series ring* $R[\![Z]\!]$*. Suppose further that* m *is the smallest positive integer for which* $a_m \notin \pi R$*, i.e.* $a_0, a_1, \ldots, a_{m-1} \in \pi R$*, but* $a_m \notin \pi R$*. Then* $f = g \cdot u$ *where* u *is a unit in* $R[\![Z]\!]$ *and* g *is a monic polynomial* (*leading coefficient equal to 1*) *of degree* m *in* $R[Z]$*. Furthermore,* g *is a* distinguished polynomial*, i.e. all the coefficients of* g*, except the leading coefficient, are in the maximal ideal* πR*.*

Proof. [La1] IV.9. □

Lemma 3.1.2. *The ring $R[\![Z]\!]$ has a unique maximal ideal (Z, π) and apart from the zero ideal, the other prime ideals are of height one. These are the ideals (π) and $(f(Z))$ where $f(Z)$ is a distinguished polynomial.*

Proof. Suppose that $\mathfrak{p}$ is a prime ideal of $R[\![Z]\!]$. Then $\mathfrak{p} \cap R$ is a prime ideal of R, hence must be equal to either (π) or (0). We distinguish the two cases. **Case 1**: $\mathfrak{p} \cap R = (0)$. The ideal $\mathfrak{p}$ contains only power series in $R[\![Z]\!]$. But $R[\![Z]\!]$ is a unique factorization domain, implying that either $\mathfrak{p} = (0)$ or $\mathfrak{p} = (f)$ for some power series $f \in R[\![Z]\!]$. By the Weierstrass Preparation Theorem we may factorize $f = g \cdot u$ where g is a polynomial and u is a unit. Then $(f) = (g)$ and $\mathfrak{p} = (g)$ where g is a distinguisehd polynomial.
Case 2: $\mathfrak{p} \cap R = (\pi)$. We may use the reduction map $\rho : R[\![Z]\!] \to k[\![z]\!]$ to aid us in describing $\mathfrak{p}$. The image of $\mathfrak{p}$ under ρ is a prime ideal of the codomain $k[\![z]\!]$, hence equal to either (0) or (Z). We conclude that either $\mathfrak{p} = (\pi)$ or $\mathfrak{p} = (\pi, Z)$, the maximal ideal of $R[\![Z]\!]$. □

Note that D is a scheme over $\mathrm{Spec}(R)$ so the first thing we do is to describe its fibres. Its special fibre is simply $D_k = D \times_R \mathrm{Spec}(k) = \mathrm{Spec}(k[\![z]\!])$ while its generic fibre is given by $D_K = D \times_R \mathrm{Spec}(K) = \mathrm{Spec}(B_K)$ where $B_K = R[\![Z]\!] \otimes_R K$.

We noted earlier that all the automorphisms of $R[\![Z]\!]$ are of the form $\sigma(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots$ where $a_0 \in \pi R$ and $a_1 \in R^\times$. We know (from the theory of schemes) that such an automorphism induces an automorphism $\tilde{\sigma} : D \to D$ and that this automorphism is given by $\tilde{\sigma}(P) = \sigma^{-1}(P)$. On the left hand side of this formula, P is a point in D, while on the right hand side it is an ideal of $R[\![Z]\!]$.

If $\tilde{\sigma}$ has finite order, one may form the quotient of the disc D by the group generated by $\tilde{\sigma}$. In particular, if $\tilde{\sigma}$ has prime order p, the quotient map $D \to D/\langle\tilde{\sigma}\rangle$ is ramified exactly at the points of D that are fixed by $\tilde{\sigma}$.

This motivates us to study the fixed points of $\tilde{\sigma}$.

An effective description of the fixed points of $\tilde{\sigma}$ depends on considering the scheme $\bar{D} = D \times_R \mathrm{Spec}(R^{\mathrm{alg}}) = \mathrm{Spec}(R^{\mathrm{alg}}[\![Z]\!])$. The points (g) of D split into different points $(Z - \alpha_i)_{1 \leq i \leq m}$ according to the factorization $g = (Z - \alpha_1)(Z - \alpha_2) \cdots (Z - \alpha_m)$ of g over R^{alg}. It will be easier to say which of these *geometric points* $(Z - \alpha)$ are fixed by $\tilde{\sigma}$.

Note that the α in these geometric points are not necessarily elements of πR, but are elements of the maximal ideal $\tilde{\pi}$ of R^{alg}. Hence they have a positive, but possibly non-integral, π-adic valuation.

Lemma 3.1.3. *For a rational geometric point $P = (Z - Z_0)$, $Z_0 \in \tilde{\pi}$, we have*

$$\tilde{\sigma}(P) = (Z - \tilde{Z}_0),$$

where $\tilde{Z}_0 = a_0 + a_1 Z_0 + a_2 Z_0^2 + \cdots$.

Proof. We need to prove that $\sigma^{-1}\big((Z - Z_0)\big) = (Z - \tilde{Z}_0)$ which, since σ is an automorphism, is equivalent to $\sigma\big((Z - \tilde{Z}_0)\big) = (Z - Z_0)$. But

$$\begin{aligned} \sigma\big((Z - \tilde{Z}_0)\big) &= (\sigma(Z) - \tilde{Z}_0) \\ &= (a_0 + a_1 Z + a_2 Z^2 + \cdots - a_0 - a_1 Z_0 - a_2 Z_0^2 - \cdots) \\ &= ((Z - Z_0)(a_1 + a_2(Z + Z_0) + \cdots)). \end{aligned}$$

The factor $(a_1 + a_2(Z + Z_0) + \cdots)$ is a unit in $R[\![Z]\!]$, since a_1 is a unit in R and $Z_0 \in \tilde{\pi}$. Therefore

$$\sigma\big((Z - \tilde{Z}_0)\big) = (Z - Z_0)$$

as ideals. □

Proposition 3.1.4. *A height one geometric point P is a fixed point of $\tilde{\sigma}$ if and only if $P \supseteq (\sigma(Z) - Z)$ or $P = (\pi)$.*

Proof. Since σ fixes R, it is clear that the point (π) is fixed. Let $P = (Z - Z_0)$ as in the previous lemma. Suppose that $\tilde{\sigma}(P) = P$. Then $\sigma^{-1}(P) = P$ as ideals of $R^{\mathrm{alg}}[\![Z]\!]$. From the previous lemma we may then conclude that $\tilde{Z}_0 = Z_0$. This is the same as saying that Z_0 is a root of the equation $\sigma(Z) - Z = 0$, which is equivalent to $P \supseteq (\sigma(Z) - Z)$.

Conversely, suppose that $P \supseteq (\sigma(Z) - Z)$. By the Weierstrass Preparation Theorem $(\sigma(Z) - Z) = (g)$. It is clear that the ideal $(Z - Z_0)$ contains the ideal (g) since $Z - Z_0$ divides g. This is the same as saying that Z_0 is a root of g which, in turn, divides $(\sigma(Z) - Z)$. Hence $\tilde{Z}_0 = Z_0$ and P is a fixed point. □

Remark. There is a corresponding result for the fixed points of D. A point P is a fixed point of $\tilde{\sigma}$ if and only if $P \supseteq (\sigma(Z) - Z)$. In this case we factorize the polynomial g from the Weierstrass Preparation Theorem over R as $g = g_1 g_2 \cdots g_r$. It is clear that the ideals (g_i) are fixed points of $\tilde{\sigma}$ and that these are the only fixed points.

Corollary. *The fixed points of $\tilde{\sigma}$ are exactly the points (0), (π), (Z, π) and those P for which $P \supseteq (\sigma(Z) - Z)$.* □

The Weierstrass Preparation Theorem allows us to factorize the power series $\sigma(Z) - Z$ into a polynomial times a unit in the ring $R[\![Z]\!]$. The unit can never be zero, so the only fixed points are the prime ideals that divide the distinguished polynomial. Hence we may count the number of geometric fixed points, i.e. the number of fixed points when passing to $R^{\mathrm{alg}}[\![Z]\!]$, the algebraic integers lying over $R[\![Z]\!]$. Next, we explain how this is done.

Let $\sigma(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots$ and set $f(Z) = a_0 + (a_1 - 1)Z + a_2 Z^2 + a_3 Z^3 + \cdots$. Suppose that m is the least positive integer for which $a_m \in R^\times$ (or that $m = 1$ if $a_1 - 1 \in R^\times$). We may then factorize $f(Z) = g(Z)u(Z)$ where $u(Z)$ is a unit in $R[\![Z]\!]$ and $g(Z)$ is a distinguished polynomial of

degree m. The polynomial $g(Z)$ then factorizes into m linear factors when considered over R^{alg}. Note that these factors are all of the form $Z - \alpha$ where $\alpha \in \widetilde{\pi}$. Let one of these fixed points be given by $(Z - Z_0)$. If we conjugate the automorphism σ with the automorphism τ given by $\tau(Z) = Z + Z_0$, we find that the point (Z) is a fixed point. This means that $\tau \circ \sigma \circ \tau^{-1}(Z) = b_1 Z + b_2 Z^2 + \cdots$.

We assumed above that σ indeed does have a fixed point. We should spend some time to dismiss the case when σ does not have a fixed point. We saw above that for σ to be an automorphism, we need $a_0 \in \pi R$ and $a_1 \in R^\times$. So, if σ has no fixed points, we need all the coefficients of $f(Z)$ to be in πR. This would mean that under reduction modulo π we obtain $f(Z) \equiv 0 \pmod{\pi}$, or $\Psi(\sigma) = \bar{\mathbf{1}}$. This contradicts the smoothness we require in a lifting of such an automorphism. We thus pay no further regard to this case.

Assuming that σ has finite order, we may prove that the m fixed points are all distinct.

Lemma 3.1.5. *Suppose that σ (not equal to the identity) has finite order and that $g(Z) = (Z - Z_1)(Z - Z_2) \cdots (Z - Z_m)$, where $g(Z)$ is the distinguished polynomial defined above. Then the Z_i are all distinct.*

Proof. Assume for a contradiction that two of them are equal. Without loss of generality let $Z_1 = Z_2$. As above we may then conjugate σ with the automorphism $\tau(Z) = Z + Z_1$ to obtain $\tau\sigma\tau^{-1}(Z) = \tau\sigma(Z - Z_1) = \tau(\sigma(Z)) - Z_1 = \tau(f(Z) + Z) - Z_1 = \tau(g(Z)u(Z)) + \tau(Z) - Z_1 = g(Z + Z_1)u(Z + Z_1) + Z$. But, by our assumption, $g(Z + Z_1)$ has a double root $Z = 0$, so that $\tau\sigma\tau^{-1} \equiv Z \pmod{Z^2}$. Since the conjugate $\tau\sigma\tau^{-1}$ has the same order as the automorphism σ, i.e. finite order, we conclude by Lemma 2.3.3(a) that $\tau\sigma\tau^{-1}$ is the identity, and hence that σ is the identity. □

Armed with the theory of fixed points of automorphisms, we may now prove Lemma 2.3.3(b).

Proof. (Completion of Lemma 2.3.3(b)) We may replace R by a finite ex-

tension of itself. We wish to replace it with the finite extension obtained by adjoining the fixed points to it. We may then conjugate σ as before and assume that (Z) is a fixed point of $\tilde{\sigma}$. Then $\sigma(Z) = a_1 Z + a_2 Z^2 + \cdots$.

First suppose that σ has order p. Then, by Lemma 2.3.1, we find that $\sigma^p(Z) \equiv a_1^p Z \pmod{Z^2}$. Since σ has order p, we require a_1 to be a p-th root of unity. We also need $a_1 \neq 1$, since otherwise $\sigma(Z) \equiv Z \pmod{Z^2}$, whence σ is the identity by Lemma 2.3.3(a). Hence a_1 is a primitive p-th root of unity.

Now suppose that σ has order p^r. Similarly $\sigma^{p^r}(Z) \equiv a_1^{p^r} Z \pmod{Z^2}$, so a_1 must be a p^r-th root of unity. Also, if a_1 has order p^s for $s < r$, then $\sigma^{p^s}(Z) \equiv Z \pmod{Z^2}$ and σ actually has order p^s. Hence a_1 must be a primitive p^r-th root of unity. □

3.2 Equidistant Geometry

We shall assume in this section that σ is an automorphism of $R[\![Z]\!]$ as in the previous section, i.e. we shall assume that it is of the form

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

This means that the induced automorphism $\tilde{\sigma}$ of D has the point (Z) as a fixed point. Suppose further that it has exactly m other fixed points, meaning that $a_1, a_2, \ldots, a_{m-1} \in \pi R$ and that $a_m \in R^\times$. We will denote the fixed points of $\tilde{\sigma}$ by $F_{\tilde{\sigma}} := \{(Z-\alpha_0), (Z-\alpha_1), (Z-\alpha_2), \ldots, (Z-\alpha_m)\}$, using the convention that $\alpha_0 = 0$.

One interesting thing one might do is to study how these α_i are distributed. To do this we shall look at the $\alpha_1, \alpha_2, \ldots, \alpha_m$ as elements of R^{alg}. Then we may speak of the distance between α_i and α_j. We define the distance between the two points $(Z - \alpha_i)$ and $(Z - \alpha_j)$ of D as the distance between the elements α_i and α_j of R^{alg}. This distance is, of course, just the π-adic absolute value of the difference $\alpha_i - \alpha_j$.

Next, we wish to explain what is meant by the term *equidistant* in the title of this section. Suppose that $B = \{\beta_1, \beta_2, \ldots, \beta_r\}$ is a subset of the set $F_\sigma := \{\alpha_0, \alpha_1, \ldots, \alpha_m\}$. We shall say that B is an *equidistant set* if the absolute values $|\beta_i - \beta_j|_\pi$ are all equal.

In this section we shall give results that under certain conditions the whole set F_σ is equidistant and describe a certain subset of F_σ which is always equidistant.

Recall, that by conjugating the automorphism σ by some τ, we may "move the fixed points around". For example, let $\omega = \tau\sigma\tau^{-1}$ be the conjugate of σ by τ. Then, if $\tau(Z) = Z + Z_0$ and $\tilde{\sigma}$ has the fixed points $(Z - \alpha_0), \ldots, (Z - \alpha_m)$, then $\tilde{\omega}$ has fixed points $(Z + Z_0 - \alpha_0), \ldots, (Z + Z_0 - \alpha_m)$. We wish to choose $Z_0 = \alpha_i$ for a suitable i. After that we wish to relabel the α_i in an appropriate way.

Let us first describe how we wish to choose Z_0. Among the α_i there are various different distances $|\alpha_i - \alpha_j|_\pi$. We are particularly interested in the minimum of these values over all $i \neq j$. If (α_i, α_j) is a pair that attains this minimum bound, we may set $Z_0 = \alpha_i$. In the end it won't matter whether we take α_i or α_j or which pair attaining this minimum we take. We just take any one — e.g. the one with lowest index. The set $\{\alpha_0 - Z_0, \alpha_1 - Z_0, \ldots, \alpha_m - Z_0\}$ represent a set of $m + 1$ fixed points. We may relabel this set as $\{\alpha_0, \alpha_1, \ldots, \alpha_m\}$, where again $\alpha_0 = 0$. (Hence they are not necessarily relabelled in the same order.)

Next we arrange the α_i, $i \geq 1$ in such a way that the quantities $|\alpha_i|_\pi$ are non-decreasing. Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_t$ are the α_i that are the closest to $\alpha_0 = 0$, i.e. suppose that $|\alpha_i|_\pi = |\alpha_1|_\pi$ for $i = 1, 2, \ldots, t$. Call the set $I = \{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_t\}$ the *inner circle* of fixed points.

Theorem 3.2.1 ([G-M2])**.** *The inner circle of automorphism are equidistant. That is* $|\alpha_i - \alpha_j|_\pi = |\alpha_1|_\pi$ *for all* i, j *such that* $1 \leq i < j \leq t$.

Proof. By the (strong) triangle inequality $|\alpha_i - \alpha_j|_\pi \leq \max(|\alpha_i|_\pi, |\alpha_j|_\pi) = |\alpha_1|_\pi$. So suppose, for a contradiction, that $|\alpha_i - \alpha_j|_\pi < |\alpha_1|_\pi$. This is

impossible, because of the way we chose α_0. If $|\alpha_i - \alpha_j|_\pi < |\alpha_1|_\pi$, then either α_i or α_j must have been chosen as Z_0. □

Theorem 3.2.2 ([G-M2]). *If σ has prime order and the number of fixed points is less than p, then the whole set F_σ is equidistant.* □

3.3 The Approach via Differents of Ring Extensions

Suppose that we are given a power series ring $k[\![z]\!]$ over an algebraically closed field of characteristic p and one of its automorphisms $\bar{\sigma}$ of order n. We compute the fixed ring of $k[\![z]\!]$ under the action of $\bar{\sigma}$ to be $k[\![z]\!]^{\langle\bar{\sigma}\rangle} = k[\![t]\!]$, where $t = z\bar{\sigma}(z)\cdots\bar{\sigma}(z)^{n-1}$. Similarly, if σ is an order n automorphism of the power series ring over R (a discrete valuation ring with residue field k), the fixed ring of $R[\![Z]\!]$ under the action of σ will be $R[\![T]\!]$ where $T = Z\sigma(Z)\cdots\sigma^{n-1}(Z)$.

Forgetting about this situation for a moment, we wish to approach this situation from a different angle. We wish to study the situation in the diagram below. Suppose that we have constructed the respective extensions $R[\![Z]\!]/R[\![T]\!]$ and $k[\![z]\!]/k[\![t]\!]$ and the reduction maps $R[\![Z]\!] \to k[\![z]\!]$ and $R[\![T]\!] \to k[\![t]\!]$.

$$\begin{array}{ccc} R[\![Z]\!] & \longrightarrow & k[\![z]\!] \\ \downarrow & & \downarrow \\ R[\![T]\!] & \longrightarrow & k[\![t]\!] \end{array}$$

There are a few problems with this point of view. Under reduction the extension $k[\![z]\!]/k[\![t]\!]$ might not be of the same degree as the extension $R[\![Z]\!]/R[\![T]\!]$. More precisely, our philosophy is this. If we start with the extension $k[\![z]\!]/k[\![t]\!]$ defined by the equation $t = \bar{f}(z)$, we wish to lift it to an

extension $R[\![Z]\!]/R[\![T]\!]$, defined by an equation $T = f(Z)$. We require that

- the polynomial f reduces to the polynomial $\bar{f}$ modulo π,
- the reduction is *good*, meaning that $\bar{f}$ does not have any repeated roots, and
- the extension $R[\![Z]\!]/R[\![T]\!]$ is galois of the same order as the extension $k[\![z]\!]/k[\![t]\!]$.

Luckily, we have a rather simple way of determining whether good reduction occurs. This involves a simple calculation of the different of the extensions $k[\![z]\!]/k[\![t]\!]$ and $R[\![Z]\!]/R[\![T]\!]$. There are two separate differents in the latter extension. We may speak of the special different, which is the different in the extension in the special fibre, and the generic different, which is the different in the extension in the generic fibre. Since the special different is exactly the different of $k[\![z]\!]/k[\![t]\!]$, we would like to compare it to the generic different in the extension $R[\![Z]\!]/R[\![T]\!]$.

Proposition 3.3.1. *Let σ be an order n automorphism of $R[\![Z]\!]$ and suppose that its reduction $\bar{\sigma}$ is an order n automorphism of $k[\![z]\!]$. Then the degree of the special different d_s equals the degree of the generic different d_η in the extension $R[\![Z]\!]/R[\![T]\!]$.*

Proof. Let us first compute the generic different. The relevant extension is B_K/A_K where $B_K = R[\![Z]\!] \otimes_R K$ and $A_K = R[\![T]\!] \otimes_R K$. Since this extension is cyclic with galois group generated by σ, the minimum polynomial of Z over $R[\![T]\!]$ is

$$f(X) = \prod_{i=0}^{n-1} (X - \sigma^i(Z)).$$

Since $R[\![Z]\!]$ is generated by the element Z, the different is the ideal generated by the derivative of this polynomial, evaluated at Z.

$$f'(X)|_{X=Z} = \prod_{i=1}^{n-1} (Z - \sigma^i(Z))$$

By the Weierstrass Preparation Theorem, this polynomial may be factored as $p(Z)u(Z)$, where p is a polynomial and u is a unit. Hence, the different is the ideal generated by $p(Z)$. We conclude that the degree of the different is equal to the degree of the polynomial $p(Z)$.

We determine the special different similarly to how we determined the generic different. If we let

$$\bar{f}(X) = \prod_{i=0}^{n-1}(X - \bar{\sigma}^i(z)),$$

then the different is the ideal generated by

$$\bar{f}'(X)|_{X=z} = \prod_{i=1}^{n-1}(z - \bar{\sigma}^i(z)).$$

But this is just the polynomial $f'(X)|_{X=Z}$ reduced modulo π. Hence the special different is the ideal generated by the polynomial $p(\bar{z})$ which is $p(Z)$ reduced modulo π. But $p(Z)$ has all its coefficients except the leading coefficient in the maximal ideal π. Hence the special different is (z^m) which has degree m. □

The converse is a theorem of Kato. In this theorem $d_\eta(B/A)$ and $d_s(B/A)$ denote the generic and special differents of the extension B/A. We also denote the residue fields of the local rings A and B by $\bar{A}$ and $\bar{B}$, respectively. Lastly, for any ring C in this theorem, $\tilde{C}$ denotes the normalization of C.

Theorem 3.3.2 ([Ka]). *Suppose that $A \to B$ is a morphism of two dimensional henselian normal local rings A and B with maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_B$. Then*

$$d_\eta(B/A) - d_s(B/A) = 2\delta_k(B) - 2[Quot(B) : Quot(A)]\delta_k(A),$$

where $\delta_k(A)$ (resp. $\delta_k(B)$) is the dimension of the quotient k^{alg} vector space $(\widetilde{\bar{A}})/(\bar{A})$ (resp. $(\widetilde{\bar{B}})/(\bar{B})$). □

Corollary. *If the special and generic differents in the extension $R[\![T]\!] \to R[\![Z]\!]$ are equal then $R[\![Z]\!]$ is integrally closed.*

Proof. If $d_\eta = d_s$ then $\delta_k(R[\![Z]\!]) = [\mathrm{Quot}(R[\![Z]\!]) : \mathrm{Quot}(R[\![T]\!])]\delta_k(R[\![T]\!])$. Since $R[\![T]\!]$ is assumed to be integrally closed, we have $\delta_k(R[\![T]\!]) = 0$, and hence $\delta_k(R[\![Z]\!]) = 0$, which implies that $R[\![Z]\!]$ is integrally closed. □

We may now rephrase what we are trying to do. Given an extension $k[\![z]\!]/k[\![t]\!]$ of degree p^n, we wish to find a galois extension $R[\![Z]\!]/R[\![T]\!]$ of degree p^n which reduces to $k[\![z]\!]/k[\![t]\!]$ and for which $d_\eta = d_s$.

This method has been the most successful in attacking the Oort-Sekiguchi conjecture. For order p or p^2 automorphisms $\bar{\sigma}$ of $k[\![z]\!]$, one may consider the ring extension $k[\![z]\!]/k[\![t]\!]$, where $k[\![t]\!]$ is the fixed ring of $k[\![z]\!]$ under $\bar{\sigma}$. Then one finds an equation for this extension, on which a Kummer-Artin-Schreier deformation is performed to lift it to an equation over the discrete valuation ring R. Then it is proved that this equation gives a galois extension of degree n of some lifting $R[\![T]\!]$ of $k[\![t]\!]$. Finally, differents are calculated to be equal and it is seen that this is indeed a smooth lifting. To date this method constitutes the only progress that has been made using the local interpretation. Many people believe that an attack from a global point of view is more likely to be successful.

Chapter 4

Parametrizing Cyclic Automorphisms of Power Series Rings

In this chapter we start with an automorphism σ of $R[\![Z]\!]$ given by

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

and compute the q-th iterate for $q = p^n$ for some positive integer n. This iterate can be written in the form

$$\sigma^q(Z) = Z(1 + E_1 Z + E_2 Z^2 + \cdots).$$

These polynomials can be used to translate whether σ has order q into certain equations. Throughout the chapter we restrict ourselves to q-th iterates where $q = p^n$. As we mentioned earlier we already know that the lifting problem is solved for the prime to p case, so this is truly what we are interested in.

This approach provides an alternative approach to the lifting problem. So far it has not been successful, but it is also interesting in its own right.

4.1 Parametrizing Cyclic Automorphisms

Suppose that $\sigma(Z) = \zeta Z(1+a_1Z+a_2Z^2+\cdots)$. It is then possible to compute $\sigma^q(Z)$ as a series $Z(E_0 + E_1Z + E_2Z^2 + \cdots)$ where the E_i are all polynomials in the variables $a_1, a_2, \ldots$. Necessary and sufficient conditions for σ to have order dividing q is that $E_0 = 1$ and $E_i = 0$ for all $i \geq 1$. We shall explore the properties of these polynomials in this section.

Example. Let us compute the first few values for E_i when $q = 3$. Set ζ as a primitive third root of unity in R. We shall use the relation $1 + \zeta + \zeta^2 = 0$ quite often to simplify these expressions.

$$\begin{aligned}
\sigma^2(Z) &= \sigma(\zeta Z(1 + a_1Z + a_2Z^2 + a_3Z^3 + \cdots) \\
&= \zeta\sigma(Z)(1 + a_1\sigma(Z) + a_2\sigma(Z)^2 + a_3\sigma(Z)^3\cdots) \\
&= \zeta^2 Z(1 + a_1Z + a_2Z^2 + \cdots)\big(1 + a_1\zeta Z(1 + a_1Z + a_2Z^2 + \cdots) + \\
&\quad a_2\zeta^2Z^2(1 + a_1Z + \cdots)^2 + \cdots\big) \\
&= \zeta^2 Z(1 + a_1Z + a_2Z^2 + \cdots)\big(1 + a_1\zeta Z + (a_1^2\zeta + a_2\zeta^2)Z^2 + \\
&\quad (a_1a_2\zeta + 2a_2a_1\zeta^2 + a_3\zeta^3)Z^3 + \cdots\big) \\
&= \zeta^2 Z(1 - \zeta^2a_1Z + (2a_1^2\zeta - \zeta a_2)Z^2 + (2a_3 + a_1a_2(2\zeta + 3\zeta^2) + a_1^3\zeta)Z^3 + \cdots)
\end{aligned}$$

$$\begin{aligned}
\sigma^3(Z) &= \sigma(\sigma^2(Z)) \\
&= \zeta^2\sigma(Z)\big(1 - a_1\zeta^2\sigma(Z) + (2a_1^2\zeta - \zeta a_2)\sigma(Z)^2 + \\
&\quad (2a_3 + a_1a_2(2\zeta + 3\zeta^2) + a_1^3\zeta)\sigma(Z)^3 + \cdots\big) \\
&= Z(1 + a_1Z + a_2Z^2 + a_3Z^3 + \cdots)\big(1 - a_1\zeta^2 \cdot \zeta Z(1 + a_1Z + a_2Z^2 + \cdots) + \\
&\quad (2a_1^2\zeta - a_2\zeta) \cdot \zeta^2Z^2(1 + a_1Z + \cdots)^2 + (2a_3 + a_1a_2(2\zeta + 3\zeta^2) + a_1^3\zeta)(1 + \cdots)^3 + \cdots\big) \\
&= Z(1 + a_1Z + a_2Z^2 + a_3Z^3 + \cdots)(1 - a_1Z + (a_1^2 - a_2)Z^2 + \\
&\quad ((4 + \zeta)a_1^3 + (-6 - \zeta)a_1a_2 + 2a_3)Z^3 + \cdots) \\
&= Z(1 + ((5 + \zeta)a_1^3 + (-8 - \zeta)a_1a_2 + 3a_3)Z^3 + \cdots).
\end{aligned}$$

Hence we conclude that $E_1 = E_2 = 0$ and that $E_3 = (5+\zeta)a_1^3 + (-8-\zeta)a_1a_2 + 3a_3$.

We will see that, in general, $E_1 = E_2 = \cdots = E_{q-1} = 0$. The part of E_3 that can be generalized is the term $3a_3$. The next theorem makes this precise. In [G-M2] the theorem is only stated for $q = p$ prime. However, the proof is essentially the same, as shown to the author in a private manuscript of Green. For the convenience of the reader the proof is presented here in greater detail than in [G-M2].

Theorem 4.1.1 ([G-M2])**.** *The following are true about the polynomials E_i, $i \geq 1$.*

(a) *If the weights $w(a_j) = j$ are assigned, then the E_i are homogeneous polynomials of degree i with coefficients in R.*

(b) $E_1 = E_2 = \cdots = E_{q-1} = 0$.

(c) *For any positive integer m, we have $E_{mq}, E_{mq+1}, \ldots, E_{(m+1)q-1} \in R[a_1, a_2, \ldots, a_{mq}]$.*

(d) *The coefficient of a_{mq} in E_{mq} is equal to q.*

(e) *Denote by J_{mq} the ideal of $R[a_1, a_2, \ldots, a_{mq}]$ generated by the polynomials $(E_{jq})_{1\leq j\leq m}$ and by KJ_{mq} the tensor product $J_{mq} \otimes K$. Then, for $mq < i < (m+1)q$ one has $E_i \in KJ_{mq}$.*

(f) *For each positive integer m, denote the image of E_m in $k[(a_i)_i]$ under the canonical reduction map, by $\bar{E}_m$. Then $\bar{E}_i \in k[a_1, \ldots, a_{mq}]$ for $mq + 1 \leq i \leq (m+1)q$, $m \geq 1$ (when $m = 0$, this is a restatement of* (b)).

Proof. (a) We introduce a dummy variable X to help us. Replace Z with XZ. Then the term a_iZ^i becomes $a_iX^iZ^i$, so that Z^i has the coefficient a_iX^i. After iteration of the automorphism, the polynomial $E_m\big((a_i)_i\big)$ becomes $E_m\big((a_iX^i)_i\big)$, i.e. all the a_i in E_m are replaced by a_iX^i. But

this is the coefficient of Z^m, so because of the way we introduced X, we must have $E_m\big((a_iX^i)_i\big) = X^m E_m\big((a_i)_i\big)$. This shows that the weights $w(a_i) = i$ make each polynomial E_m homogeneous of weight m. It is clear that each E_i is defined over R, since $\zeta \in R$.

(b) To show this we look only at the expansions of $\sigma(Z)$ and $\sigma^q(Z)$ modulo Z^{q+1}. Formally, if we let $A = R[a_1, a_2, \ldots, a_q]$ and $B = AZ \oplus AZ^2 \oplus \cdots \oplus AZ^q$, then truncating σ like this, induces an endomorphism $\tilde{\sigma}$ of B. (Though the notation is the same, $\tilde{\sigma}$ should not be confused with the induced automorphism of the p-adic open disc.) Note that the elements

$$Z^i = (\underbrace{0, 0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0, 0)$$

form a basis for B over A. So $\tilde{\sigma}$ can be described by saying what it does to each of these elements.

$$\begin{aligned}
\tilde{\sigma}\big((1,0,0,\ldots,0)\big) &= (\zeta, \zeta a_1, \ldots, \zeta a_{q-1}) \\
\tilde{\sigma}\big((0,1,0,0,\ldots,0)\big) &= (0, \zeta^2, \ldots) \\
\tilde{\sigma}\big((0,0,1,0,\ldots,0)\big) &= (0, 0, \zeta^3, \ldots) \\
&\vdots \\
\tilde{\sigma}\big((0,0,\ldots,0,1)\big) &= (0, 0, \ldots, 0, \zeta^q).
\end{aligned}$$

We may thus represent $\tilde{\sigma}$ as a triangular matrix with the elements $\zeta, \zeta^2, \ldots, \zeta^q$ on the diagonal. Hence, this endomorphism has the characteristic polynomial $\xi(X) = \prod_{1 \le i \le q}(X - \zeta^i) = X^q - 1$. The Cayley-Hamilton Theorem now implies that $\tilde{\sigma}^q = \mathbf{1}_B$, the identity on B. Hence $E_i = 0$ for $i = 1, 2, \ldots, q-1$.

We prove (e) before (c) since the result in (e) is used to prove (c).

(e) We prove this by strong induction, assuming that the result is true for all $j < i$. Note that m is uniquely determined by i and that q does not

divide i. We have

$$\sigma(Z) \equiv \zeta Z(1 + a_1 Z + \cdots + a_i Z^i) \pmod{Z^{i+2}},$$

so, by the inductive hypothesis we have

$$\sigma^q(Z) \equiv Z(1 + E_i Z^i) \pmod{KJ_{mq}, Z^{i+2}}.$$

If we now compute $\sigma \circ \sigma^q(Z)$ and $\sigma^q \circ \sigma(Z)$ modulo (KJ_{mq}, Z^{i+2}), we see that

$$\begin{aligned} \sigma \circ \sigma^q(Z) &\equiv \sigma(Z(1 + E_i Z^i)) \\ &\equiv \zeta Z(1 + a_1 Z + \cdots + a_i Z^i)(1 + E_i \zeta^i Z^i) \pmod{(KJ_{mq}, Z^{i+2})} \end{aligned}$$

and

$$\begin{aligned} \sigma^q \circ \sigma(Z) &\equiv \sigma^q(\zeta Z(1 + a_1 Z + \cdots + a_i Z^i)) \\ &\equiv \zeta Z(1 + E_i Z^i)(1 + a_1 Z + \cdots + a_i Z^i) \pmod{(KJ_{mq}, Z^{i+2})}. \end{aligned}$$

After simplifying we obtain

$$\zeta Z(E_i \zeta^i Z^i) \equiv \zeta Z(E_i Z^i) \pmod{(KJ_{mq}, Z^{i+2})}$$

or

$$E_i(\zeta^i - 1) \equiv 0 \pmod{(KJ_{mq}, Z)}.$$

Since i is not divisible by q, the scalar $\zeta^i - 1$ is invertible in K, which means that E_i must lie in the ideal (KJ_{mq}).

(c) By definition the polynomials E_i are polynomials over R, but (e) implies that if $mq < i < (m+1)q$ then also $E_i \in K[a_1, \ldots, a_{mq}]$. Hence $E_i \in R[a_1, \ldots, a_i] \cap K[a_1, \ldots, a_{mq}] = R[a_1, \ldots, a_{mq}]$.

(d) Note that (a) implies that the coefficient of a_{mq} in E_{mq} must be a constant. To compute this constant, we look at σ and its iterates

modulo the ideal $I = (a_1, a_2, \ldots, a_{mq-1}, Z^{mq+2})$.

$$\begin{aligned}
\sigma(Z) &\equiv \zeta Z(1 + a_{mq}Z^{mq}) \pmod{I} \\
\sigma^2(Z) &\equiv \zeta^2 Z(1 + 2a_{mq}Z^{mq}) \pmod{I} \\
&\vdots \\
\sigma^q(Z) &\equiv \zeta^q Z(1 + qa_{mq}Z^{mq}) \pmod{I},
\end{aligned}$$

as before. This shows that $E_{mq} \equiv qa_{mq} \pmod{I}$ and the coefficient of a_{mq} is indeed q.

(f) The previous statements take care of most of (f). We are only further require to show that $\overline{E_{(m+1)q}} \in k[a_1, \ldots, a_{mq}]$. This follows, as in (e), from the fact that $\bar{\sigma} \circ \bar{\sigma}^q = \bar{\sigma}^q \circ \bar{\sigma}$ on $k[\![z]\!]$. We work modulo the ideal $I = (\overline{I_{(m+1)q-1}}, z^{(m+1)q+3})$.

$$\begin{aligned}
\bar{\sigma}(z) &\equiv z(1 + a_1 z + \cdots + a_{(m+1)q+1}z^{(m+1)q+1}) \pmod{I}, \\
\bar{\sigma}^q(z) &\equiv z(1 + \overline{E_{(m+1)q}}z^{(m+1)q} + \overline{E_{(m+1)q+1}}z^{(m+1)q+1}) \pmod{I}.
\end{aligned}$$

We have

$$\begin{aligned}
\bar{\sigma} \circ \bar{\sigma}^q(z) &\equiv \bar{\sigma}\big(z(1 + \overline{E_{(m+1)q}}z^{(m+1)q} + \overline{E_{(m+1)q+1}}z^{(m+1)q+1})\big) \pmod{I} \\
&\equiv \bar{\sigma}(z)(1 + \overline{E_{(m+1)q}}\bar{\sigma}(z)^{(m+1)q} + \overline{E_{(m+1)q+1}}\bar{\sigma}(z)^{(m+1)q+1}) \pmod{I} \\
&\equiv z(1 + a_1 z + \cdots + a_{(m+1)q+1}z^{(m+1)q+1}) \times \\
&\qquad (1 + \overline{E_{(m+1)q}}z^{(m+1)q} + \overline{E_{(m+1)q+1}}z^{(m+1)q+1}) \pmod{I}
\end{aligned}$$

and

$$\begin{aligned}
\bar{\sigma}^q \circ \bar{\sigma}(z) &\equiv \bar{\sigma}^q\big(z(1 + a_1 z + \cdots + a_{(m+1)q+1}z^{(m+1)q+1})\big) \pmod{I} \\
&\equiv \bar{\sigma}^q(z)(1 + a_1\bar{\sigma}^q(z) + \cdots + a_{(m+1)q+1}\bar{\sigma}^q(z)^{(m+1)q+1}) \pmod{I} \\
&= z(1 + \overline{E_{(m+1)q}}z^{(m+1)q} + \overline{E_{(m+1)q+1}}z^{(m+1)q+1}) \times \\
&\qquad (1 + a_1(z + \overline{E_{(m+1)q}}z^{(m+1)q}) + \cdots + a_{(m+1)q+1}z^{(m+1)q+1}) \pmod{I}
\end{aligned}$$

It follows that $a_1\overline{E_{(m+1)q}} \equiv 0 \pmod{I}$. Hence, if $\overline{E_{(m+1)q}}$ contains some a_i for $mq < i \leq (m+1)q$, then this a_i occurs in the form $a_i \cdot f$, where f is a polynomial in I. The smallest degree f can possibly have is q (from $\overline{E_q}$). Hence the degree of $a_i \cdot f$ is at least $i + q > (m+1)q$ which is impossible since $\overline{E_{(m+1)q}}$ is homogeneous of degree $(m+1)q$. $\square$

The moduli space approach.

It is possible to form the so-called *moduli space* of order q automorphisms with a fixed point at $Z = 0$. Of course, by this last statement we mean that the induced automorphism of D has a fixed point at (Z). As with other moduli spaces, this moduli space will be a space in which each point represents an object we are interested in. Normally, the objects of interest are isomorphism classes of curves. In our case each point represents an order q automorphism of the form $\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots)$. One hopes that by studying this moduli space, one may obtain a new method to attack the lifting problem. It would be interesting, even if it works only for a few special cases.

Recall that we defined J_{mq} of $R[a_1, a_2, \dots]$ as the ideal generated by the elements $E_1, E_2, \dots, E_{mq}$ and KJ_{mq} as the tensor product $J_{mq} \otimes K$. Set $\mathcal{I}_{mq} = J_{mq} \cap R[a_1, a_2, \dots, a_{mq}]$. Define the schemes $\mathcal{X}_{mq} := \mathrm{Spec}(R[a_1, a_2, \dots, a_{mq}]/\mathcal{I}_{mq})$. Note that for any positive integer m, we have a natural inclusion of ideals

$$\mathcal{I}_{mq} R[a_1, a_2, \dots, a_{(m+1)q}] \to \mathcal{I}_{(m+1)q}.$$

This inclusion makes it possible to define a natural map

$$R[a_1, a_2, \dots, a_{mq}]/\mathcal{I}_{mq} \to R[a_1, a_2, \dots, a_{(m+1)q}]/\mathcal{I}_{(m+1)q}.$$

The inclusion of ideals ensures that this map is well-defined. Alternatively, we may look at it geometrically and speak about morphisms $\mathcal{X}_{(m+1)q} \to \mathcal{X}_{mq}$.

Note that the R-rational points in the scheme $\mathcal{X}_{mq}$ correspond to those automorphisms whose q-th iterate vanishes modulo $Z^{(m+1)q-1}$. Our goal is to pass to the limit of this system. We form the direct limit of the system

$$R[a_1, \dots, a_q]/\mathcal{I}_q \to \cdots \to R[a_1, a_2, \dots, a_{mq}]/\mathcal{I}_{mq} \to R[a_1, a_2, \dots, a_{(m+1)q}]/\mathcal{I}_{(m+1)q} \to \cdots$$

which corresponds to the inverse limit of the system

$$\cdots \to \mathcal{X}_{(m+1)q} \to \mathcal{X}_{mq} \to \cdots \to \mathcal{X}_q.$$

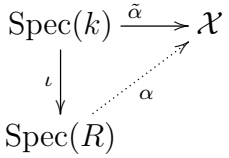
Call this limit $\mathcal{X} = \mathrm{Spec}(R[(a_i)_{i\geq 1}]/(\mathcal{I}_{mq})_{m\geq 1})$.

Definition. We call $\mathcal{X}$ the *moduli space of order q automorphisms with fixed points of the open disc* $\mathrm{Spec}(R[\![Z]\!])$.

The R-rational points of $\mathcal{X}$ now correspond to those automorphisms of the open disc $\mathrm{Spec}(R[\![Z]\!])$ whose q-th iterates vanish modulo $Z^{(m+1)q-1}$ for every positive integer m, i.e. the automorphisms of order q. The k-rational points, in turn, correspond to the automorphisms of $k[\![z]\!]$ whose q-th iterates vanish modulo $Z^{(m+1)q-1}$ for every positive integer m. In this case we obtain all the automorphisms of order dividing q.

We may rephrase the Oort-Sekiguchi conjecture once more, using the terminology of the moduli space which we just introduced.

Conjecture 3 (Moduli Space Oort-Sekiguchi)**.** *Every k-rational point of $\mathcal{X}$ factors through an R-rational point of $\mathcal{X}$. In terms of the diagram below that means that given the morphism $\tilde{\alpha} : \mathrm{Spec}(k) \to \mathcal{X}$, there exists a morphism $\alpha : \mathrm{Spec}(R) \to \mathcal{X}$ such that $\tilde{\alpha} = \alpha \circ \iota$ where $\iota : \mathrm{Spec}(k) \to \mathrm{Spec}(R)$ is the closed immersion corresponding to the reduction map $\rho : R \to k$.*



4.2 Sufficient Conditions for Lifting

In this section we present a theorem which gives sufficient conditions for lifting. The condition is the assumption that an automorphism can be lifted modulo some power of π. Actually, it is slightly more intricate than that.

The variables $a_1, a_2, \ldots$ need to be lifted modulo different powers of π. We shall also concentrate on a finite number of variables at a time.

Suppose that we are given a k-rational point $\tilde{\alpha}$ of $\mathcal{X}$. We wish to find an R-rational point α of $\mathcal{X}$ which has $\tilde{\alpha}$ as its special fibre. In the inverse system

$$\cdots \to \mathcal{X}_{mq} \to \cdots \to \mathcal{X}_{2q} \to \mathcal{X}_q$$

we wish to cut it at some stage and only consider the scheme $\mathcal{X}_{mq}$ and its R-rational points. If, for any m, we can find an R-rational point of $\mathcal{X}_{mq}$ with special fibre $\tilde{\alpha}$ viewed as a k-rational point of $\mathcal{X}_{mq}$, then there will exist an R-rational point α with special fibre $\tilde{\alpha}$. This is because $\mathcal{X}$ is defined to be the inverse limit of the $\mathcal{X}_{mq}$.

We recall the theorem by Greenberg which we mentioned in chapter 1. We restate it here, because most of this section revolves around it in some way.

Theorem 4.2.1 ([Gr])**.** *Assume that R is a complete discrete valuation ring and that K is its field of fractions. Let $f_1, f_2, \ldots, f_r$ be a system of r polynomials in n variables, denoted collectively by Z. Then there are constants $N \geq 1, c \geq 1, s \geq 0$ depending on the ideal of $R[Z]$ generated by $f_1, f_2, \ldots, f_r$ such that for every $\nu \geq N$ and any X in R^n such that*

$$f_i(X) \equiv 0 \pmod{\pi^\nu} \quad \text{for every } i = 1, 2, \ldots, r$$

there exists $Y \in R^n$ such that $f_i(Y) = 0$ for every $i = 1, 2, \ldots, r$ and

$$Y \equiv X \pmod{\pi^{\lfloor \nu/c \rfloor - s}}.$$

Our goal will be to compute some constants ν, N, c, s which will serve in the theorem above. The polynomials $f_1, \ldots, f_r$ will, naturally, be replaced by the polynomials $E_q, \ldots, E_{mq}$ from the previous section. The variables X will be $a_1, a_2 \ldots, a_{mq}$. We shall make use of the special form of the polynomials E_{iq}. Particularly useful will be the linear term qa_{iq} in $E_{iq} = qa_{iq} + \cdots$.

Proposition 4.2.2. *Let r be a positive integer and let $F \in R[X_0, X_1, \ldots, X_n]$ be a polynomial of the form*

$$F = c_1 X_0 + c_2 g_1 + g_2$$

where $g_1 \in R[X_0, X_1, \ldots, X_n]$, $g_2 \in R[X_1, \ldots, X_n]$ and c_1 and c_2 are constants such that $v_\pi(c_1) = m$ and $v_\pi(c_2) > m$ (v_π denotes the π-adic valuation). If there exist $\tilde{x}_0, \ldots, \tilde{x}_n$ such that $F(\tilde{x}_0, \ldots, \tilde{x}_n) \equiv 0 \pmod{\pi^{m+r}}$ then we can find $x_0, x_1, \ldots, x_n \in R$ such that

- $F(x_0, \ldots, x_n) = 0$,
- $x_0 \equiv \tilde{x}_0 \pmod{\pi^r}$ *and*
- $x_i \equiv \tilde{x}_i \pmod{\pi^{m+r}}$.

Proof. We keep the values of $\tilde{x}_i$ modulo π^{m+r}, lift them arbitrarily to x_i and solve for X_0 in the resulting equation. We have

$$F(X_0, x_1, \ldots, x_n) = c_1 X_0 + c_2 g_1(X_0, x_1, \ldots, x_n) + g_2(x_1, \ldots, x_n).$$

If we fix the lifting $(x_1, \ldots, x_n)$ of $(\tilde{x}_1, \cdots \tilde{x}_n)$, we may think of this as a polynomial in the variable X_0. Furthermore the expression $g_2(x_1, \ldots, x_n)$ will be some constant b. We know that b must be divisible by π^m since otherwise the tuple $(\tilde{x}_0, \ldots, \tilde{x}_n)$ couldn't be a solution modulo π^{m+r} (or even modulo π^m). So we may divide by c_1 in this equation, since c_1 is π^m times some unit of R.

The equation $F = 0$ is now equivalent to

$$X_0 + \frac{c_2}{c_1} g(X_0, x_1, \ldots, x_n) + \frac{b}{c_1} = 0.$$

We use Hensel's Lemma to show that this polynomial has a solution x_0 with $x_0 \equiv \tilde{x_0} \pmod{\pi^r}$. Firstly, note that $X_0 = \tilde{x_0}$ is a solution to this equation modulo π^r, since $(x_0, \ldots, x_n)$ was a solution to $F \equiv 0$ modulo π^{m+r} and we

only divided F by $c_1 \in \pi^m R^\times$. The derivative of this polynomial with respect to X_0 is

$$\frac{\mathrm{d}}{\mathrm{d}X_0}\big(X_0 + \frac{c_2}{c_1}g(X_0, x_1, \ldots, x_n) + \frac{b}{c_1}\big) = 1 + \frac{c_2}{c_1}\frac{\mathrm{d}}{\mathrm{d}X_0}g(X_0, x_1, \ldots, x_n).$$

This is always congruent to 1 modulo π, since $\frac{c_2}{c_1}$ is divisible by π. In particular, this is true when $X_0 = \tilde{x_0}$, meaning that $\tilde{x_0}$ can be lifted to as solution x_0 of F over R. □

Remark. If c_1X_0 is the only term containing an X_0, i.e. if we can set $g_1 = 0$, then the hypothesis that R is complete is not necessary. It will work for any discrete valuation ring.

The idea is that we can lift the $\bar{a}_i$ to any a_i whenever q does not divide the index i and then solve for the a_{qi} from the equations $E_{qi} = 0$ by Proposition 4.2.2. In this way we may conclude that if one can simultaneously lift all the equations to a solution modulo π^{m+1} for $m = v_\pi(q)$, then one may lift all the way to a solution in R. Actually, there is a slight subtlety which does not allow us to proceed in exactly this fashion.

Suppose we have the two equations $E_q = 0$ and $E_{2q} = 0$. They are of the form

$$qa_q + \cdots = 0$$

$$qa_{2q} + \cdots = 0.$$

So the proposition applies to each separately, but the problem is that the same a_q must work in both equations. In the first equation, a_q is calculated as a solution to a certain polynomial equation, while in the second it is lifted arbitrarily. One might think that choosing the solution of a_q as the arbitrary lifting in the second equation solves the problem. It doesn't, because the hypotheses are that $(a_1, \ldots, a_{2q})$ give a solution modulo π^{m+1} and that we wish to lift it in such a way that they stay the same modulo π^m. In the first equation, however, a_q only stays the same modulo π. Hence, lifting a_q to the

solution of the first equation might make it impossible to solve the second equation modulo π^{m+1}.

We may fix this by being satisfied with a slightly more complicated statement.

Theorem 4.2.3. *Set $m = v_\pi(q)$, let n be a positive integer and suppose that $\bar{\sigma}(z) = z(1 + \bar{a}_1 z + \cdots)$ is an order q automorphism of $k[\![z]\!]$. Also suppose that there exist $\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_{nq} \in R$ such that*

- $\tilde{a}_i \equiv \bar{a}_i \pmod{\pi}$ *for* $1 \leq i \leq nq$,
- $E_{(n-i)q}(\tilde{a}_1, \ldots, \tilde{a}_{(n-i)q}) \equiv 0 \pmod{\pi^{(i+1)m+1}}$ *for* $0 \leq i \leq n-1$.

Then there exist $a_1, \ldots, a_{mq} \in R$ such that

- $E_{iq}(a_1, \ldots, a_{mq}) = 0$ *for* $1 \leq i \leq n$,
- $a_i \equiv \bar{a}_i \pmod{\pi}$ *for* $1 \leq i \leq nq$, *i.e. each a_i is a lifting of $\bar{a}_i$.*

Proof. We first apply Proposition 4.2.2 to equation $E_q = 0$ with $r = (n-1)m + 1$. We may lift $\tilde{a}_1, \ldots, \tilde{a}_{q-1}$ in any way we like to $a_1, \ldots, a_{q-1}$ and solve for a_q. Then $a_i \equiv \tilde{a}_i \pmod{\pi^{nm+1}}$ for $1 \leq i \leq q-1$ and $a_q \equiv \tilde{a}_q \pmod{\pi^{(n-1)m+1}}$. So, for $1 \leq i \leq q$ we have

$$a_i \equiv \tilde{a}_i \pmod{\pi^{(n-1)m+1}}.$$

Next we apply the proposition to $E_{2q} = 0$ with $r = (n-2)m + 1$. We may lift $\tilde{a}_1, \ldots, \tilde{a}_q$ to the $a_1, \ldots, a_q$ we just computed. Then we may lift $\tilde{a}_{q+1}, \ldots, \tilde{a}_{2q-1}$ in any way and solve for a_{2q} from the resulting equation. This time we have

$$a_i \equiv \tilde{a}_i \pmod{\pi^{(n-2)m+1}}$$

for $1 \leq i \leq 2q$. We continue this process until we have lifted $\tilde{a}_1, \ldots, \tilde{a}_{nq}$ in such a way that $E_{iq} = 0$ for $1 \leq i \leq n$ and $a_i \equiv \tilde{a}_i \pmod{\pi^{(n-n)m+1}}$. This last congruence is equivalent to $a_i \equiv \bar{a}_i \pmod{\pi}$, as required. □

In some sense this gives us a finite criterion to attack the Oort-Sekiguchi conjecture. If we were able to fulfill the requirements of the theorem above for an arbitrary positive integer n we would be able to take the inverse limit of these solutions and obtain a lifting of all the $\bar{a}_i$ simultaneously. There is no need to worry about the compatibility of the solutions with the morphisms

$$R[a_1, a_2, \ldots, a_{(n-1)q}]/\mathcal{I}_{(n-1)q} \to R[a_1, a_2, \ldots, a_{nq}]/\mathcal{I}_{nq}$$

from the previous section, since if the conditions in the above theorem are satisfied for n, they are immediately also satisfied for $n-1$.

We summarize:

Corollary. *If, for any positive integer n, the coefficients $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{nq}$ of an order q automorphism $\bar{\sigma}$ can be lifted to some $a_1, a_2, \ldots, a_{nq}$ which define an automorphism σ of $R[\![Z]\!]$ whose q-th iterate vanishes modulo a high enough power of π, then there exists an order q automorphism τ of $R[\![Z]\!]$ lifting $\bar{\sigma}$.*

Concluding Remarks

Let us quickly summarize what we did. The first major theme was stating the Oort-Sekiguchi conjecture and discussing the progress that has been made on it. The local-global principle was especially important to us (even though we don't prove it), since this allows us to look exclusively at automorphisms of power series rings. This is what we did in this thesis.

We looked at some of the elementary properties of automorphisms, mainly to prove that they take a certain nice form. Some of the author's own results were included in section 2.2 on conjugacy classes of automorphisms.

Then we described the geometry of automorphisms of the p-adic disc, focussing almost exclusively on the "fixed points". One exception is the approach using the two different differents to determine if a lifting is smooth. We described how this approach works and mentioned its efficiency.

Lastly we parametrized the order q automorphisms where $q = p^n$ and obtained equations whose solutions correspond to order q automorphisms. More of the author's own work was presented in the form of "sufficient conditions" under which the Oort-Sekiguchi conjecture would hold.

We leave the reader with something to think about. This is in the form of open problems and different approaches as well as ideas with which some of these results may be extended.

We noted that the approach using differents of ring extensions has proved effective. In this method, the first step is to find a deformation of the equation of the ring extension $k[\![z]\!]/k[\![t]\!]$. To get such a deformation is sometimes quite

difficult. To add to this difficulty the special and generic differents must be computed, and on top of that, they must be equal. So, to use this method for automorphisms of order p^n, $n \geq 3$ becomes quite computationally intensive and difficult to get the required control over.

One different angle of attack is a global method using generalised Jacobians. This is the way [O-O-S] solved the lifting problem for prime order automorphisms. Another angle is with higher dimensional local class field theory. If k were a finite field, we would be able to describe the abelian extensions of $k[\![z]\!]$ by local class field theory. In particular, we would be able to describe the p^n cyclic extensions. In a similar way one may hope to be able to describe the abelian extensions of the two-dimensional local ring $R[\![Z]\!]$ and obtain a way to relate the two. References for this theory are [F-V] and [F-K], though they focus on developing the theory and not on its application to this conjecture.

Clearly the Oort-Sekiguchi conjecture itself is still open, but there are many more open problems that come from attempts to solve it. We mentioned a theorem that the fixed points of an order p automorphism are equidistant if there are fewer than p fixed points. This is not known for an order p^n automorphism. Building on the work in the last chapter, one may ask if the polynomials E_i can be given some structure, in order to conclude some general result.

Bibliography

[E-S] Eakin, P., Sathaye, A., *R-Automorphisms of Finite Order in $R[\![X]\!]$*, Journal of Algebra, **67** (1980), pp. 110-128.

[F-K] Fesenko, I. B., Kurihara, M. *Invitation to Higher Local Fields*, Geometry and Topology Monographs **3**, Geometry and Topology Publications, International Press (1999).

[F-V] Fesenko, I. B., Vostokov, S. V., *Local Fields and Their Extensions (Second Edition)*, American Mathematical Society Translations of Mathematical Monographs **121** (2002).

[G] Green, B. W., *Automorphisms of Formal Power Series Rings over a Valuation Ring*, Fields Institute Communications **33** (2003), pp. 79-87.

[G-M1] Green, B. W., Matignon, M., *Liftings of Galois Covers of Smooth Curves*, Compositio Math. **104** (1996), pp. 239-274.

[G-M2] Green, B. W., Matignon, M., *Order p Automorphisms of the Open Disc of a p-adic Field*, Journal of the AMS, **12** (1999), pp. 269-303.

[Gr] Greenberg, M. J., *Rational points in henselian discrete valuation rings*, Publications Mathématique de l'I.H.É.S, **31** (1961), pp. 59-64.

[Ha] Hartshorne, R., *Algebraic Geometry*, Springer-Verlag Graduate Texts in Mathematics **52** (1977).

[H-K-T] Hirschfeld, J. W. P, Korchmáros, G., Torres, F., *Algebraic Curves over a Finite Field*, Princeton University Press Series in Applied Mathematics (2008).

[Ka] Kato, K., *Vanishing Cyles, Ramification of Valuations, and Class Field Theory*, Duke Mathematical Journal **55** No. 3 (1987), pp. 629-659.

[La1] Lang, S., *Algebra* (Third Edition), Springer-Verlag Graduate Texts in Mathematics **211** (2002).

[La2] Lang, S., *Algebraic Number Theory* (Second Edition), Springer-Verlag Graduate Texts in Mathematics **110** (1986).

[Liu] Liu, Q., *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics **6** (2002).

[Mu] Muckenhoupt, B., *Automorphisms of Formal Power Series Under Substitution*, Transactions of the AMS, **99** (1961), pp. 373-383.

[Na] Nakajima, S., *On Abelian Automorphism Groups of Curves*, J. London Math. Soc. (2) **36** (1987), pp. 23-32.

[O-O-S] Oort, F., Sekiguchi, T., Suwa, N. *On the deformation of Artin-Schreier to Kummer*, Ann. Sci. École Norm Sup. (4) **22** (1989), pp. 345-375.

[Sa] Villa Salvador, G. D., *Topics in the Theory of Algebraic Function Fields*, Birkhäuser (2006).

[Se] Serre, J.-P., *Local Fields*, Springer-Verlag Graduate Texts in Mathematics **67** (1979).

[Si] Silverman, J., *The Arithmetic of Elliptic Curves*, Springer-Verlag Graduate Texts in Mathematics **106** (1986).

[SGA1] Grothendieck, A., *Seminaire Geometrie Algebrique 1 – Revêtements étales et groupe fondamental*, Springer-Verlag Lecture Notes in Mathematics **224** (1960-61).

[St] Stichtenoth, H., *Algebraic Function Fields and Codes* (Second Edition), Springer-Verlag Graduate Texts in Mathematics **254** (2009).