On the Constant Reductions of Valued Function Fields and their Automorphism Groups

by

Tovondrainy Christalin Razafindramahatsiaro

Dissertation presented for the degree of Doctor of Philosophy in Mathematics in the Faculty of Science at Stellenbosch University

African Institute for Mathematical Sciences,
6-8, Melrose Road, Muizenberg, Cape Town, South Africa.

Promoter: Prof. Barry W. Green

December 2015

Declaration

By submitting this dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: ....December 2015..........

Abstract

On the Constant Reductions of Valued Function Fields and their Automorphism Groups

T. C. Razafindramahatsiaro

African Institute for Mathematical Sciences,
6-8, Melrose Road, Muizenberg, Cape Town, South Africa.

Dissertation: PhD (Mathematics)

December 2015

The aim of the project is to investigate properties of the automorphism group of a function field in one variable over an algebraically closed field in relation to its reductions with respect to special valuations.

Let $\mathcal{X}$ be a stable curve defined over a Dedekind scheme S, with smooth generic fiber $\mathcal{X}_\eta$. It is well known (From Deligne and Mumford) that there exists a natural injective homomorphism between the automorphism groups of $\mathcal{X}_\eta$ and any special fibre of $\mathcal{X}$. In this thesis, we give a generalisation of this theorem in the function field setting of Deuring's theory of constant reductions. The result brings us to one of the central topic in Arithmetic Geometry after Grothendieck, Deligne and Mumford: The lifting problem for curves. We will consider the so-called "weak" Lifting problem for automorphism groups of cyclic curves in this thesis.

We will also study good reduction for function fields. In particular, we are interested in corresponding reduction of divisors via the Deuring's arithmetic divisor homomorphism. Together with the generalised Deligne and Mumford Theorem above, we will discuss the Tchebotarev Density Theorem for function fields.

Uittreksel

Oor die Konstante Reduksie van Funksieliggame en hulle Outomorfisme Groepe

T. C. Razafindramahatsiaro

Afrika Institut vir Wiskundige Wetenskappe,
6-8 Melrose Weg, Muizenberg, Kaapstad, Suid Afrika.

Proefskrif: PhD (Wiskunde)

Desember 2015

Die doel van hierdie projek is om die eienskappe van die Outomorfisme Groep van 'n Funksieliggaam in een veranderlike oor 'n algebraiese afgeslote liggaam in samehang met die reduksies daarvan te studeer.

Laat $\mathcal{X}$ 'n stabile kurwe wees wat oor 'n Dedekind Scheme S gedefinieerd is met generiese vesel $\mathcal{X}_\eta$. Dit is bekend, uit werk van Deligne en Mumford, dat daar 'n natuurlike injektiewe homomorfisme tussen die outomorfisme groep van $\mathcal{X}_\eta$ en die van enige spesiale vesel bestaan. In hierdie tesis bewys ons 'n veralgemening van hierdie resultaat in die geval van funksieliggame in die raamwerk van Deuring se teorie van Konstanterekuksie. Die resultaat lei na een van die sentrale onderwerpe in Aritmetiese Meetkunde in die gees van Grothendieck, Deligne en Mumford, naamlik: Die Heffingsprobleem vir kurwes. Ons sal die sogenaamde "Swak Heffingsprobleem"vir die outomorfisme groep van sikliese kurwes in die tesis behandel.

Verder bestudeer ons ook vrae binne die raamwerk van die goeie reduksie van kurwes. In besonder stel ons belang in die eienskappe van divisore met behulp van Deuring se divisorreduksie homomorfisme. Deur gebruik te maak van die veralgemening van die Deligne Mumford Stelling wat hierbo na verwys word, bespreek ons die Tschebotarev Digtheidsstelling vir funksieliggame.

Acknowledgements

First and foremost, I would like to thank my supervisor Barry Green, not only for his constant guidance, his encouragement throughout the thesis, but also even for helping me to get over problems outside my study programme related to my study permit during my Phd study. Words will not suffice to express my gratitude to him.

I would like also to thank the Fondation Science Mathématique de Paris (FSMP) and the African Institute for Mathematical Sciences (AIMS) for financial support during the last five years of my graduate study. A special thanks goes to all who have contributed to the success of AIMS, especially Neil Turok, for his great vision to build the Institute and to my teacher Gerard Razafimanantsoa, without whom I could not have been part of the AIMS family. Without their joint effort to promote Mathematics in Africa, it would have been difficult for me to achieve a Phd.

Thanks to all my friends and the Malagasy community in Cape Town (especially the AIMS alumni) for all the activities outside school we had during the last three years. I would like to mention Andry Rabenantoandro for his time reading the manuscript.

I will not forget my family for their prayers, love, continuous encouragement and for always believing in me.

Last but not least: To my wife Rafetrarivony Lala Fanomezantsoa, "Thank you very much for your patience and understanding!"

Contents

Chapter 1

Introduction

Let X_g be a smooth projective irreducible curve of genus g defined over an algebraically closed field k. Denote by p the characteristic of k. Determining which groups can occur as automorphism groups $\mathrm{Aut}_k(X_g)$ of X_g is a classic problem in mathematics. In the case when $g \leq 1$, the problem is well understood.

For convenience, in this thesis, we assume that the genus of a given curve is at least 2*, unless otherwise specified.*

It is well known that $G = \mathrm{Aut}(X_g)$ is a finite group. So, one can ask: For a given g, which finite groups can occur as automorphism groups on algebraic curves of genus g? And, conversely, for a given finite group G, for which genera g does there exist a curve of genus g which has G as automorphism group?

In [Hur93a], Hurwitz proved that the order of the group G is less than or equal to $84(g-1)$ in characteristic 0. As an example, equality holds for the curve of genus 3 defined by:

$$x^3y + y^3z + z^3x = 0.$$

Such curves are called `Hurwitz curves.` Furthermore, in the case when k is the field of complex numbers, there are methods to find precisely which finite groups can occur on the curve X_g. Indeed, first, recall that the category of algebraic curves over the complex numbers $\mathbb{C}$ is equivalent to the category of Riemann surfaces and fields of transcendence degree 1 over $\mathbb{C}$. So to determine which finite groups can act as groups of automorphisms of algebraic curves, it is sufficient to answer the inverse Galois problem for the rational function field $\mathbb{C}(x)$. That is what Hurwitz did. By Lefshetz Principle, Hurwitz results hold also over any algebraically closed field of characteristic 0.

Unfortunately, the methods in the characteristic 0 case do not seem to apply in positive characteristic. And there are very few results on this problem in positive characteristic. Although the group G must be finite, there is no precise bound. In [Roq87], Roquette gave an example of a curve with automorphism group whose order is greater than $84(g-1)$. In [Sti73], Stichtenoth proved that the order of G must be less than $16g^4$ for $p > 0$.

One way to understand why the methods in characteristic 0 do not apply in general characteristic is the study of the reductions theory of curves. Indeed, we want to compare, for example, the automorphism group of a curve X defined in characteristic 0 with the automorphism group of the reduction $\overline{X}$ modulo a prime p of X. In [DM69], Deligne and Mumford proved that if $\mathcal{X}$ is a stable model of a smooth irreducible curve X (defined in characteristic 0 and the generic fiber of $\mathcal{X}$ is assumed to be isomorphic to X), then for any special fibre $\overline{X}$ of $\mathcal{X}$, there is a natural injective homomorphism from $\mathrm{Aut}(X)$ to $\mathrm{Aut}(\overline{X})$. This solves partially the problem.

Chapter 4 will be devoted to generalise this result of Deligne and Mumford. Our approach is similar to what Hurwitz did to solve the problem of determining finite groups than can occur as automorphism groups of algebraic curves in characteristic 0. We use the fact that the category of smooth projective irreducible curves over an algebraically closed field k is equivalent to the category of function fields in one variable over k. So, instead of working directly on curves, we will work on function fields in one variable. More precisely, we will use Deuring's theory of constant reductions. Since this is the theory that we will use most of the time, a survey will be given in Chapter 2. The main new results in Chapter 4 are Lemma 4.3.3, Theorem 4.3.5 and Proposition 4.3.7. Theorem 4.3.5 is a generalisation of the result by P. Deligne and D. Mumford we mentioned above.

Throughout this thesis, a function field is always a finite algebraic extension of a rational function field of transcendental degree one.

Now, we have a little understanding on why the methods in charateristic 0 do not seem to apply in positive characteristic. That is the fact that, in general, we have injectivity not isomorphism between the automorphism group of the curve and its reduction. One explicit example is the Roquette curve in [Roq87]. So, one natural question to ask is under which condition we have isomorphism? This problem is related to be the `Lifting Problem on algebraic curves.` That is the purpose of Chapter 5. In this chapter, we study the case of cycle curves. The main new results are Lemma 5.1.5, Theorem 5.2.1 and Theorem 5.2.4. Theorem 5.2.4 gives the list of hyperelliptic curves and their automorphism groups in odd prime characteristic that can be lifted to characteristic 0.

Let $(\mathbb{F}|k, v)$ be a valued function field where v is assumed to be a good reduction. In chapter 4, we compare the automorphism group $\mathrm{Aut}(\mathbb{F}|k)$ with the automorphism group of the corresponding residue function field $\mathbb{F}v|kv$ using mainly Deuring's theory of constant reductions. It turns out that automorphism groups are not the only important objects that we can compare via the Deuring's theory of constant reductions on function fields, but also, Divisor Groups. Indeed in [Deu42], Deuring constructed a homomorphism between the Divisor groups of $\mathbb{F}|k$ and its residue field $\mathbb{F}v|kv$. Using this Divisor homomorphism, we are, for example, able to compare also the Different of extensions of function fields with the Different of the corresponding residue extensions of function fields. We can also give an alternative proof to some classical results on function fields. We will discuss this in Chapter 3. The main new results in this chapter are Lemma 3.2.8, Lemma 3.3.1 and Theorem 3.3.4.

Finally, Lemma 3.2.8 together with Theorem 4.3.5 can be used in the study of the Tchebotarev Density Theorem for function fields. That is our goal in the last chapter, Chapter 6. There is a Tchebotarev Density Theorem version for global function field, but not (in general) for function field defined over a field of characteristic 0. So, the idea is to "lift" the Tchebotarev Density Theorem of global function field to characteristic 0 in the sense that we will define in Chapter 6. The main new results are Theorem 6.2.5 and 6.2.6.

Chapter 2

Preliminary results from valuation theory

In this chapter, we give a brief introduction to Deuring's theory of constant reductions. The first section will be devoted to some indispensable definitions and results on general valuation theory. Other notions will be dealt later, as they are needed. General references for this chapter are [End72], [Sti09], [GMP89] and [GMP90].

2.1 The general setting

Let $\mathbb{K}$ be an arbitrary field. Consider a mapping

$$v: \mathbb{K} \to (\Gamma, \leq)$$

which satisfies the following conditions:

For all $x, y \in \mathbb{K}$,

(i) $v(x) = 0 \Leftrightarrow x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x+y) \geq \min\{v(x), v(y)\}$,

where $(\Gamma, \leq)$ is an ordered abelian group. The symbol ∞ is an extra element such that, for all $a, b \in \Gamma$, we have $\infty > a$ and $\infty = \infty + \infty = \infty + b = b + \infty$. Such map is called `a (non-archimedean) valuation` for the field $\mathbb{K}$. We call the set $v(\mathbb{K}^{\times})$ *valued group.*

The valuation v has the following properties:

Properties 2.1.1. *1. The restriction of v to $\mathbb{K}^{\times}$ is a group homomorphism.*

2. For all $x, y \in \mathbb{K}$ such that $v(x) \neq v(y)$, we have $v(x+y) = \min\{v(x), v(y)\}$.

3. The set

$$\mathcal{O}_v := \{x \in \mathbb{K} \mid v(x) \geq 0\}$$

is a local ring. The corresponding maximal ideal is

$$\mathcal{M}_{\mathcal{O}_v} := \{x \in \mathbb{K} \mid v(x) > 0\} = \mathcal{O}_v \setminus \mathcal{O}_v^{\times}.$$

The field $\mathbb{K}v := \mathcal{O}_v / \mathcal{M}_{\mathcal{O}_v}$ is called **the residue field** *of the ring $\mathcal{O}_v$. If there is no ambiguity, we simply denote the residue field by $\overline{\mathbb{K}}$.*

Definition 2.1.2. *A local ring $\mathcal{O}$ of $\mathbb{K}$ is called a* **valuation ring** *of $\mathbb{K}$ if there exists a valuation v of $\mathbb{K}$ such that $\mathcal{O} = \mathcal{O}_v$.*

Remark 2.1.3. *A subring $\mathcal{O}$ is a valuation ring of $\mathbb{K}$ if and only if for all $x \in \mathbb{K}^{\times}$, we have either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. If v denotes the valuation of $\mathbb{K}$ which corresponds to a valuation ring $\mathcal{O}$, then we can choose the canonical homomorphism*

$$v|_{\mathbb{K}^{\times}} : \mathbb{K}^{\times} \twoheadrightarrow \mathbb{K}^{\times}/\mathcal{O}^{\times}$$

as the restriction of v on $\mathbb{K}^{\times}$. The value group of v is $\Gamma = \mathbb{K}^{\times}/\mathcal{O}^{\times}$, endowed by the following ordering:

$$x\mathcal{O}^{\times} \leq y\mathcal{O}^{\times} \Leftrightarrow yx^{-1} \in \mathcal{M}_{\mathcal{O}} \text{ or } x\mathcal{O}^{\times} = y\mathcal{O}^{\times}.$$

Theorem 2.1.4 (Chevalley)**.** *Let R be a subring of $\mathbb{K}$. Let $\mathfrak{p} \subseteq R$ be a prime ideal. Then there is a valuation ring $\mathcal{O}$ of $\mathbb{K}$ with the properties:*

$$R \subseteq \mathcal{O} \quad \text{and} \quad \mathcal{M}_{\mathcal{O}} \cap R = \mathfrak{p}.$$

Let $\mathbb{L}|\mathbb{K}$ be an algebraic field extension. Let $\mathcal{O}_{\mathbb{K}}$ be a valuation ring of $\mathbb{K}$. A valuation ring $\mathcal{O}_{\mathbb{L}}$ of $\mathbb{L}$ is called an **extension** of $\mathcal{O}_{\mathbb{K}}$ if $\mathcal{O}_{\mathbb{L}} \cap \mathbb{K} = \mathcal{O}_{\mathbb{K}}$. Note that we may regard the value group $\Gamma_{\mathbb{K}}$ of $\mathcal{O}_{\mathbb{K}}$ as a subgroup of $\Gamma_{\mathbb{L}}$, the value group which corresponds to the valuation ring $\mathcal{O}_{\mathbb{L}}$. Then, the index $e := e\left(\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}\right) = \left[\Gamma_{\mathbb{L}} : \Gamma_{\mathbb{K}}\right]$ and $f := f\left(\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}\right) = \left[\overline{\mathbb{L}} : \overline{\mathbb{K}}\right]$ are, respectively, called the **ramification index** and the **residue degree** of the extension $\left(\mathbb{K}, \mathcal{O}_{\mathbb{K}}\right) \subseteq \left(\mathbb{L}, \mathcal{O}_{\mathbb{L}}\right)$.

Theorem 2.1.5. *Let $\mathbb{L}|\mathbb{K}$ be an algebraic field extension. Let $\mathcal{O}$ be a valuation ring of $\mathbb{K}$. Then, there exists an extension of $\mathcal{O}$ in $\mathbb{L}$. Assume that the field extension $\mathbb{L}|\mathbb{K}$ is finite. Then, there are only finitely many valuation rings $\mathcal{O}_1, \cdots, \mathcal{O}_r$ which extend $\mathcal{O}$ in $\mathbb{L}$. Furthermore, if we denote the ramification index by e_i and residue degrees by f_i for each extension $\mathcal{O}_i$, we have:*

$$\sum_{1 \leq i \leq r} e_i f_i \leq [\mathbb{L} : \mathbb{K}].$$

The integral closure of $\mathcal{O}$ in $\mathbb{L}$ is

$$\mathcal{O}' = \bigcap_{1\le i\le r} \mathcal{O}_i.$$

Now suppose that $\mathbb{L}|\mathbb{K}$ is a finite Galois extension with G:=Gal($\mathbb{L}|\mathbb{K}$).

Proposition 2.1.6. *Let $\mathcal{O}$ be a valuation ring in $\mathbb{K}$. Consider two valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ in $\mathbb{L}$ extending $\mathcal{O}$. Then there exists $\sigma \in G$ such that $\sigma(\mathcal{O}_1) = \mathcal{O}_2$. In particular, the integral closure of $\mathcal{O}$ in $\mathbb{L}$ is invariant under the action of G. Moreover, the rings $\mathcal{O}_1$ and $\mathcal{O}_2$ have the same ramification index e and residue degree f.*

Proof. See [PD01] Conjugation Theorem A.2.9. □

To end the section, we consider an important class of valuations of function fields, namely, discrete valuations.

Let $\mathbb{F}|k$ be a function field where k is the full constant field of $\mathbb{F}$. A valuation v of $\mathbb{F}|k$ is called a `discrete valuation` of $\mathbb{F}|k$ if its value group is isomorphic to the ring of integers $\mathbb{Z}$ and $v(x) = 0$ for all $x \in k$.

Proposition 2.1.7. *Consider a valuation ring $\mathcal{O}$ of $\mathbb{F}$ with the additional property $k \subsetneqq \mathcal{O} \subsetneqq \mathbb{F}$. Then the corresponding valuation is a discrete valuation of $\mathbb{F}|k$. By abuse of language, such valuation rings are called* ***valuation*** *rings of $\mathbb{F}$ over k, or simply valuation rings of $\mathbb{F}|k$.*

Proof. See [Sti09] Theorem 1.1.3. □

Definition 2.1.8. *Let $\mathbb{F}|k$ be a function field. A* ***place*** *P of $\mathbb{F}|k$ is the maximal ideal of some valuation ring of $\mathbb{F}|k$. We denote by $S(\mathbb{F}|k)$ the set of all places of $\mathbb{F}|k$. Let $P \in S(\mathbb{F}|k)$ and $x \in \mathbb{F}$. We say that P is a zero (resp. pole) of x if $v_P(x) > 0$(resp. < 0). If $v_P(x) = m > 0$(resp. < 0), P is a zero (resp. pole) of x of order m.*

Remark 2.1.9. *Using Chevalley's theorem, every transcendental element x in $\mathbb{F}|k$ has at least one zero and one pole. Furthermore, every function field has infinitely many places.*

Example 2.1.10. *Let us consider the rational function field $\mathbb{F} = k(x)$, where x is transcendental over k. For each irreducible monic polynomial $p(x)$ in $k(x)$*

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k(x), p(x) \nmid g(x) \right\}$$

is a local ring with maximal ideal

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k(x), p(x)|f(x), p(x) \nmid g(x) \right\}$$

and the local ring

$$\mathcal{O}_{\infty} := \left\{ \frac{f(x)}{g(x)} \mid f(x), \deg\, f(x) \leq \deg\, g(x) \right\}$$

with maximal ideal

$$P_{\infty} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k(x), \deg\, f(x) < \deg\, g(x) \right\}$$

are all discrete valuation rings of the rational function field $\mathbb{F}|k$. Furthermore, there are no places of the function field $\mathbb{F}|k$ other than the places $P_{p(x)}$ and P_{∞} defined above.

2.2 On Deuring's theory of Constant Reductions

Let $\mathbb{F}|k$ be a function field over the field of constants k which is equipped with a valuation v_k. Denote by $\mathcal{O}_k$ the corresponding valuation ring in k.

Let x be a transcendental element in $\mathbb{F}$. There is one and only extension, denoted by v_x (called `Gauss valuation`), of v_k to the rational function field $k(x)$ for which the reduction $\overline{x}$ of x is transcendental over $\overline{k}$. The value $v_x(f)$ of a polynomial

$$f = \sum_i a_i x^i \in k\,[x]$$

is given by

$$v_x(f) = \mathrm{min}_i v_k(a_i).$$

The value group and residue field are respectively:

$$v_x(k\,[x]) = v_k(k) \text{ and } \overline{k(x)} = \overline{k}(\overline{x}).$$

Definition 2.2.1. *Any prolongation v of v_k to $\mathbb{F}$ is called a* `constant reduction` *of $\mathbb{F}|k$ if the residue field $\mathbb{F}v$ is also a function field over the residue field $\overline{k}$.*

Remark 2.2.2. *Note that constant reductions of $\mathbb{F}|k$ always exist. Indeed, by Gauss's theorem, for a given transcendental element x in $\mathbb{F}$, we can choose a valuation v of $\mathbb{F}$ to be the extension of the Gauss valuation v_x on $k(x)$.*

Now, let $V = \{v_i, 1 \leq i \leq s\}$ be a finite set of constant reductions of $\mathbb{F}|k$ such that $v_i|_k = v_k$. For all i, denote by $g_{\mathbb{F}_{v_i}}$ the genus of the residue field $\mathbb{F}v_i$.

Theorem 2.2.3 ([GMP89], theorem 3.1.)**.** *We have:*

$$\sum_{1 \leq i \leq s} g_{\mathbb{F}_{v_i}} \leq g_{\mathbb{F}}.$$

A straightforward corollary of this theorem is the following:

Corollary 2.2.4. *Let v be a constant prolongation of v_k to $\mathbb{F}$ and suppose that we have $g_{\mathbb{F}} = g_{\mathbb{F}v} > 0$. Then v is unique with this property.*

Definition 2.2.5. *[GMP89] We say that an element $x \in \mathbb{F}$ is* ***residually transcendental*** *for a valuation v in V if the restriction of v to $k(x)$ is the Gauss valuation v_x. Let x be a transcendental element in $\mathbb{F}$. Denote by V_x the set of all prolongations of v_x to $\mathbb{F}$ and suppose $v_x = v|_{k(x)}$ for all $v \in V$. Then:*

(i) The element x is defined to be an element with the uniqueness property for V if $V = V_x$;

(ii) The element x is called V-regular for $\mathbb{F}|k$ if

$$\deg\, x := [\mathbb{F} : k(x)] = \sum_{v \in V} \left[\mathbb{F}v : \overline{k}(\overline{x})\right] := \sum_{v \in V} \deg\, \overline{x}.$$

Note that if $x \in \mathbb{F}$ is V-regular then $V = V_x$. And in the case where $V = \{v\}$, by abuse of notation, x is said to be v-regular or simply regular. In this case, we have $[\mathbb{F} : k(x)] = \left[\mathbb{F}v : \overline{k}(\overline{x})\right]$.

Definition 2.2.6. *Let $(\mathbb{F}|\mathbb{K}, v)$ be a valued function field with regular elements. We say that the constant reduction is a* ***good reduction*** *if the genus of the function field $\mathbb{F}$ is the same as the residue field $\mathbb{F}v$.*

Theorem 2.2.7 ([GMP90] Theorem 3.1 and Theorem 3.2)**.** *Let $(\mathbb{K}, v_{\mathbb{K}})$ be an algebraically closed valued field and $(\mathbb{F}|\mathbb{K}, v_i)_{1 \le i \le s}$ valued function fields with v_i prolongations of $v_{\mathbb{K}}$ to $\mathbb{F}$. Then there exist elements f which are $V = \{v_i | 1 \le i \le s\}$-regular for $\mathbb{F}|\mathbb{K}$.*

Let f be a V-regular element for $\mathbb{F}|\mathbb{K}$. We define the `infnorm` w with respect to V as (see [GMP90]):

$$w(x) = \inf_{v \in V} v(x), \;\; x \in \mathbb{F}.$$

Let

$$\mathcal{O}_w = \{x \in \mathbb{F} \mid w(x) \ge 0\}\,, \;\; \mathcal{M}_w = \{x \in \mathbb{F} \mid w(x) > 0\}\,.$$

Proposition 2.2.8. *We have:*

$$w|_{\mathbb{K}(f)} = v_f,$$

$$\mathcal{O}_w = \bigcap_{v \in V} \mathcal{O}_v, \;\; \mathcal{M}_w = \bigcap_{v \in V} \mathcal{M}_v$$

where $\mathcal{O}_v$ *and* $\mathcal{M}_v$ *are respectively the valuation ring and its maximal ideal for each* $v \in V$*. Furthermore,*

$$\mathbb{F}w{:=}\mathcal{O}_w/\mathcal{M}_w \simeq \prod_{v\in V}\mathbb{F}_v.$$

Proof. See [End72] (18.5). □

Chapter 3

Reduction of Divisors

In this chapter, we study the Deuring's arithmetic divisor homomorphism (See section 2). Our aim is the following: To compare some important divisors (such as the different) and the Riemann-Roch space associated to a divisor of a valued function field with respect to its residue function field. With Lemma 3.2.8, our main results in this chapter are in the last section. But, first of all, let us recall some important definitions and results.

Throughout the rest of the thesis, $\mathbb{F}|k$ will always denote a function field where k is the full constant field. Any valuation denoted by v on $\mathbb{F}$ is assumed to be a constant reduction.

3.1 Divisors

We call the free additively written abelian group generated by the places of $\mathbb{F}|k$ `the divisor group of` $\mathbb{F}|k$ ([Sti09] Definition 1.4.1). We denote it by $\mathrm{Div}(\mathbb{F}|k)$ or simply by $\mathrm{Div}(\mathbb{F})$ if there is no confusion. Its elements are called `divisors` of $\mathbb{F}|k$. The elements of $S(\mathbb{F}|k)$ are called the prime divisors of $\mathbb{F}|k$.

Let D be a divisor of $\mathbb{F}|k$. By definition, there exists a unique finite set denoted by $\mathrm{Supp}\ D \subset S(\mathbb{F}|k)$, called the support of D, such that

$$D = \sum_{P \in \mathrm{Supp}\ D} n_P\ P,$$

where $v_P(D){:=}n_P$ are non-zero integers. For a prime divisor $Q \notin \mathrm{Supp}(D)$, we define $v_Q(D){:=}0$. The integer

$$\deg\ D{:=}\sum_{P \in \mathbf{P}_{\mathbb{F}}} v_P(D) \cdot \deg\ P$$

is called the degree of the divisor D.

We define a partial ordering on $\mathrm{Div}(\mathbb{F})$ as follows:

$$D_1 \leq D_2 :\Leftrightarrow v_P(D_1) \leq v_P(D_2) \text{ for all } P \in S(\mathbb{F}|k).$$

A divisor $D \geq 0$ is called effective or positive.

Now, we want to associate a divisor to a non-zero element $x \in \mathbb{F}$. Consider the set of prime divisors Z and N which, respectively, consist of zeros and poles in $S(\mathbb{F}|k)$ of x. Since we know that N and Z are finite subsets of $S(\mathbb{F}|k)$, the divisor (x) associated to x is defined as follows:

$$\begin{aligned} (x) &:= (x)_0 - (x)_\infty \\ \text{where } (x)_0 &:= \sum_{P \in Z} v_P(x) P, && \text{the zero divisor of } x \\ \text{and } (x)_\infty &:= \sum_{P \in N} v_P(x) P, && \text{the pole divisor of } x. \end{aligned}$$

The set of divisors

$$\mathrm{Prin}(\mathbb{F}|k) := \{(x) \,|\, 0 \neq x \in \mathbb{F}\}$$

is called the group of principal divisors of $\mathbb{F}|k$.

Theorem 3.1.1 ([Sti09] Theorem 1.4.11)**.** *Let $\mathbb{F}|k$ be a function field. Let x be a transcendental element of $\mathbb{F}$. Then, we have:*

$$\deg\ (x)_0 = \deg\ (x)_\infty = [\mathbb{F} : k(x)]\,.$$

Definition 3.1.2. *Let D be a divisor of $\mathbb{F}|k$. The space defined by*

$$\mathcal{L}(D) := \{x \in \mathbb{F} | (x) \geq -D\} \cup \{0\}$$

is called the `Riemann-Roch space` (or `linear space`) `associated to` D.

Properties 3.1.3. *Let D be a divisor of $\mathbb{F}|k$. We have:*

1. *$\mathcal{L}(D)$ is a finite vector space over k. We denote its dimension by $l(D)$;*

2. *$\mathcal{L}(0) = k$;*

3. *If $D > 0$, then $\mathcal{L}(D) = \{0\}$;*

4. *The set of integers*

$$\{\deg\ D - l(D) + 1 | D \in \mathrm{Div}(\mathbb{F})\}$$

has a maximum denoted by g. The integer g is a non-negative integer and it is called the `genus` of $\mathbb{F}|k$.

5. *If $\deg(D) \geq 2g - 1$, then $l(D) = \deg\ D + 1 - g$.*

Theorem 3.1.4 (Riemann-Roch Theorem)**.** *Let D be a divisor of $\mathbb{F}|k$. There exists a uniquely determined divisor W, called* `the canonical divisor` *of $\mathbb{F}|k$, such that:*

$$l(D) = \deg\, D + 1 - g + l(W - D).$$

Therefore, we have:

$$\deg\, W = 2g - 2 \quad \textit{and} \quad l(W) = g.$$

To end this introductory section, let us recall the Riemann-Hurwitz Genus Formula. This formula is one of the important results with the Riemann-Roch Theorem that we shall use in this chapter. For that, we need to introduce some notions on algebraic extensions of function fields. More details can be found in [Sti09] or [Sal06].

Definition 3.1.5. *A function field $\mathbb{F}'|k'$ is called an extension of $\mathbb{F}|k$ if $\mathbb{F}'|\mathbb{F}$ and $k'|k$ are field extensions. We call the function field $\mathbb{F}|k$ sub-extension of $\mathbb{F}'|k'$ and we simply write $\mathbb{F}'|\mathbb{F}$ if $k = k'$.*

Throughout this thesis, every extension of function fields is assumed to be finite, algebraic and they have the same constant field denoted by k.

Let $\mathbb{F}|\mathbb{E}$ be an extension of function fields. Consider a prime divisor P of $\mathbb{E}$. Denote by $\mathcal{O}_P$ the valuation ring which corresponds to the place P. A place P', the maximal ideal of an extension of the valuation ring $\mathcal{O}_P$, is called `an extension of` P. We also say that P' `lies over` P or P `lies under` P' and we write $P'|P$. We shall denote the ramification index $e\left(\mathcal{O}_{P'}|\mathcal{O}_P\right)$ and the residue degree $f\left(\mathcal{O}_{P'}|\mathcal{O}_P\right)$ by $e(P'|P)$ and $f(P'|P)$ respectively.

We say that $P'|P$ is `unramified` if $e(P'|P) = 1$, and it is said to be `ramified` otherwise. The place P is `unramified` (resp. `ramified`) in $\mathbb{F}|\mathbb{E}$ if all extensions $P'|P$ are unramified (resp. if there exists a ramified extension $P'|P$). An extension P' of P is said to be `tamely` (resp. `wildly`) ramified if $P'|P$ is ramified and the prime characteristic of k does not divide $e(P'|P)$ (resp. char k divides $e(P'|P)$).

The place P is `unramified` (resp. `ramified`) in $\mathbb{F}|\mathbb{E}$ if all extensions $P'|P$ are unramified (resp. if there exists an ramified extension $P'|P$). The place P is said to be `tamely ramified` (resp. `wildly ramified`) if it is ramified in $\mathbb{F}|\mathbb{E}$ and an extension of P in $\mathbb{F}$ is either unramified or tamely ramified (resp. there is at least one wildly ramified extension of P in $\mathbb{F}$).

Definition 3.1.6. *let $\mathbb{F}|\mathbb{E}$ be an extension of function fields and P be a place of $\mathbb{E}$. Then,*

> *$\mathbb{F}|\mathbb{E}$ is said to be unramified (resp. ramified) if every place $P \in S(\mathbb{E}|k)$ is unramified in $\mathbb{F}|\mathbb{E}$ (resp. at least one place P in $\mathbb{E}$ is ramified in $\mathbb{F}|\mathbb{E}$).*

$\mathbb{F}|\mathbb{E}$ is said to be tame if no place P in $\mathbb{E}$ is wildly ramified in $\mathbb{F}|\mathbb{E}$.

Remark 3.1.7. *By theorem 2.1.5, every place P in $S(\mathbb{E}|k)$ has finitely many extensions $P' \in S(\mathbb{F}|k)$.*

Proposition 3.1.8. *Let $\mathbb{F}|\mathbb{E}$ be an extension of function fields. For every place P' in $\mathbf{P}_{\mathbb{F}}$, there exists a unique place P in $S(\mathbb{E}|k)$ such that P' lies over P and $P = P' \cap \mathbb{E}$. Furthermore, if $P_1, \cdots, P_s$ denote all the places of $\mathbb{F}$ lying over a place $P \in S(\mathbb{E}|k)$, then we have:*

$$\sum_{i=1}^{s} e_i f_i = [\mathbb{F} : \mathbb{E}] \tag{3.1.1}$$

where e_i and f_i denote the ramification index and the residue degree of each $P_i|P$. We call the equality 3.1.1 **`the fundamental equality`** *of the extension $\mathbb{F}|\mathbb{E}$.*

Proof. See [Sti09] Proposition 3.1.7 and Theorem 3.1.11. □

Definition 3.1.9. *Let $\mathbb{F}|\mathbb{E}$ be an extension of function fields. To every place P of $\mathbb{E}$, the divisor of $\mathbb{F}$ defined by:*

$$\mathrm{Con}_{\mathbb{F}|\mathbb{E}}(P) := \sum_{P'|P} e(P'|P) \cdot P'$$

is called **`the conorm`** *of P with respect to $\mathbb{F}|\mathbb{E}$. We call it simply by conorm of P if there is no confusion. We extend this conorm map to an injective homomorphism from $\mathrm{Div}(\mathbb{E})$ to $\mathrm{Div}(\mathbb{F})$ by setting*

$$\mathrm{Con}_{\mathbb{F}|\mathbb{E}}(D) := \sum_{P \in \mathrm{supp}(D)} v_P(D) \cdot \mathrm{Con}_{\mathbb{F}|\mathbb{E}}(P).$$

Remark 3.1.10. *Using the fundamental equality of the extension $\mathbb{F}|\mathbb{E}$, we can easily deduce that, for every divisor $D \in \mathrm{Div}(\mathbb{E})$, we have:*

$$\mathrm{deg}\mathrm{Con}_{\mathbb{F}|\mathbb{E}}(D) = [\mathbb{F} : \mathbb{E}] \deg D.$$

Proposition 3.1.11. *Let $\mathbb{F}|\mathbb{E}$ be an extension of function fields. For a non-zero element $x \in \mathbb{E}$, we have:*

$$\begin{aligned} \mathrm{Con}_{\mathbb{F}|\mathbb{E}}\left((x)_0^{\mathbb{E}}\right) &= (x)_0^{\mathbb{F}} \\ \mathrm{Con}_{\mathbb{F}|\mathbb{E}}\left((x)_\infty^{\mathbb{E}}\right) &= (x)_\infty^{\mathbb{F}} \\ \mathrm{Con}_{\mathbb{F}|\mathbb{E}}\left((x)^{\mathbb{E}}\right) &= (x)^{\mathbb{F}}. \end{aligned}$$

where $(x)_0^{\mathbb{E}}, (x)_\infty^{\mathbb{E}}, (x)^{\mathbb{E}}$ (resp. $(x)_0^{\mathbb{F}}, (x)_\infty^{\mathbb{F}}, (x)^{\mathbb{F}}$ denote the zero, pole, principal divisors of x in $\mathrm{Div}(\mathbb{E})$ (resp. $\mathrm{Div}(\mathbb{F})$).

Proof. See [Sti09] Proposition 3.1.9. □

In order to state the Riemann-Hurwitz genus formula, we need one more important object, namely the different of the extension $\mathbb{F}|\mathbb{E}$.

Let $P \in S(\mathbb{E}|k)$. Consider the ring $\mathcal{O}'_P$, the integral closure of $\mathcal{O}_P$ in $\mathbb{F}$. Using theorem 2.1.5, we know that

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}.$$

The set

$$\mathcal{C}_P := \{x \in \mathbb{F} \,|\, \mathrm{Tr}\,(x \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}\,,$$

where Tr denote the trace map from $\mathbb{F}$ to $\mathbb{E}$ has the following properties:

Properties 3.1.12 ([Sti09] Proposition 3.4.2 and Theorem 3.5.1)**.**

1. *$\mathcal{C}_P$ is an $\mathcal{O}'_P$-module and $\mathcal{O}'_P \subseteq \mathcal{C}_P$.*
2. *There is an element $t \in \mathbb{F}$ such that $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ with $v_{P'}(t) \leq 0$ for all $P'|P$. Moreover, for every $t' \in \mathbb{F}$ such that $\mathcal{C}_P = t' \cdot \mathcal{O}'_P$, we have $v_{P'}(t') = v_{P'}(t)$ for all $P'|P$. The converse is also true. For each $P'|P$, we denote the positive integer $-v_{P'}(t)$ by $d(P'|P)$.*
3. *In general, $d(P'|P) \geq e(P'|P)-1$. We have equality if and only if $e(P'|P)$ is not divisible by* char k *where k is the constant field of $\mathbb{E}$ and $\mathbb{F}$, i.e, the extension $P'|P$ is tamely ramified. Moreover, $d(P'|P) \geq e(P'|P)$ if and only if $P'|P$ is wildly ramified.*
4. *For all but only finitely many $P \in S(\mathbb{E}|k)$, we have $\mathcal{C}_P = \mathcal{O}'_P$. Thus, almost all places P in $\mathbb{E}$ are unramified in $\mathbb{F}|\mathbb{E}$.*

The $\mathcal{O}'_P$-module $\mathcal{C}_P$ is called ***the complementary module over*** *$\mathcal{O}_P$.*

Hence, the following definition makes sense:

Definition 3.1.13. *Let $\mathbb{F}|\mathbb{E}$ be an extension of function fields. The effective divisor defined by*

$$\mathrm{Diff}(\mathbb{F}|\mathbb{E}) := \sum_{P \in \mathbf{P}_{\mathbb{E}}} \sum_{P'|P} d(P'|P) \cdot P'$$

is called ***the different*** *of $\mathbb{F}|\mathbb{E}$.*

Theorem 3.1.14 (Riemann-Hurwitz Genus Formula)**.** *Let $\mathbb{F}|\mathbb{E}$ be a separable extension of function fields. Then, we have:*

$$2g_{\mathbb{F}} - 2 = [\mathbb{F} : \mathbb{E}]\,(2g_{\mathbb{E}} - 2) + \deg\ \mathrm{Diff}(\mathbb{F}|\mathbb{E})$$

where $g_{\mathbb{F}}$ and $g_{\mathbb{E}}$ denote the genus of $\mathbb{F}$ and $\mathbb{E}$ respectively.

An important application of the Riemann-Hurwitz genus formula is the following:

Corollary 3.1.15 (Luroth's Theorem)**.** *Every subfield of a rational function field is rational.*

3.2 The Divisor Reduction Map

For an arbitrary function field $\mathbb{F}|k$, we define a positive divisor $(M)_\infty$ associated to any finite-dimensional k-module M of $\mathbb{F}$ as follows:

$$(M)_\infty = \{\sup(x)_\infty \mid 0 \neq x \in M\}\,.$$

Lemma 3.2.1. *Let $\mathbb{F}|k$ be a function field with constant field k which is assumed to be infinite. Let M be a finite-dimensional k-module. Then there exists $x \in M$ such that*

$$(x)_\infty = (M)_\infty.$$

Proof. By definition, the divisor $(M)_\infty$ is a positive divisor. So, we may assume $(M)_\infty > 0$. Let $P_1, P_2, \cdots, P_r$ be the prime divisors in $\mathrm{Supp}(M)_\infty$ with multiplicities $n_1, n_2, \cdots, n_r$. Let v_i be the discrete valuation which corresponds to the place P_i for each i. Then, there exist $x_i \in M$ such that $v_i(x_i) = -n_i$. For each i, let N_i be the submodule of M consisting of all $y \in M$ with the property $v_i(y) > -n_i$. Clearly, $N_i \subsetneqq M$. So, we can consider a maximal submodule of M_i which contains N_i for each i. Let $u_1, u_2, \cdots, u_n$ be a basis of M as a k-module. Thus, every element y in M_i is of the form

$$y = u_1y_1 + u_2y_2 + \cdots + u_ny_n$$

where the y_j's are in k and satisfy the following condition:

$$c_{i1}y_1 + c_{i2}y_2 + \cdots + c_{in}y_n = 0.$$

Note that the c_{ij}'s are fixed in k and depend only on i and the basis of M. If we consider the polynomial

$$f(Y_1, Y_2, \cdots, Y_n) = \prod_{1\leq i\leq r} c_{i1}Y_1 + c_{i2}Y_2 + \cdots + c_{in}Y_n \in k(Y_1, Y_2, \cdots, Y_n),$$

since k is assumed to be infinite, there exist $x_1, x_2, \cdots, x_n \in k$ such that $f(x_1, x_2, \cdots, x_n) \neq 0$. Thus, the element $x = u_1x_1 + u_2x_2 + \cdots + u_nx_n \in M$

is not contained in any of the M_i. Hence, $v_i(x) \leq -n_i$ i.e $(x)_\infty \geq (M)_\infty$. On the other hand, by definition of $(M)_\infty$, we have $(x)_\infty \leq (M)_\infty$ for all nonzero element x of M. Therefore, $(x)_\infty = (M)_\infty$. □

Without loss of generality, let us assume that the constant field k has infinitely many elements (Even if the arithmetic divisor homomorphism of Deuring that we are going to discuss now still exists and is well-defined in the case when k is finite).

Let us now consider a valued function field $(\mathbb{F}|k, v)$ where v denotes a constant reduction on $\mathbb{F}$. Assume first that v is a good reduction. According to Deuring (see [Deu42]), when the valuation v is discrete, there is *a natural homomorphism*

$$\mathbf{h} : \text{Div}(\mathbb{F}|k) \rightarrow \text{Div}(\mathbb{F}v|kv)$$

defined by: For any divisor $A \in \text{Div}(\mathbb{F}|k)$ of sufficiently large degree,

$$\mathbf{h}(A){:=}\overline{A}{=}\,(\mathcal{L}(A)v)_\infty$$

where $\mathcal{L}(A)$ is the Riemann-Roch space associated to A and for a given divisor $A \in \text{Div}(\mathbb{F}|k)$, we write $A = B - C$ where B and C are divisors of $\mathbb{F}|k$ of sufficiently large degree, then

$$\overline{A} = \overline{B} - \overline{C}.$$

The homomorphism $\mathbf{h}$ is unique with the following properties $(*)$:

$$A \leq B \Rightarrow \overline{A} \leq \overline{B}, \tag{3.2.1}$$

$$\overline{(x)} = (\overline{x}) \quad (\text{if } \overline{x} \neq 0, \infty), \tag{3.2.2}$$

$$\text{deg}A = \text{deg}\overline{A}. \tag{3.2.3}$$

Note that for a function field $\mathbb{F}|k$, a divisor $A \in \text{Div}(\mathbb{F}|k)$ is said to be sufficiently large if $\text{deg}A \geq 2g - 1$, where g is the genus of $\mathbb{F}$. We call such homomorphism `the arithmetic divisor homomorphism of` $\mathbb{F}$. In [Roq87], Roquette gives a proof that such homomorphism still exists in the general case. So, all we need is that v to be a good reduction.

Remark 3.2.2. *When the constant field k is assumed to be algebraically closed, note that the homomorphism $\mathbf{h}$ is surjective. For a proof, see [Roq87]. However, if we assume that $(\mathbb{F} = k(x), v)$ is rational, then the corresponding homomorphism $\mathbf{h}$ is also surjective. Indeed, one considers the Gauss valuation $v{:=}v_x$, the homomorphism $\mathbf{h}$ is defined as follows: Let P be a place in $\mathbb{F}$. If $P = P_\infty$, then we choose the infinite place in $\mathbb{F}v$ to be the image of P. Otherwise, there exists an irreducible polynomial $p(x)$ in $\mathbb{F}$ such that $P = P_{p(x)}$. In this case, if*

$$\overline{p}(\overline{x}) = \prod_i \overline{p}_i(\overline{x})^{n_i}$$

is the factorisation of the reduction of $p(x)$ modulo v as a product of irreducible polynomials in $\mathbb{F}v$ up to unit, we set

$$\mathbf{h}(P){:=}\sum_i n_i \cdot P_{\overline{p}(\overline{x})}.$$

In [GMP90], Green, Matignon and Pop give a generalisation of the homomorphism $\mathbf{h}$ as follows.

Let V be a finite set of valuations on $\mathbb{F}$. Suppose there is a V-regular element f for $\mathbb{F}|k$. Let us recall the infnorm w that we defined in the last section of chapter 1.

The set $S(\mathbb{F}|k)$(resp. $S(\mathbb{F}v|kv)$ for $v \in V$) being the set of prime divisors of $\mathbb{F}|k$ (resp. $\mathbb{F}v|kv$) and set

$$S(\mathbb{F}w|kw){:=}\bigcup_v S(\mathbb{F}v|kv).$$

For a given divisor $A \in \mathrm{Div}(\mathbb{F}|k)$ we define

$$\mathcal{A}_f = \{x \in \mathbb{F} \mid \forall P \in S_f, v_P(x) \geq v_P(A)\}\,, \text{ where } S_f = \{P \in S(\mathbb{F}|k) \mid fP \neq \infty\}\,.$$

Denote by $(\mathcal{A}_f w)'$ the fractional $(Rw)'$-ideal, $\mathcal{A}_f w(Rw)'$, where R is the integral closure of $k\,[f]$ in $\mathbb{F}$ and Rw denotes the reduction of R with respect to w. Then the `divisor reduction map`

$$\mathbf{r} : \mathrm{Div}(\mathbb{F}|k) \to \mathrm{Div}(\mathbb{F}w|kw){:=}\sum_v \mathrm{Div}(\mathbb{F}v|kv).$$

is defined by:

$$\mathbf{r}(A) = Aw = \sum_v Av,$$

where for each $v \in V, Av \in \mathrm{Div}(\mathbb{F}v|kv)$ and

$$v_Q(Av) = \begin{cases} v_Q(\mathrm{pr}_v((\mathcal{A}_f w)')) & \text{for } Q \in S(\mathbb{F}v|kv),\ fv(Q) \neq \infty, \\ v_Q(\mathrm{pr}_v((\mathcal{A}_{f^{-1}} w)')) & \text{for } Q \in S(\mathbb{F}v|kv),\ fv(Q) \neq 0. \end{cases}$$

where pr_v is the projection from $\mathbb{F}w$ onto $\mathbb{F}v$. We call this divisor map as the divisor reduction map associated to the set of valuations V. Note that, by definition, the divisor reduction map depends also on the V-regular element f.

If we define the set of prime divisors

$$S_f^0 = \left\{P \in S(\mathbb{F}|k) : v_k(fP) = 0 \text{ and } \mathrm{supp}(N_{k(f)}^{\mathbb{F}}(P)w) \cap \mathrm{supp}(\mathcal{F}w) = \emptyset\right\}$$

where $\mathcal{F}w$ is the conductor of $(Rw)'$ in Rw and denote by $\mathrm{Div}_f^0(\mathbb{F}|k)$ the subgroup of $\mathrm{Div}(\mathbb{F}|k)$ of divisors with support in S_f^0, then the restriction of the divisor reduction map $\mathbf{r}$ on $\text{Div}_f^0(\mathbb{F}|k)$ is a degree preserving homomorphism ([GMP90] theorem 2.2). Furthermore, we have

$$\mathcal{L}(A)w \subseteq \mathcal{L}(Aw)$$

for any divisor $A \in \text{Div}_f^0(\mathbb{F}|k)$ where $\mathcal{L}$ denotes the Riemann-Roch space operator acting on divisors and $\mathcal{L}(A)w := \prod_{v\in V} \mathcal{L}(Av)$.

Remark 3.2.3. *Let $(\mathbb{F}|k, v)$ be a valued function field. If we assume that the valuation v is a good reduction, then the arithmetic divisor homomorphism $\mathbf{h}$ coincides with the reduction divisor homomorphism associated to $\{v\}$. This is true because, on one hand, the arithmetic divisor homomorphism is unique with the properties $(\star)$. On the other hand, the homomorphism $\mathbf{r}$ satisfies these properties on $\text{Div}_f^0(\mathbb{F}|k)$.*

Now we will introduce an important theorem, called the `Inertia Theorem`, that we will use to compare the Riemann-Roch spaces $\mathcal{L}(A)v$ and $\mathbf{h}(\mathcal{A})$.

Definition 3.2.4. *Let $(\mathbb{F}|k, v)$ be a valued function field. Any finite k-module $N \subset \mathbb{F}$ is said to be inert if $\dim_k N = \dim_{kv} Nv$ where Nv is the image of $N \cap \mathcal{O}_{\mathbb{F}}$ under the residue map ($\mathcal{O}_{\mathbb{F}}$ is the valuation ring of v). More generally, any k-module M of $\mathbb{F}$ is inert if every finite-dimensional k-submodule N of M is inert.*

The next theorem is due to Roquette from one of his unpublished papers.

Theorem 3.2.5 (Inertia Theorem)**.** *Let $(\mathbb{F}|k, v)$ be a valued function field in one variable with v-regular elements. Then every k-module of $\mathbb{F}$ is inert.*

Proposition 3.2.6. *Let $(\mathbb{F}|k, v)$ be a valued function field. Suppose that the valuation v is a good reduction. Then, for any sufficiently large divisor $A \in$ $\text{Div}(\mathbb{F}|\mathbb{E})$, we have*

$$\mathcal{L}(A)v = \mathcal{L}(\mathbf{h}(A)).$$

Proof. We observe that, by definition of the homomorphism $\mathbf{h}$, we have

$$\mathcal{L}(A)v \subseteq \mathcal{L}(\mathbf{h}(A))$$

and there exists a v-regular element in $\mathbb{F}$ such that

$$(x)_\infty = A,\ (\overline{x})_\infty = \mathbf{h}(A),\ \text{deg}A = \text{deg}\mathbf{h}(A).$$

According to the Inertia Theorem, we have

$$l(A){:=}\dim_k \mathcal{L}(A) = \dim_{kv} \mathcal{L}(A)v.$$

On the other hand, since v is a good reduction, using Riemann-Roch Theorem,

$$1 - g = l(A) - \deg A = l(\mathbf{h}(A)) - \deg\mathbf{h}(A)$$

where g is the genus of $\mathbb{F}$. Hence,

$$\dim_{kv}\mathcal{L}(A)v = l(A) = l(\mathbf{h}(A)) = \dim_{kv}\mathcal{L}(\mathbf{h}(A)).$$

□

Now let $(\mathbb{F}|k, v)$ be a valued function field. Assume the valuation v is a good reduction. The following result that we will state without proof was proved by Youssefi in [You93] in the special case of rank 1 valuations and generalised in the general case later by Green in [Gre96]:

Theorem 3.2.7. *Let $\mathbb{E}|k$ be a sub-extension of $\mathbb{F}|k$. Then, the restriction of the valuation v in $\mathbb{E}$ is also a good reduction.*

Our first result is the following:

Lemma 3.2.8. *Let $(\mathbb{F}|k, v)$ be a valued function field where the valuation v is assumed to be a good reduction. Let $\mathbb{E}|k$ be a sub-extension of $\mathbb{F}|k$ such that $[\mathbb{F} : \mathbb{E}] = [\mathbb{F}v : \mathbb{E}v]$. Then the following diagram is commutative:*

$$\begin{tikzcd} \mathrm{Div}(\mathbb{E}|k) \arrow[r, "\mathbf{h}_{\mathbb{E}}"] \arrow[d, "\mathbf{c}"] & \mathrm{Div}(\mathbb{E}v|kv) \arrow[d, "\overline{\mathbf{c}}"] \\ \mathrm{Div}(\mathbb{F}|k) \arrow[r, "\mathbf{h}"] & \mathrm{Div}(\mathbb{F}v|kv) \end{tikzcd}$$

where $\mathbf{c}$ and $\overline{\mathbf{c}}$ are respectively the conorm with respect to $\mathbb{F}|\mathbb{E}$ and $\mathbb{F}v|\mathbb{E}v$. The divisor reduction maps $\mathbf{h}_{\mathbb{E}}$ and $\mathbf{h}$ are respectively the arithmetic divisor reduction map on $\mathbb{E}$ and $\mathbb{F}$.

Proof. Note that by Theorem 3.2.7, the restriction of v on $\mathbb{E}$ is also a good reduction, so the homomorphism $\mathbf{h}_{\mathbb{E}}$ is precisely the arithmetic divisor map on $\mathbb{E}$. Since $\mathbf{h}$ and $\mathbf{h}_{\mathbb{E}}$ are degree preserving divisor homomorphism, it suffices to prove the proposition for a given divisor $A \in \mathrm{Div}(\mathbb{E}|k)$ with sufficiently large degree. By definition of the homomorphism $\mathbf{h}_{\mathbb{E}}$ and using Lemma 5.1.6, there exists $x \in \mathbb{E}$ such that

$$(\overline{x})_\infty = \mathbf{h}_{\mathbb{E}}(A) = \overline{A}, \quad (x)_\infty \leq A, \text{and } \deg\overline{A} = \deg A.$$

But, we know that

$$\deg\overline{A} = \deg(\overline{x})_\infty = [\mathbb{F}v : kv(\overline{x})] \leq [\mathbb{F} : k(x)] = \deg(x)_\infty.$$

Hence

$$(x)_\infty = A.$$

On the other hand, we have:

$$\mathbf{c}(A) = (x)_\infty^{\mathbb{F}}, \quad \overline{\mathbf{c}}(\mathbf{h}_{\mathbb{E}}(A)) = (\overline{x})_\infty^{\mathbb{F}v}$$

where $(x)_\infty^{\mathbb{F}}$ and $(x)_\infty^{\mathbb{F}v}$ are the pole divisors of x and $\overline{x}$ respectively in $\mathbb{F}$ and in $\mathbb{F}v$. Furthermore, by definition of $\mathbf{h}$, we have

$$\mathcal{L}(\mathbf{c}(A))v \subset \mathcal{L}(\mathbf{h}(\mathbf{c}(A)))$$

which means

$$\overline{\mathbf{c}}(\mathbf{h}_{\mathbb{E}}(A)) = (\overline{x})_\infty^{\mathbb{F}v} \leq \mathbf{h}(\mathbf{c}(A)).$$

Since

$$\deg\overline{\mathbf{c}}(\mathbf{h}_{\mathbb{E}}(A)) = \deg(\overline{x})_\infty^{\mathbb{F}v} = [\mathbb{F}v : \mathbb{E}v] \deg\mathbf{h}_{\mathbb{E}}(A) = \deg\mathbf{c}(A) = \deg\mathbf{h}(\mathbf{c}(A)),$$

it follows that

$$\overline{\mathbf{c}}(\mathbf{h}_{\mathbb{E}}(A)) = \mathbf{h}(\mathbf{c}(A)).$$

□

More generally, let $\mathbb{E}|k$ be a sub-extension of $\mathbb{F}|k$. Denote by $v_{\mathbb{E}}$ the restriction of v on $\mathbb{E}$ where, now, v is not necessarily a good reduction on $\mathbb{F}$. Let V be the finite set of prolongations of $v_{\mathbb{E}}$ to $\mathbb{F}$ and assume that we have:

$$[\mathbb{F}:\mathbb{E}] = \sum_{v \in V} [\mathbb{F}v:\mathbb{E}v_{\mathbb{E}}].$$

Suppose there is a $v_{\mathbb{E}}$ regular element on $\mathbb{E}$. Consider the divisor reduction maps $\mathbf{r}_{\mathbb{E}}$ and $\mathbf{r}$ respectively associated to the set of valuations $\{v_{\mathbb{E}}\}$ and V. Since a $v_{\mathbb{E}}$-regular element in $\mathbb{E}$ is also V-regular in $\mathbb{F}$, we expect the following generalisation of Lemma 3.2.8 (Of course, the V-regular element we use to define the reduction map $\mathbf{r}$ has to be the same as for the divisor map $\mathbf{r}_{\mathbb{E}}$). At present we are unable to prove this.

Conjecture 3.2.9. *Let $(\mathbb{F}|k, v)$ be a valued function field. Let $\mathbb{E}|k$ be a sub-extension of $\mathbb{F}|k$. Then the following diagram is commutative:*

$$\begin{tikzcd}
\mathrm{Div}(\mathbb{E}|k) \arrow[r, "\mathbf{r}_{\mathbb{E}}"] \arrow[d, "\mathbf{c}"] & \mathrm{Div}(\mathbb{E}v|kv) \arrow[d, "\overline{\mathbf{c}}"] \\
\mathrm{Div}(\mathbb{F}|k) \arrow[r, "\mathbf{r}"] & \mathrm{Div}(\mathbb{F}w|kv)
\end{tikzcd}$$

where $\mathbf{c}$ *is the conorm with respect to* $\mathbb{F}/\mathbb{E}$, *the homomorphism* $\mathbf{r}$ *is the divisor map, as defined in the section 1, associated to the set* $V = \{v = v_1, v_2, \cdots, v_s\}$

of prolongation of $v|_{\mathbb{E}}$ to $\mathbb{F}$, the infnorm w is associated to V and we define the map $\overline{\mathbf{c}}$ by:

$$\overline{\mathbf{c}}(Av) = \sum_{v_i \in V} \mathrm{Con}_{\mathbb{F}v_i/\mathbb{E}v}(Av)$$

for a given $Av \in \mathrm{Div}(\mathbb{E}v|kv)$.

3.3 Some Applications

Let $\mathbb{F}|\mathbb{E}$ be an extension of function fields. Assume we have a good reduction v on $\mathbb{F}$. Our first application is about the relationship between the reduction of the different of $\mathbb{F}|\mathbb{E}$ under the good reduction v and the different of the corresponding residue extension of function fields $\mathbb{F}v|\mathbb{E}v$.

Lemma 3.2.8 gives a relation between the divisors on $\mathbb{F}$ and $\mathbb{E}$ with their reduction respectively via the arithmetic homomorphisms $\mathbf{h}$ and $\mathbf{h}_{\mathbb{E}}$ where $\mathbb{E}$ is a subextension of $\mathbb{F}$ with the property $[\mathbb{F} : \mathbb{E}] = [\mathbb{F}v : \mathbb{E}v]$. So, a natural question to ask is what happens to the different of the extension $\mathbb{F}|\mathbb{E}$ under reduction. In [Kas90] Lemma 2.4.2, Kasser proved that the reduction, via the arithmetic homomorphism $\mathbf{h}$, of the different of $\mathbb{F}|k(x)$ is exactly the different of $\mathbb{F}v|k(x)v$ where x is a v-regular element in $\mathbb{F}$. Our next lemma is a generalisation of that lemma.

Lemma 3.3.1. *Let $(\mathbb{F}|k, v)$ be a valued function field with the same hypothesis as in Lemma 3.2.8. Suppose that both of the extensions $\mathbb{F}|\mathbb{E}$ and $\mathbb{F}v|\mathbb{E}v$, are separable. If the extension $\mathbb{F}|\mathbb{E}$ is tame, then*

$$\mathbf{h}\left(\mathrm{Diff}(\mathbb{F}|\mathbb{E})\right) = \mathrm{Diff}(\mathbb{F}v|\mathbb{E}v). \tag{3.3.1}$$

In particular, the extension $\mathbb{F}v|\mathbb{E}v$ is also tame.

Proof. Let $\overline{P}$ be a prime divisor of $\mathrm{Div}(\mathbb{E}v|kv)$. Since the homomorphism $\mathbf{h}_{\mathbb{E}}$ is surjective, there exists a prime divisor $P \in \mathrm{Div}(\mathbb{E}|k)$ such that $\mathbf{h}_{\mathbb{E}}(P) = \overline{P}$. Using Proposition 3.2.8, we have

$$\mathbf{h}(\mathbf{c}(P)) = \overline{\mathbf{c}}(\overline{P}). \tag{3.3.2}$$

Denote respectively by S and $\overline{S}$ the finite set of places of $\mathbb{F}|k$ and $\mathbb{F}v|kv$ lying over P and $\overline{P}$. Let $\overline{P'} \in \overline{S}$. By the equation 3.3.2, there exists a prime divisor P' in S such that $\mathbf{h}(P') = \overline{P'}$. Furthermore, the cardinality of the set $\overline{S}$ is less than or equal to the cardinal of S. Otherwise, there would exist at least two different places in $\overline{S'}$ which have the same preimage in S. Hence, we have:

$$\sum_{\overline{P'} \in \overline{S}} \overline{P'} \leq \mathbf{h}(\sum_{P' \in S} P').$$

Since the extension $\mathbb{F}|\mathbb{E}$ is tame by hypothesis,

$$\begin{aligned}\mathbf{h}\left(\mathrm{Diff}(\mathbb{F}|\mathbb{E})\right) &= \sum_{P\in\mathbb{P}_{\mathbb{F}}}\left(\mathbf{h}(\mathbf{c}(P)) - \mathbf{h}(\sum_{P'\in S} P')\right)\\ &\leq \sum_{\overline{P}\in\{\mathbf{h}_{\mathbb{E}}(P)|P\in\mathbb{P}_{\mathbb{F}}\}}\left(\overline{\mathbf{c}}(\overline{P}) - \sum_{\overline{P'}\in\overline{S}}\overline{P'}\right)\\ &\leq \mathrm{Diff}(\mathbb{F}v|\mathbb{E}v).\end{aligned}$$

Since both of the extensions $\mathbb{F}|\mathbb{E}$ and $\mathbb{F}v|\mathbb{E}v$ are separable, using the Riemann-Hurwitz genus formula, we get:

$$\mathrm{degDiff}(\mathbb{F}|\mathbb{E}) = 2g_{\mathbb{F}} - 2 - [\mathbb{F}{:}\mathbb{E}]\,(g_{\mathbb{E}} - 1) \qquad (3.3.3)$$

and

$$\mathrm{degDiff}(\mathbb{F}v|\mathbb{E}v) = 2g_{\mathbb{F}v} - 2 - [\mathbb{F}v{:}\mathbb{E}v]\,(g_{\mathbb{E}v} - 1) \qquad (3.3.4)$$

where $g_{\mathbb{F}}, g_{\mathbb{E}}, g_{\mathbb{F}v}$ and $g_{\mathbb{E}v}$ denote the genera of the function field $\mathbb{F}, \mathbb{E}, \mathbb{F}v$ and $\mathbb{E}v$ respectively. However by hypothesis, we have $[\mathbb{F} : \mathbb{E}] = [\mathbb{F}v : \mathbb{E}v]$ and $g_{\mathbb{F}} = g_{\mathbb{F}v}$. By Theorem 3.2.7, we have $g_{\mathbb{E}} = g_{\mathbb{E}v}$, thus $\mathrm{degDiff}(\mathbb{F}|\mathbb{E}) = \mathrm{degDiff}(\mathbb{F}v|\mathbb{E}v)$. Therefore,

$$\mathbf{h}\left(\mathrm{Diff}(\mathbb{F}|\mathbb{E})\right) = \mathrm{Diff}(\mathbb{F}v|\mathbb{E}v).$$

□

Remark 3.3.2. *In the proof of Proposition 3.3.1, without using Theorem 3.2.7, we observe that we would have*

$$\mathbf{h}\left(\mathrm{Diff}(\mathbb{F}|\mathbb{E})\right) = \mathrm{Diff}(\mathbb{F}v|\mathbb{E}v)$$

if for each $\overline{P} \in \mathrm{Div}(\mathbb{E}v|kv)$ there exists $P \in \mathrm{Div}(\mathbb{E}|k)$ such that

$$\mathrm{h}(c(P)) = \overline{c}(\overline{P})$$

and the extension $\mathbb{F}v|\mathbb{E}v$ is tame. Thus, we have an "elementary proof" of Theorem 3.2.7 in this case.

Examining the proof of Proposition 3.2.6, we now observe that v is a good reduction if and only if for a sufficiently large divisor $A \in \mathrm{Div}(\mathbb{F}|k)$, we have

$$\mathcal{L}(A)v = \mathcal{L}(\mathbf{h}(A)). \qquad (3.3.5)$$

A natural question to ask is: What happen to the divisors with degree less than $2g - 1$ under reduction? Under which conditions would any divisor of $\mathbb{F}|k$ verify the equation 3.3.5? The following theorem is an answer to these questions in the case when the function field is hyperelliptic. Before proving this we first recall a lemma from [Sal06]:

Lemma 3.3.3. *Let $\mathbb{F}|k$ be a hyperelliptic function field. Let W be the canonical divisor of $\mathbb{F}|k$ and A be a positive divisor in $\mathbb{F}|k$, then we have:*

$$l(W - A) = g - \mu.$$

where $\mu = \min\left\{\deg_{k(x)}(A \cap k(x)), g\right\}$.

Proof. [Sal06] lemma 14.2.66. □

We have:

Theorem 3.3.4. *Let $(\mathbb{F}|k, v)$ be a valued hyperelliptic function field. Assume that the valuation v is a good reduction. Then, if* $\mathbf{h}$ *denotes the arithmetic divisor homomorphism map from* $\operatorname{Div}(\mathbb{F}|k)$ *to* $\operatorname{Div}(\mathbb{F}v|kv)$, *for any positive divisor* $A \in \operatorname{Div}(\mathbb{F}|k)$, *we have:*

$$\mathcal{L}(A)v = \mathcal{L}(\mathbf{h}(A)).$$

Proof. Denote by W the canonical divisor of $\mathbb{F}|k$. First, let us prove that $\mathbf{h}(W)$ is the canonical divisor of $\overline{\mathbb{F}}|\overline{k}$. For that, let $\overline{x} \in \overline{F}$ such that $\left[\overline{F} : \overline{k}(\overline{x})\right] = 2$. Since $\mathbb{F}|k$ is a good lifting of $\overline{\mathbb{F}}|\overline{k}$, there exists $x \in \mathbb{F}$ such that $\overline{x}$ is the reduction of x and we have $[\mathbb{F} : k(x)] = 2$. But, it is well known that the divisors $(g-1)(x)_\infty^{\mathbb{F}}$ and $(g-1)(\overline{x})_\infty^{\overline{\mathbb{F}}}$ are respectively canonical divisors of $\mathbb{F}$ and $\overline{\mathbb{F}}$ where g denotes the genus of both of the function fields $\mathbb{F}$ and $\overline{\mathbb{F}}$. Since x is a regular element with respect to the valuation v, we have $\mathbf{h}((x)_\infty^{\mathbb{F}}) = (\overline{x})_\infty^{\overline{\mathbb{F}}}$ using the proposition 3.2.8. Thus $\mathbf{h}(W)$ is a canonical divisor of $\overline{\mathbb{F}}|\overline{k}$.

Let A be a positive divisor in $\mathbb{F}|k$ and $\mathfrak{B}$ a prime divisor in $\operatorname{supp}(A)$. By the lemma 3.2.8, we have:

$$\mathbf{h}_{k(x)}(\mathfrak{B} \cap k(x)) = \mathbf{h}(\mathfrak{B}) \cap \overline{k}(\overline{x}).$$

Therefore,

$$\mathbf{h}_{k(x)}(A \cap k(x)) = \mathbf{h}(A) \cap \overline{k}(\overline{x}).$$

Since $\mathbf{h}$ and $\mathbf{h}_{k(x)}$ are degree preserving homomorphisms,

$$\deg_{k(x)}(A \cap k(x)) = \deg_{\overline{k}(\overline{x})}(\mathbf{h}(A) \cap \overline{k}(\overline{x})).$$

Using the lemma 3.3.3 we have:

$$l(W - A) = l(\mathbf{h}(W - A)). \tag{3.3.6}$$

However, by the definition of $\mathbf{h}$,

$$\mathcal{L}(A)v \subset \mathcal{L}(\mathbf{h}(A)).$$

Using the Riemann-Roch Theorem, we obtain:

$$1 - g = l(A) - \deg A - l(W - A) = l(\mathbf{h}(A)) - \deg\mathbf{h}(A) - l(\mathbf{h}(W - A)).$$

On the other hand, by the Inertia Theorem, we have $\dim_{kv}\mathcal{L}(A)v = l(A)$ and since $\mathbf{h}$ is a degree preserving homomorphism, $\deg A = \deg\mathbf{h}(A)$. Hence

$$\mathcal{L}(A)v = \mathcal{L}(\mathbf{h}(A)). \tag{3.3.7}$$

□

To end this chapter, as a corollary of Theorem 3.3.4, let us give an alternative proof of the fact that the gap sequence of a hyperelliptic curve of genus g is classical, that is $\{1, 2, \cdots, g\}$.

Definition 3.3.5. *Let P be a prime divisor for a given function field $\mathbb{F}|k$. A positive integer n is called a pole number of P if there exists an element $x \in \mathbb{F}$ such that $(x)_\infty = nP$. Otherwise n is said to be a gap number of P.*

Let $\mathbb{F}|k$ be a function field with genus $g{>}1$ where k is assumed to be algebraically closed. Let us assume the following results (see [Sal06]): For a given prime divisor $P \in \mathrm{Div}(\mathbb{F}|k)$, the are exactly g gap numbers $1 = i < \cdots < i_g \leq 2g - 1$ of P. We denote by G_P the sequence of the g gap numbers of P and we call it the gap sequence of P. Note also that almost all places of $\mathbb{F}|k$ have the same gap sequence. Such places are called ordinary places. And the gap sequence of all ordinary places is said to be the gap sequence of the function field $\mathbb{F}|k$. A non-ordinary place is called a Weierstrass point of $\mathbb{F}|k$. If $\mathbb{F}|k$ is of characteristic 0, then its gap sequence is $G_0 = \{1, 2, \cdots, g\}$.

Now, as a corollary of Theorem 3.3.4, we have:

Corollary 3.3.6. *Let $\mathbb{F}|k$ be a hyperelliptic function field of characteristic $p \geq 0$. Then the gap sequence of $\mathbb{F}|k$ is G_0.*

Proof. Since it is well known that a function field of genus $g > 1$ and characteristic 0 has G_0 as gap sequence, then we may assume that $p > 0$. Consider a hyperelliptic function field, a good lift[1] of $\mathbb{F}|k$, denoted by $\mathbb{F}_0|k_0$ in characteristic 0.

Now let P_0 be a prime divisor in $\mathbb{F}_0|k_0$ and denote by P its image by the divisor homomorphism $\mathbf{h}$. Using Theorem 3.3.4, for any $n \in \mathbb{N}$, we have:

$$l(nP_0) = l(nP).$$

Thus, P_0 and P have the same gap sequence. Consider an infinite set S of ordinary prime divisors of $\mathbb{F}|k$. The homomorphism $\mathbf{h}$ is surjective, so the set S_0 which is the preimage of S is also an infinite set of prime divisors in $\mathbb{F}_0|k_0$. However, we know that each prime divisor in S_0 has the same gap sequence as the ordinary prime divisors in S. Since S_0 is an infinite set of prime divisors in $\mathbb{F}_0|k_0$, we conclude that $\mathbb{F}_0|k_0$ and $\mathbb{F}|k$ have the same gap sequence. Hence, the gap sequence of $\mathbb{F}|k$ is precisely G_0. □

[1] For a definition, one can refer to Chapter 5.

Chapter 4

Reduction of the Automorphism Group

In this chapter, we investigate properties of the automorphism group of a function field over a field k in relation to its reductions with respect to special valuations. Our motivation is to generalise a theorem by Deligne and Mumford in [DM69] (Theorem 4.2.4) that we will discuss in the second section. In order to give our main results, we first recall some general results on automorphism groups of function fields. The main new results in this chapter are Lemma 4.3.3 and Theorem 4.3.5.

Throughout this chapter, unless otherwise specified, the field k is assumed to be algebraically closed and any function field has genus ≥ 2.

4.1 Automorphism group of function fields

Let $\mathbb{F}|k$ be a function field. Denote by g its genus and by p the characteristic of the field k. Let us consider the automorphism group of the function field $\mathbb{F}$ defined by

$$G = \mathrm{Aut}(\mathbb{F}|k) := \{\sigma : \mathbb{F} \to \mathbb{F} \mid \sigma \text{ a field automorphism such that } \sigma|_k = \mathrm{Id}_k\}\,.$$

It is well known that the group G is of infinite order if and only if $g = 0$ or 1. Furthermore, we have:

1. If $g = 0$, then G is isomorphic to the projective linear group $\mathrm{PGL}_2(k)$.

2. If $g = 1$, then G is isomorphic to

$$\begin{aligned} \mathrm{Cl}^0(\mathbb{F}) \rtimes \mathbb{Z}/2\mathbb{Z}, &\quad j \neq 0, 1728 \\ \mathrm{Cl}^0(\mathbb{F}) \rtimes \mathbb{Z}/4\mathbb{Z}, &\quad j = 1728; p \notin \{2,3\} \\ \mathrm{Cl}^0(\mathbb{F}) \rtimes \mathbb{Z}/6\mathbb{Z}, &\quad j = 0; p \notin \{2,3\} \\ \mathrm{Cl}^0(\mathbb{F}) \rtimes \left(\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}\right), &\quad j = 0, 1728; p = 3 \\ \mathrm{Cl}^0(\mathbb{F}) \rtimes \left(Q_8 \rtimes \mathbb{Z}/3\mathbb{Z}\right), &\quad j = 0, 1728; p = 2 \end{aligned}$$

where j is the j-invariant of the elliptic function field $\mathbb{F}$. The group $\mathrm{Cl}^0(\mathbb{F})$ denotes the group of divisor classes $\mathrm{Div}(\mathbb{F})/\mathrm{Prin}(\mathbb{F})$ of $\mathbb{F}$. It is a normal subgroup of G and an infinite abelian group. Note that the semi-products are all non-trivial.

Now suppose that the genus of the function field $\mathbb{F}|k$ is $g \geq 2$. Then:

Theorem 4.1.1 (Hurwitz)**.** *The group* $\mathrm{Aut}(\mathbb{F}|k)$ *is finite. Moreover, if* $p = 0$ *or* $\geq 2g+2$, *we have*

$$|\mathrm{Aut}(\mathbb{F}|k)| \leq 84(g-1). \tag{4.1.1}$$

Proof. See [Sal06] Theorem 14.3.13. □

Note that, In [Hur93b], Hurwitz first proved Theorem 4.1.1 using the theory of Riemann surfaces, which means, in the case where k is the complex numbers. By the Lefschetz Principle, the theorem also holds over any field of characteristic 0.

Remark 4.1.2. *We observe that in the proof of Theorem 4.1.1 in [Sal06], Theorem 4.1.1 still holds even if* $p \leq 2g+1$ *except in the case when the fixed field* $\mathbb{F}^G$ *of* $\mathrm{Aut}(\mathbb{F}|k)$ *is rational, the number of ramified places in* $\mathbb{F}$ *is* ≤ 3 *and the extension* $\mathbb{F}|\mathbb{F}^G$ *is wildly ramified. However, Roquette, in [Roq], proved that the bound in 4.1.1 holds if* $p > g+1$ *with an exception in characteristic* $p = 2g+1$ *for a single function field defined by*

$$F = k(x,y), \; y^2 = x^p - x.$$

For this function field, the order of the automorphism group is exactly equal to $2p(p^2-1)$.

4.2 A Deligne-Mumford Theorem

Let us consider a normal, connected, projective curve X over k. The arithmetic genera $p_a(X)$ of the curve X coincides with the genus of the associated function field. The non-negative integer $g(X)$:=$\dim_k H^1(X, \mathcal{O}_X)$ is the geometric genus of X. The two invariants $p_a(X)$ and $g(X)$ are equal if X is geometrically connected.

Let S be a Dedekind scheme of dimension 1. Denote by η its generic point and by s a closed point in S. A fibered surface (integral, projective, flat S-scheme of dimension 2)

$$\pi : \mathcal{X} \to S$$

is called a `model` of X over S if its generic fibre $\mathcal{X}_\eta$ and the projective curve X are isomorphic. The fiber $\mathcal{X}_s$ of the model $\mathcal{X}$ is called `a reduction` of X at s. If the curve X admits a smooth model over Spec $(\mathcal{O}_{S,s})$, we say that X has a `good reduction` at s. Otherwise, we say that C has `bad reduction` at s.

Definition 4.2.1. *A proper scheme C over an algebraic closed field k of pure dimension 1 is said to be a* ***stable curve*** *if it is reduced, has only nodal singularities (Its singular points are ordinary double points) and every irreducible component of C which is isomorphic to $\mathbb{P}^1_k$ intersects the other irreducible components at at least three points.*

A model $\mathcal{X}$ is called a `stable model` of X if

$$\mathcal{X} \to S$$

is a stable curve. Note that such model, if it exists, is unique (see [Liu02] Theorem 3.34). The special fiber $\mathcal{X}_s$ for every closed point $s \in S$ is called `the stable reduction` of X at s. In particular, if C has a good reduction at s, then it has stable reduction at s.

Now, we assume that k is an algebraic closure of a discretely valued field with prolongation v to k. Denote by $\mathcal{O}_k$ the valuation ring on k with respect to v. Note also that we may assume that the residue field which corresponds to the field k is algebraically closed. Denote by S the affine scheme Spec $(\mathcal{O}_k)$ with generic point η and closed point s.

Remark 4.2.2. *A smooth projective curve over $\mathcal{O}_k$ does not always have stable reduction over $\mathcal{O}_k$. An example is given by the projective curve defined over $\mathbb{Q}$ by:*

$$x^4 + y^4 = z^4.$$

For more details, see [Liu02] Example 10.1.14 and Theorem 10.3.34(a).

However, it is well known that

Theorem 4.2.3. *If X is an irreducible smooth projective curve over k of genus $g \geq 2$, then there exists a unique stable curve $\mathcal{X}$ over $\mathcal{O}_k$ such that the generic fibre $\mathcal{X}_\eta$ and X are isomorphic.*

For a reference, see [GMP92].

As far as we know, the following important theorem first appeared in [DM69] by Deligne and Mumford. Besides, our aim in this chapter is to generalize this theorem.

Theorem 4.2.4. *Consider a stable model*

$$\mathcal{X} \to \operatorname{Spec}(\mathcal{O}_k)$$

of genus ≥ 2. *Denote respectively by* η *and* s *the generic and closed points of* $\operatorname{Spec}(\mathcal{O}_k)$ *and assume that the generic fibre* $\mathcal{X}_\eta$ *is smooth. Then, any automorphism* σ *in* $\operatorname{Aut}_k(\mathcal{X}_\eta)$ *extends naturally to an automorphism in* $\operatorname{Aut}_k(\mathcal{X})$. *Furthermore, the canonical homomorphism*

$$\operatorname{Aut}_k(\mathcal{X}_\eta) \to \operatorname{Aut}_k(\mathcal{X}_s)$$

is injective.

Proof. See [DM69] Lemma **I.12** and [Liu02] Proposition 10.3.38. □

It is well known that the following two categories are equivalent (see [Har10] Corollary 6.12.):

(i) Smooth projective curves over k, and dominant morphisms;

(ii) Function fields of one variable over k, and k-homomorphisms.

Therefore, Theorem 4.2.4, together with Theorem 4.2.3, implies the following result:

Corollary 4.2.5. *Let* $(\mathbb{F}|k, v)$ *be a valued function field where the valuation* v *is a constant prolongation (prolongation which is a constant reduction) on* $\mathbb{F}$ *of the valuation on* k *which corresponds to the discrete valuation ring* $\mathcal{O}_k$ *above. We assume that* v *is a good reduction (Definition 2.2.6). Then, there exists a natural injective homomorphism*

$$\phi : \operatorname{Aut}(\mathbb{F}|k) \hookrightarrow \operatorname{Aut}(\mathbb{F}v|kv) \tag{4.2.1}$$

where $\mathbb{F}v|kv$ *denotes the residue function field.*

Indeed, we can consider the smooth projective curve X over k associated to the function field $\mathbb{F}|k$ via the equivalent categories described above. Using Theorem 4.2.3, there exists a stable curve $\mathcal{X}$ over $\operatorname{Spec}(\mathcal{O}_k)$ which is a model of X. The result follows immediately using Theorem 4.2.4 and the fact that $\operatorname{Aut}_k(\mathcal{X}_\eta) = \operatorname{Aut}_k(X) = \operatorname{Aut}(\mathbb{F}|k)$ and $\operatorname{Aut}_k(\mathcal{X}_s) = \operatorname{Aut}(\mathbb{F}v|kv)$ where η and s are respectively the generic point and the closed point of the affine scheme $\operatorname{Spec}(\mathcal{O}_k)$.

One natural question to ask is whether Corollary 4.2.5 is still true for good non-discrete valuations. Following a suggestion and earlier work done by Roquette, Knaf has considered this question and got a positive answer in [Kna90]. In this thesis, we generalise the result to the case where the valuation v is not assumed to be good reduction nor discrete.

4.3 A Generalisation of the Deligne-Mumford Theorem

In this section, we study a natural homomorphism between the group of automorphisms of a valued function field and its reduction.

Let $\mathbb{F}|k$ be a function field over the field of constants k. Let us assume that the field k is equipped with a valuation v_k. Here, the valuation v_k is not necessarily discrete. Let v be a constant prolongation of v_k to $\mathbb{F}$. Denote by p the characteristic of the residue field kv.

Denote respectively by G and $\mathbb{E}$ the automorphism group $\mathrm{Aut}(\mathbb{F}|k)$ and the fixed field of G in $\mathbb{F}$. Since the group G is finite as the genus $g \geq 2$, the set V of prolongations of $v_{\mathbb{E}}:=v|_{\mathbb{E}}$ to $\mathbb{F}$ is finite of cardinal $t \geq 1$.

Note that we have,

$$\mathcal{O}'_{v_{\mathbb{E}}} = \bigcap_{\mathcal{O}\in\mathcal{A}} \mathcal{O} \quad \text{(Theorem 2.1.5)}$$

where $\mathcal{A}$ denotes the set of the valuation rings of $\mathbb{F}$ which lie over the valuation ring $\mathcal{O}_v \cap \mathbb{E}$ of $\mathbb{E}$.

Let $\mathcal{O} \in \mathcal{A}$ and

$$Z(\mathcal{O}) := \{\sigma \in G | \sigma(\mathcal{O}) = \mathcal{O}\}$$

be *the decomposition group* of $\mathcal{O}$ over $\mathbb{E}$. The map

$$G \ni \sigma \mapsto \sigma\mathcal{O} \in \mathcal{A}$$

induces a bijection from $G/Z(\mathcal{O})$ into $\mathcal{A}$. By definition, for any $\sigma \in G$, we have $\sigma Z(\mathcal{O})\sigma^{-1} \subseteq Z(\sigma\mathcal{O})$ and $\sigma^{-1}Z(\sigma\mathcal{O})\sigma \subseteq Z(\mathcal{O})$. So for any $\sigma \in G$,

$$Z(\sigma\mathcal{O}) = \sigma Z(\mathcal{O})\sigma^{-1}. \tag{4.3.1}$$

The next proposition was inspired from [End72].

Proposition 4.3.1. *Let π be a place corresponding to $\mathcal{O}$. There is a natural homomorphism*

$$\phi_\pi : Z(\mathcal{O}) \to \mathrm{Aut}(\mathbb{F}v|\mathbb{E}v_{\mathbb{E}}) \hookrightarrow \mathrm{Aut}(\mathbb{F}v|kv) \tag{4.3.2}$$

defined for any $\sigma \in Z(\mathcal{O})$ by

$$\pi \circ \sigma = \phi_\pi(\sigma) \circ \pi.$$

Moreover, if we denote by $T(\mathcal{O})$ its kernel called the inertia group of $\mathcal{O}$ over $\mathbb{E}$, then we have:

i. $T(\mathcal{O}) = \{\sigma \in G \mid \sigma(x) - x \in \mathcal{M}_{\mathcal{O}}, for\ all\ x \in \mathcal{O}\}$;

ii. $T(\sigma(\mathcal{O})) = \sigma G^T(\mathcal{O})\sigma^{-1}$ *for all* σ *in* G.

iii. $T(\mathcal{O})$ *is a* p*-group and the extension* $\mathbb{F}v|\mathbb{F}^{T(\mathcal{O})}v$ *is purely inseparable where* $\mathbb{F}^{T(\mathcal{O})}$ *is the fixed field of* $T(\mathcal{O})$ *in* $\mathbb{F}$.

Proof. i. Let $\sigma \in Z(\mathcal{O})$ such that $\phi_{\mathcal{O}}(\sigma) = \mathrm{Id}_{\mathbb{F}v}$. Then $[\phi_\pi(\sigma)](\pi(x)) = \pi(\sigma(x)) = \pi(x)$ for any $x \in \mathcal{O}$, therefore, $\sigma(x) - x \in \mathcal{M}_{\mathcal{O}}$. Now, if for all x in $\mathcal{O}$, we have $\sigma(x) - x \in \mathcal{M}_{\mathcal{O}}$ $(\sigma \in G)$ which implies

$$[\pi(\sigma(x) - x) = 0 \Leftrightarrow (\phi_\pi(\sigma))(\pi(x)) = \pi(x)]\,,$$

then $\phi_\pi(\sigma) = \mathrm{Id}_{\mathbb{F}v}, \sigma(\mathcal{O}) \subseteq \mathcal{O}$ and $\sigma \in Z(\mathcal{O})$ since $\sigma(\mathcal{O}) \in \mathcal{A}$. This proof is the same as the one in [End72] 19.1 c).

ii. By definition of π, the corresponding place for $\sigma\mathcal{O}$ is just $\pi \circ \sigma^{-1}$. So for any $\tau \in T(\mathcal{O})$ and $x \in \sigma\mathcal{O}$, we have:

$$\pi \circ \sigma^{-1}\left(\sigma\tau\sigma^{-1}(x) - x\right) = \pi\left(\tau\sigma^{-1}(x) - \sigma^{-1}(x)\right).$$

Since $x \in \sigma\mathcal{O}$, then $\sigma^{-1}(x)$ is in $\mathcal{O}$. Using i. and the fact that τ is an element of $T(\mathcal{O})$, we conclude that $(\tau\sigma^{-1}(x) - \sigma^{-1}(x))$ is in $\mathcal{M}_{\mathcal{O}}$. Therefore, $\sigma\tau\sigma^{-1}(x) - x \in \sigma\mathcal{M}_{\mathcal{O}}$. Hence, $\sigma T(\mathcal{O})\sigma^{-1} \subseteq T(\sigma(\mathcal{O}))$ for any σ in G. Conversely, we have $\sigma^{-1}T(\sigma(\mathcal{O}))\sigma \subseteq T(\mathcal{O})$.

iii- The field k is algebraically closed, so v is unramified and the ramification group $V(\mathcal{O})$ coincides with the inertia group. Furthermore, $V(\mathcal{O})$ is the p-Sylow subgroup of $T(\mathcal{O})$ ([End72] Theorem 20.18). Thus, $T(\mathcal{O})$ is a p-group and $\mathbb{F}v|\mathbb{F}^{T(\mathcal{O})}v$ is purely inseparable.

□

Let us now define an $\mathcal{O}_k$-curve associate to the set of valuations V as described in [GMP92]. For that, let us make some convention of notations:

Notations:

- $\mathcal{R}_f := (\mathcal{O}_k\,[f])' = R_f \cap \mathcal{O}_w$;
- $R_f := (k\,[f])' = \mathcal{R}_f \otimes_{\mathcal{O}_k} k$;
- Since f^{-1} is also V-regular, we define in the same way the rings $\mathcal{R}_{f^{-1}}$ and $R_{f^{-1}}$;
- $R_{fw} := (kw\,[fw])'$.

The $\mathcal{O}_k$-curve, say $\mathcal{C}_f$, is defined to be the $\mathcal{O}_k$-scheme

$$\mathcal{C}_f := \mathrm{Spec}\mathcal{R}_f \cup \mathrm{Spec}\mathcal{R}_{f^{-1}}$$

obtained by glueing the affine $\mathcal{O}_k$-schemes $\mathrm{Spec}\mathcal{R}_f$ and $\mathrm{Spec}\mathcal{R}_{f^{-1}}$ along $\mathrm{Spec}(\mathcal{O}_k\,[f, f^{-1}])'$.

Theorem 4.3.2. *The $\mathcal{O}_k$-curve $\mathcal{C}_f$ has the following properties:*

1. *The $\mathcal{O}_k$-curve depends only on V in the following sense:*

   If g is an another V-regular element for $\mathbb{F}|k$, the corresponding $\mathcal{O}_k$-curve, $\mathcal{C}_g$, is $\mathcal{O}_k$-isomorphic to $\mathcal{C}_f$. We denote the curve by $\mathcal{C}_V$.

2. *The $\mathcal{O}_k$-curve $\mathcal{C}_V$ is a projective integral normal flat $\mathcal{O}_k$-scheme of pure relative dimension* 1. *More precisely:*

   $$\mathcal{C}_V \cong \mathrm{Proj}S$$

   where

   $$S = \bigoplus_{n\geq 0} \mathcal{L}(nD) \cap \mathcal{O}_w$$

   and D is a pole divisor of a V-regular element for $\mathbb{F}|k$.

3. *The generic fibre of $\mathcal{C}_V$ is k-isomorphic to the non-singular irreducible projective curve C associated to the function field $\mathbb{F}$.*

Proof. [GMP92] Theorem 1.1. □

Our first result in this chapter is the following lemma:

Lemma 4.3.3. *Let $(\mathbb{F}|k, v)$ be a valued function field in one variable. Let G=*Aut$(\mathbb{F}|k)$*. If H is a subgroup of G such that the extension $\mathbb{F}v|\mathbb{F}^Hv$ is purely inseparable, then H is trivial.*

Proof. Let σ be an element of H of order > 1. Denote by $\langle\sigma\rangle$ the subgroup of H generated by σ. Choose a regular transcendental element f for the valuation v. Let $\mathcal{C}_v$ be the $\mathcal{O}_k$-curve associated to $\{v\}$. So the generic fibre of $\mathcal{C}_v$ is isomorphic to the curve

$$C := \mathrm{Spec}R_f \cup \mathrm{Spec}R_{f^{-1}}$$

which is the unique smooth projective curve with $\mathbb{F}$ as function field (Theorem 4.3.2). On the other hand, the closed fibre of $\mathcal{C}_v$ is isomorphic to the curve

$$Cv := \mathrm{Spec}\mathcal{R}_f v \cup \mathrm{Spec}\mathcal{R}_{f^{-1}} v = \mathcal{C} \times (kv)$$

which has $\mathbb{F}v$ as function field (but may have singularities in case v is not a good reduction). Let us consider the smooth projective curve

$$\overline{C} := \mathrm{Spec}R_{fv} \cup \mathrm{Spec}R_{f^{-1}v}$$

which is the normalisation of Cv.

Then we have:

$$g_{Cv} = g_{\overline{C}} + \delta, \tag{4.3.3}$$

where δ is the *singularity number* (see [Liu02] Propostion 7.5.4). And we have:

$$\delta = \dim_{kv}\left(R_{fv}/\mathcal{R}_f v\right) + \dim_{kv}\left(R_{f^{-1}v}/\mathcal{R}_{f^{-1}}v\right).$$

Since the Euler-Poincaré characteristic does not change under reduction and k is algebraically closed, we conclude that the curves C and Cv have the same arithmetic genus, i.e,

$$g_{Cv} = g_{\overline{C}} + \delta = g_C. \tag{4.3.4}$$

Furthermore, the extension $\mathbb{F}v|\mathbb{F}^{\langle\sigma\rangle}v$ is purely inseparable which implies

$$g_{\overline{C^r}} = g_{\overline{C}} \text{ ([Sti09] 3.10)}$$

where C^r denotes the restriction of C on $\mathbb{F}^{\langle\sigma\rangle}$. The curve $\overline{C^r}$ is the normalization of the reduction of the curve C^r.

On the other hand, we have

$$g_{C^r} = g_{\overline{C^r}} + \delta^r, \tag{4.3.5}$$

where

$$\delta^r = \dim_{kv}\left(R_{fv}/\mathcal{R}^r_f v\right) + \dim_{kv}\left(R_{f^{-1}v}/\mathcal{R}^r_{f^{-1}}v\right)$$

and $\mathcal{R}^r_f v = R_{fv} \cap \mathbb{E}v$. The ring $\mathcal{R}^r_{f^{-1}}v$ is also defined in the same way as $\mathcal{R}^r_f v$. Since,

$$\mathcal{R}^r_f v \subseteq \mathcal{R}_f v \subseteq R_{fv},$$

we conclude that $\delta^r \geq \delta$. Therefore,

$$g_{\mathbb{F}^{\langle\sigma\rangle}} = g_{C^r} = g_{\overline{C^r}} + \delta^r \geq g_{\overline{C}} + \delta = g_{\overline{C^r}} + \delta = g_C = g_{\mathbb{F}}.$$

This can only happen if $g_{\mathbb{F}^{\langle\sigma\rangle}} = g_{\mathbb{F}} = 0$ or 1 by the Hurwitz genus formula. Thus, $g_{\mathbb{F}^{\langle\sigma\rangle}} = g_{\mathbb{F}}$ and $\mathbb{F}^{\langle\sigma\rangle} = \mathbb{F}$. This contradicts the fact that the extension $\mathbb{F}|\mathbb{F}^{\langle\sigma\rangle}$ is Galois, hence, separable. Thus, H is the trivial subgroup. □

Observe that:

Remark 4.3.4. *In the proof of Lemma 4.3.3, we use the same technique as in the proof of Theorem 4.2.4 in [Liu02] (Proposition 10.3.38.). But here, we are not restricted to the case of stable reduction. We made the proof more general using directly the $\mathcal{O}_k$-curve associated to the valuation v.*

Now, we are able to state our main result of this chapter:

Theorem 4.3.5. *The homomorphism ϕ_π defined above is injective. More precisely, we have*

$$Z(\mathcal{O}) \simeq \mathrm{Aut}(\mathbb{F}v|\mathbb{E}v_{\mathbb{E}})$$

where $\mathbb{E}$ is the fixed field of G.

Proof. According to a theorem in [End72] (Theorem 19.6), the homomorphism

$$\phi_\pi : Z(\mathcal{O}) \to \mathrm{Aut}(\mathbb{F}v|\mathbb{E}v)$$

is surjective. However, by Theorem 4.3.1 iii., the extension $\mathbb{F}v|\mathbb{F}^{T(\mathcal{O})}v$ is purely inseparable where $T(\mathcal{O})$ is the kernel of ϕ_π. Using Lemma 4.3.3, we conclude that $T(\mathcal{O})$ is a trivial group. □

Remark 4.3.6. *In the previous theorem, let us assume that the valuation v is a good reduction. Using Corollary 2.2.4, the valuation v is the only prolongation of the valuation $v_{\mathbb{E}}$ on $\mathbb{E}$. Hence, we have:*

$$Z(\mathcal{O}) = \mathrm{Aut}(\mathbb{F}|k).$$

By Theorem 4.3.5, we conclude that

$$\mathrm{Aut}(\mathbb{F}|k) \subseteq \mathrm{Aut}(\mathbb{F}v|kv)$$

via the homomorphism ϕ_π. Hence, Theorem 4.3.5 is a generalisation of the Knaf's theorem in [Kna90] which generalizes Theorem 4.2.4 of Deligne and Mumford in the case when the reduction is good.

Moreover, we can generalize Theorem 4.3.5 as follows:

Consider the infnorm w with respect to the set of valuations V. We have

$$\mathbb{F}w := \mathcal{O}'_{v_{\mathbb{E}}} / \left(\mathcal{M}_{\mathcal{O}_{v_{\mathbb{E}}}} \cdot \mathcal{O}'_v\right) = \prod_{\mathcal{O}\in\mathcal{A}} \mathcal{O}/\mathcal{M}_{\mathcal{O}} \simeq (\mathbb{F}v)^s.$$

Since the ring $\mathcal{O}'_{v_{\mathbb{E}}}$ is invariant under the action of G, there exists an homomorphism

$$\phi : G \ni \sigma \mapsto \phi(\sigma) \in \mathrm{Aut}(\mathbb{F}w|\mathbb{E}v_{\mathbb{E}}) \subseteq \mathrm{Aut}(\mathbb{F}w|kv)$$

such that for any $\sigma \in G$,

$$\psi \circ \sigma = \phi(\sigma) \circ \psi$$

where ψ is the canonical homomorphism

$$\psi : \mathcal{O}'_{v_{\mathbb{E}}} \to \mathbb{F}w$$

induced by the place π corresponding to the valuation $\mathcal{O}$ above. Note that ψ does not depend on which place we consider. Indeed, $\mathcal{O}'_{v_{\mathbb{E}}}$ is invariant under G and any prolongation of $\mathcal{O}_{v_{\mathbb{E}}}$ in $\mathbb{F}$ is given by $\sigma(\mathcal{O})$ for some $\sigma \in G$. The kernel of the homomorphism ϕ is

$$\mathrm{Ker}\phi = \left\{ \sigma \in G \mid \sigma(x) - x \in \bigcap_{\mathcal{O} \in \mathcal{A}} \mathcal{M}_{\mathcal{O}}, \text{ for all } x \in \mathcal{O}'_{v_{\mathbb{E}}} \right\}.$$

We have:

Proposition 4.3.7. *Consider the normal subgroup*

$$N := \bigcap_{\mathcal{O} \in \mathcal{A}} Z(\mathcal{O})$$

of G. Then, the restriction of the homomorphism ϕ on N is injective. In particular, if G is abelian, for a given valuation ring $\mathcal{O}$ in $\mathcal{A}$, we have

$$Z(O) \subseteq \mathrm{Aut}(\mathbb{F}w|\mathbb{E}v_{\mathbb{E}})$$

via the homomorphism ϕ.

Proof. Let us denote by T the kernel of the restriction of ϕ to the normal subgroup N.

For any σ in G, consider the following homomorphism which is defined by

$$\begin{aligned} h_\sigma \ : \ \mathbb{F}^\times/\mathbb{E}^\times &\to \mathbb{F}^\times \\ x \cdot \mathbb{E}^\times &\mapsto \frac{\sigma(x)}{x}. \end{aligned}$$

Denote respectively by Δ and Γ the value group of w and $v_{\mathbb{E}}$. The mapping

$$\begin{aligned} \mathbb{F} &\to \Delta \\ x &\mapsto w(x) \end{aligned}$$

induces a sujective map $w^\times$ from $\mathbb{F}^\times/\mathbb{E}^\times$ to Δ/Γ. Note that for any $\sigma \in N$ and $x \in \mathbb{F}^\times$ we have

$$h_\sigma(x \cdot \mathbb{E}^\times) \in U_{\mathcal{O}'_{v_{\mathbb{E}}}}. \tag{4.3.6}$$

Indeed, fix a valuation ring $\mathcal{O}$ in $\mathcal{A}$. Denote by v the corresponding valuation. For any $x \in \mathbb{F}^\times$, we have

$$v\left(\frac{\sigma(x)}{x}\right) = v \circ \sigma(x) - v(x).$$

But, since σ is in N, in particular, σ belongs to $Z(\mathcal{O})$. Hence, $v \circ \sigma = v$. Thus, $v\left(\frac{\sigma(x)}{x}\right) \in U_{\mathcal{O}}$. The valuation ring $\mathcal{O}$ being arbitrary, the statement 4.3.6 holds. Furthermore, for any $\sigma \in T$ and $u \in U_{\mathcal{O}'_{v_{\mathbb{E}}}}$, we have:

$$h_\sigma(u \cdot \mathbb{E}^\times) \in 1 + \bigcap_{\mathcal{O} \in \mathcal{A}} \mathcal{M}_{\mathcal{O}}.$$

The set $U_{\mathcal{O}'_{v_{\mathbb{E}}}}$ denotes the group of all unit of the ring $\mathcal{O}'_{v_{\mathbb{E}}}$. Since the vanishing set of the map $w^{\times}$ is the set

$$V_w = \left\{ u \cdot \mathbb{E}^{\times} \mid u \in U_{\mathcal{O}'_{v_{\mathbb{E}}}} \right\}$$

and the kernel of the homomorphism $\psi \circ h_\sigma$ contains V_w, we conclude, with the surjectivity of $w^{\times}$, that for any $\sigma \in T$, there exists a unique map $\overline{h}_\sigma \in \mathrm{Hom}(\Delta/\Gamma, \mathbb{F}w)$ such that

$$\overline{h}_\sigma \circ w^{\times} = \psi \circ h_\sigma.$$

However, the base field k is assumed to be algebraically closed. This implies that any prolongation of the valuation $v_{\mathbb{E}}$ on $\mathbb{F}$ is unramified. Hence, $\Delta = \Gamma$. Let $\sigma \in T$. Then, we have $\overline{h}_\sigma = \mathrm{Id}_{\Delta/\Gamma}$. That is, for any $x \in \mathbb{F}^{\times}$, we have

$$\psi\left(\frac{\sigma(x)}{x}\right) = (\psi \circ h_\sigma)(x \cdot \mathbb{E}^{\times}) = \mathrm{Id}_{\Delta/\Gamma}(w(x) + \Gamma) = 1.$$

Therefore, for any $x \in \mathbb{F}^{\times}$, we conclude that

$$\frac{\sigma(x)}{x} - 1 \in \bigcap_{\mathcal{O} \in \mathcal{A}} \mathcal{M}_{\mathcal{O}}.$$

In particular, for all $x \in \mathcal{O}$ where $\mathcal{O}$ is any valuation ring in $\mathcal{A}$, we have

$$\sigma(x) - x \in \mathcal{M}_{\mathcal{O}}.$$

Thus, $\sigma \in T(\mathcal{O})$, the kernel of the homomorphism ϕ_π defined above where π is the place which corresponds to the valuation ring $\mathcal{O}$. According to Theorem 4.3.5, $T(\mathcal{O})$ is the trivial group. Hence, $\sigma = \mathrm{Id}_{\mathbb{F}}$. In fact, we have

$$T = \bigcap_{\mathcal{O} \in \mathcal{A}} T(\mathcal{O}).$$

□

Remark 4.3.8. *The proof of the previous proposition is, somehow, a generalisation of a theory developed in [End72] to compute the ramification group $V(\mathcal{O})$ of a valuation ring $\mathcal{O}$ in $\mathcal{A}$ over $\mathbb{E}$. Besides, recall that our proof of Theorem 4.3.5 use the fact that the kernel $T(\mathcal{O})$ coincides with the ramification group $V(\mathcal{O})$ since Δ/Γ is trivial. Note that the group $V(\mathcal{O})$ is a p-subgroup of G (see [End72] Table p. 171).*

Observing Proposition 4.3.7 and its proof, our first guess is the following:

Conjecture 4.3.9. *The kernel of the homomophism ϕ is a p-subgroup of G where p is the characteristic of the residue field kv.*

Chapter 5

Lifting Problems on Automorphism Groups of Cyclic Curves

Let k be an algebraically closed field of prime characteristic p. Given a smooth projective curve X over k, consider a good lifting $(X_0/k_0, v)$ of X/k to characteristic 0, with k_0 is the algebraically closed field of the fraction field of $W(k)$, the ring of Witt vectors over k and v is a valuation such that $k_0v = k$. According to Theorem 4.3.5, together with the two equivalent categories described in Chapter 4, there is a natural injective homomorphism

$$\phi : \ G_0{:=}\mathrm{Aut}_{k_0}(X_0) \hookrightarrow G{:=}\mathrm{Aut}_k(X).$$

Moreover, if ϕ is surjective, we say that the automorphism group G `is liftable` to characteristic 0. So, one can ask: Under which conditions is ϕ surjective? The aim of this chapter is to answer this question.

We have a partial answer when the order of the group G and p, the characteristic of k, are relatively prime. Indeed, in [Gro71] Exposé XIII §2, Grothendieck proved that if p does not divide the order of G, then G could always be lifted to characteristic 0. However, in the case when G is divisible by p, the problem is not completely solved.

It is important to point out that this problem is related to `Oort groups` and `Lifting problems` (Definition 5.1.1) that we can see in [CGH08]. By definition, an Oort group for k is clearly liftable to characterisitic 0. But, the converse is not always true. So, a priori, for an automorphism group of a smooth projective curve over k, the condition of being an Oort group is stronger than being liftable to characteristic 0.

In this chapter, we restrict to the case of cyclic curves (Definition 5.1.3) over prime characteristic field. The main reason is the fact that we know all of the groups which can occur as an automorphism group of a cyclic curve in any characteristic which is not equal to 2 (See [Sha03] and [San09]). Therefore, a priori, a quite elementary covering theory, some group theory and representation of finite subgroups of $\mathrm{PGL}_2(k)$ would suffice. We will show that, in fact, the full automorphism groups of certain type of cyclic curves (such as hyperelliptic curves) over k are liftable to characteristic 0 if and only if they are Oort groups for k. We will eventually give a list of all possible liftable groups that can occur as automorphism groups of cyclic curves over k.

To begin with, let us first recall some results on Oort groups for k. And also, some preliminary results that we will need to prove our results in the second section.

Throughout this chapter, k denotes an algebraically closed field of prime characteristic p.

5.1 Results on Oort Groups

Definition 5.1.1. *A finite group G is called an* `Oort group` *for k if every faithful action of G on a smooth connected projective curve over k lifts to characteristic* 0.

Oort conjectured that we can lift any cyclic group. It turns out that this conjecture is true according to the works of Pop (See [Pop14]), mainly using deformation theory and a special case of a result by Obus and Wewers that we can see in [OW14]. Moreover, Chinburg, Guralnick and Harbater, in [CGH08], proved that if G is liftable to characteristic zero, then any cyclic-by-p subgroup (extensions of a prime-to-p cyclic group by a p-group) of G must be either cyclic or dihedral of the form D_{p^n}, with the exception of $\mathcal{A}_4$ in characteristic 2. They also predict that the converse is true. But as far as we know, no one has given a proof that the dihedral group D_{p^n} for $n > 1$ can be lifted to characteristic zero. This conjecture is called the *Strong Oort conjecture.*

The following lemma is a summary of what we will need about Oort groups:

Lemma 5.1.2 ([CGH08])**.**

- *A p-regular group (its order is not divisible by p), a finite cyclic group, the dihedral group D_p and the Klein four-group V_4 (in the case $p = 2$) are Oort groups for k;*
- *The quaternion group Q_8 (in the case $p = 2$), the group $(\mathbb{Z}/p\mathbb{Z})^n$ where $n \geq 2$ (resp. > 2) if $p \neq 2$ (resp. $p = 2$) are not Oort groups;*
- *Let G be a finite group. Then G is an Oort group if and only if every cyclic-by-p subgroup $H \subset G$ is an Oort group;*
- *If a cyclic-by-p group is an Oort group for k, then it must be cyclic or dihedral of the form D_{p^n} for some integer n.*

Definition 5.1.3. *We say that a function field $\mathbb{F}|k$ is* `cyclic` *(or* `superelliptic`*) if the following condition is satisfied: There exists a transcendental element x such that the rational function field $k(x)$ is invariant under the action of the full automorphism group G of $\mathbb{F}|k$ and the subgroup N=Aut $(\mathbb{F}|k(x))$ is cyclic, Galois and a normal subgroup of G.*

Here, the base field k is an algebraically closed field of characteristic $p \geq 0$. The smooth projective curve X over k associated to $\mathbb{F}|k$ is called `cyclic curve`*.*

Proposition 5.1.4. *Let $(\mathbb{F}|\mathbb{K}, v)$ be a valued function field where the valuation v is assumed to be a good reduction. Denote by $\mathbb{E}$ the fixed field of the full automorphism group G of $\mathbb{F}|\mathbb{K}$. Then, for any subfield $\mathbb{L}v$ between $\mathbb{F}v$ and $\mathbb{E}v$, there exists a unique subfield $\mathbb{L}$ between $\mathbb{F}$ and $\mathbb{E}$ such that $\mathbb{L}v$ is the exact reduction of $\mathbb{L}$ by the valuation v.*

Note that, the subfield $\mathbb{L}$ and $\mathbb{L}v$ have the same genus (Theorem 3.2.7).

Proof. We know that $G \simeq \mathrm{Aut}(\mathbb{F}v|\mathbb{E}v)$ and $\mathbb{F}v|\mathbb{E}v$ is Galois. The result follows by the Galois correspondence. Indeed, the extension $\mathbb{F}v|\mathbb{L}v$ is also Galois and denote by Hv its Galois group. By the Galois correspondence theorem, if n is the number of subgroups, H_i $(1 \leq i \leq n)$, of G which have the same order as Hv, then there exists exactly n extensions, $\mathbb{F}v|\mathbb{L}_i v$ $(1 \leq i \leq n)$, such that $H_i v$=Aut $(\mathbb{F}v|\mathbb{L}_i v)$ for each $1 \leq i \leq n$. The group $H_i v$ denotes the reduction of H_i by the natural isomorphism between G and $\mathrm{Aut}(\mathbb{F}v|\mathbb{E}v)$ for each $1 \leq i \leq n$. Therefore, there must be a unique subgroup H (one of the subgroups H_i) of G such that $H \simeq Hv$ (via the natural isomorphism between G and $\mathrm{Aut}(\mathbb{F}v|\mathbb{E}v)$) and $\mathbb{F}^H v = \mathbb{L}v$. Thus, $\mathbb{L} = \mathbb{F}^H$. □

Now, let $\mathbb{F}|k$ be a cyclic function field. Denote by X the smooth cyclic curve over k associated to $\mathbb{F}|k$. Now, let X_0 be a good lifting of X to characteristic 0 over an algebraically closed field k_0. Then, there exists a valued function field $(\mathbb{F}_0|k_0, v)$ such that v is a good reduction, $\mathbb{F} = \mathbb{F}_0 v$ and $k = k_0 v$. Suppose that the full automorphism group G of the curve X/k is liftable to characteristic zero and assume that $G \simeq G_0$=$\mathrm{Aut}(\mathbb{F}_0|k_0)$. Using Proposition 5.1.4, there exists a residually transcendental element x such that the extensions $\mathbb{F}_0|k_0(x)$ and $\mathbb{F}|k(\overline{x})$ are Galois. Hence, $\mathbb{F}_0|k_0$ is also a cyclic function field and N=Aut $(\mathbb{F}_0|k_0(x)) \simeq \mathrm{Aut}(\mathbb{F}|k\,(\overline{x}))$. Note also that the curve X_0/k_0 is cyclic. Furthermore, the groups G/N and G_0/N are isomorphic and respectively embedded in $\mathrm{PGL}_2(k)$ and $\mathrm{PGL}_2(k_0)$. Therefore, it is important to know which kind of groups could be finite subgroups of both $\mathrm{PGL}_2(k)$ and $\mathrm{PGL}_2(k_0)$.

Lemma 5.1.5. *Let H be a finite subgroup of $\mathrm{PGL}_2(k)$. The group H can be embedded in $\mathrm{PGL}_2(k_0)$ if and only if one of the following statements holds:*

- *The prime characteristic p does not divide $|H|$, the order of H;*
- *If p divides $|H|$, then up to isomorphism, H is one of the following groups:*
  - $H = \mathbb{Z}/p\mathbb{Z}$;
  - $H = D_p$ *if* $p \neq 2$;
  - $H = \mathcal{A}_4$ *or a dihedral group D_n where n is a positive odd integer if* $p = 2$;
  - $H = \mathcal{A}_5$ *in the case when* $p \leq 5$;
  - $H = \mathcal{A}_4$ *or* $\mathcal{S}_4$ *when* $p = 3$.

Proof. In order to prove the lemma, we shall recall the following theorem from [Fab12] Theorem B and Theorem C:

Proposition 5.1.6. *Let $\mathbb{K}$ be an algebraically closed field of characteristic q. Let H be a finite subgroup of $\mathrm{PGL}_2(\mathbb{K})$. Then:*

- *If $q = 0$ or $q > 0$ and $q \nmid |H|$, the group H is isomorphic to a cyclic group, a dihedral group, $\mathcal{A}_4, S_4$ or $\mathcal{A}_5$;*
- *If $q > 0$ and q divides the order of H, then H is isomorphic to one of the following groups: $\mathrm{PGL}_2(\mathbb{F}_{q^n})$,$\mathrm{PSL}_2(\mathbb{F}_{q^n})$ for some integer n or to a q-semi-elementary subgroup. Note that the conjugacy classes of q-semi-elementary subgroups of $\mathrm{PGL}_2(\mathbb{K})$ of order $p^m n (n \in \mathbb{N} \backslash q\mathbb{N}$ and $m \in \mathbb{N}^\star)$ are parameterized by the set of homothety classes of rank-m subgroups Γ satisfying $\mathbb{F}_{q^e} \subset \Gamma \subset \mathbb{K}$ via the map*

$$\Gamma \mapsto \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_n(\mathbb{K}) & \\ & 1 \end{pmatrix}$$

where e is the order of q in $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\mu_n(\mathbb{K})$ is the group of primitive n-th roots of unity in $\mathbb{K}$.

With the following exceptional possibilities:

- *Suppose that $q = 3$, then H could also be isomorphic to $\mathcal{A}_5$;*
- *If $q = 2$, H is isomorphic to a dihedral group D_n where n is an odd positive integer.*

Let us now prove our lemma. If $p \nmid |H|$, then by the first statement of Proposition 5.1.6 , the subgroup H can be embedded in $\mathrm{PGL}_2(k_0)$. Therefore for the rest of the proof of Lemma 5.1.5, we may assume that p divides the order of H.

Let us assume first that $p>5$. Using Proposition 5.1.6, since p divides $|H|$, the group H is not isomorphic to one of the groups $\mathcal{A}_4, S_4$ or $\mathcal{A}_5$. Therefore, H is either cyclic or dihedral. However, the groups $\mathrm{PGL}_2(\mathbb{F}_{p^n})$ and $\mathrm{PSL}_2(\mathbb{F}_{p^n})$ for some integer n are not cyclic nor dihedral. Hence, H is isomorphic to a p-elementary group of order $p^m n(n \in \mathbb{N} \setminus q\mathbb{N}$ and $m \in \mathbb{N}^{\star})$ parameterized by a set of homothety classes of a rank-m subgroup Γ satisfying $\mathbb{F}_{p^e} \subset \Gamma \subset k$ via the map

$$\Gamma \mapsto \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_n(k) & \\ & 1 \end{pmatrix}$$

where e is the order of p in $(\mathbb{Z}/n\mathbb{Z})^{\times}$ and $\mu_n(k)$ is the group of primitive n-th root of unity in k. Furthermore, by the definition of p-elementary groups, H is cyclic if $m = 1$ or dihedral if $m = 1$ and $n = 2$. Thus, $H \simeq \mathbb{Z}/pn\mathbb{Z}$ or D_p where n is a non-negative integer prime to p. However if we assume that $n > 1$. This would suggest that there is a cyclic group of order pn generated by the two matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}$$

where ζ is a primitive n-root of unity. But, those two matrices do not commute with each other. Hence, n must be equal to 1.

In the case when $p \leq 5$, if H is a p-elementary group, then $H \simeq \mathbb{Z}/p\mathbb{Z}$ or D_p with the exceptional case $\mathcal{A}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$ in characteristic $p = 2$.

If $p = 5$, since $\mathcal{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$, then H could be isomorphic to $\mathcal{A}_5$.

Now if $p = 3$, since $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathcal{S}_4$ and $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathcal{A}_4, H$ could be isomorphic to $\mathcal{A}_4, \mathcal{S}_4$ and $\mathcal{A}_5$ according to the third statement of Proposition 5.1.6.

Finally, if $p = 2$, according to the last statement of Proposition 5.1.6, H could be a dihedral group and $H \simeq D_n$ where n is an odd integer. We know also that $\mathrm{PGL}(2,4)$ is isomorphic to $\mathcal{A}_5$, thus, the group $H = \mathrm{PGL}(2,4)$ can be embedded in $\mathrm{PGL}_2(k_0)$.

□

5.2 Lifting Automorphism Group of Cyclic Curves

As we have already mentioned, according to Grothendieck in [Gro71], if the order of the automorphism group G of a smooth curve (of genus $g \geq 2$) is not divisible by p, then G is liftable to characteristic zero. Therefore, for the rest of this chapter, the order of the automorphism group of any curve over k, unless otherwise specified, is assumed to be divisible by p.

A direct corollary of Lemma 5.1.5 is the following:

Theorem 5.2.1. *Let $(\mathbb{F}_0|k_0, v)$ be a valued cyclic function field where the base field k_0 is of characteristic 0. Suppose that the valuation v is invariant under the action of the group $G_0 = \mathrm{Aut}(\mathbb{F}_0|k_0)^1$. Denote by N the normal subgroup of G_0 as we defined in 5.1.3.*

If G_0 is isomorphic to the full automorphism group G of the residue function field $\mathbb{F}|k$, then G/N is isomorphic to one of the groups:

- $\mathbb{Z}/p\mathbb{Z}$;
- D_p *if* $p \neq 2$;
- $\mathcal{A}_4$ *or a dihedral group* D_n *where* n *is a positive odd integer if* $p = 2$;
- $\mathcal{A}_5$ *in the case when* $p \leq 5$;
- $\mathcal{A}_4$ *or* $\mathcal{S}_4$ *when* $p = 3$.

with the following additional possibilities:

- $\mathbb{Z}/m\mathbb{Z}$ *or a dihedral* D_m *if* p *divides* $|N|$, *the order of the group* N;

The integers m is prime to p.

Proof. Suppose we have $G_0 \simeq G$. By hypothesis, there exists a transcendental element x of $\mathbb{F}_0$ such that $k(x)$ is invariant under G and $N = \mathrm{Aut}(\mathbb{F}|k)$ is Galois. Therefore, via the natural isomorphism between G_0 and G and the fact that N is a finite Galois group, the element x is residually transcendental and the groups G_0/N and G/N are respectively finite subgroups of $\mathrm{PGL}_2(k_0)$ and $\mathrm{PGL}_2(k)$. Moreover, the isomorphism between G_0 and G induces an isomorphism from G_0/N to G/N. Note that the group G/N is a finite subgroup of $\mathrm{PGL}_2(k)$. If we assume that p does not divide the order of N, then p must divide $|G/N|$, since p divides the group G by hypothesis. So, in this case, using Lemma 5.1.5, G_0/N must be isomorphic to one of the groups:

$$\mathbb{Z}/p\mathbb{Z}, D_p, \mathcal{A}_5, \mathcal{S}_4, \mathcal{A}_4,$$

with the exceptional group D_m, where m is an odd integer in characteristic 2.

Now, if p divides $|N|$, the order of the group G/N could be prime to p. Hence, if this is the case, according to Lemma 5.1.5, the group G/N could be isomorphic to one of the following groups:

$$\mathbb{Z}/n\mathbb{Z}, D_n, \mathcal{A}_5, \mathcal{S}_4, \mathcal{A}_4$$

where the integer n is prime to p. The results follow immediately using the list of possible finite subgroups of rational function fields that can be lifted to characteristic 0 in Lemma 5.1.5. □

[1] Note if $\mathbb{F}_0|k_0$ has good reduction at v then it is invariant under G_0 as good reduction is unique for $g \geq 1$.

Let us make some observations in this context:

Let X/k be a smooth cyclic curve with automorphism group G that is liftable to characteristic 0. Denote by X_0/k_0 its good lifting to characteristic 0. Suppose that the prime characteristic of k is odd. Let $\mathbb{F}|k$ and $\mathbb{F}_0|k_0$ be the function fields which correspond to X/k and X_0/k_0 respectively. Since the characteristic of k is $p \neq 2$, we may assume that the function fields $\mathbb{F}_0|k_0$ and $\mathbb{F}|k$ are defined respectively by the equations:

$$y_0^2 = P(x_0)$$

and

$$y^2 = \overline{P}(x)$$

with $P(x_0) \in \mathcal{O}_{k_0}[x_0]$ where $\mathcal{O}_{k_0}$ is the valuation ring of k_0 which corresponds to the restriction of v, the good reduction of $\mathbb{F}_0|k_0$, to k_0. The polynomial P is the reduction of the polynomial P_0 under the Gauss valuation v_{x_0}, prolongation of v to $k_0(x_0)$. The transcendental elements x and y in $\mathbb{F}$ are, respectively, the reductions of the transcendental elements x_0 and y_0 of $\mathbb{F}_0$.

Now, denote by G_0 and N the automorphism group of $\mathbb{F}_0|k_0$[2] and the normal subgroup of G_0 such that the quotient space X_0/N has genus 0. In the proof of Theorem 5.2.1, we know that there is an injective homomorphism

$$\iota : G_0/N \hookrightarrow G/N.$$

The groups G_0/N and G/N are respectively subgroups of $\text{Aut}(k_0(x_0)|k_0) \simeq \text{PGL}_2(k_0)$ and $\text{Aut}(k(x)|k) \simeq \text{PGL}_2(k)$. The restriction of the good reduction on $\mathbb{F}_0$ to $k_0(x_0)$ is the Gauss valuation v_{x_0}. So, we remark that:

Remark 5.2.2. *The injective homomorphism ι is defined as follows:*

$$\begin{aligned} \iota :& G_0/N \hookrightarrow G/N \\ &\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \end{aligned}$$

where a, b, c and d belong to k_0. For any element u in k_0, we denote its reduction under the valuation v by $\overline{u}$.

Let us illustrate this with an example:

[2] Note that the function field $F_0|k_0$ has the same automorphism group as the cyclic curve X_0/k_0.

Example 5.2.3. *Suppose that $G_0/N = \mathbb{Z}/p\mathbb{Z}$. Denote by σ the generator of the group G_0/N. The generator σ can not be equal to*

$$\gamma = \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}$$

where ζ is a p-primitive root of unity in k_0. Indeed, the image of γ via the homomorphism ι is the identity in G/N. However, the image, by ι, of the element

$$\tau = \begin{pmatrix} \zeta + \zeta^{-1} + 1 & -1 \\ 1 & 1 \end{pmatrix}$$

which is a conjugate of γ in $\mathrm{PGL}_2(k_0)$ is

$$\overline{\tau} = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}.$$

Furthermore, for every odd prime p, the 2 by 2 matrix $\overline{\tau}$ has order p in $\mathrm{PGL}_2(\mathbb{F}_p)$. Note also that $\overline{\tau}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are conjugate in $\mathrm{PGL}_2(\mathbb{F}_p)$.

With Theorem 5.2.1, we are able to solve our lifting problem for certain type of cyclic curves. Indeed, it is clear that hyperelliptic curves are cyclic curves. The next theorem gives us all of possible finite groups of hyperelliptic curves over k that can be lifted to characteristic 0.

Theorem 5.2.4. *Let X/k be a smooth projective irreducible hyperelliptic curve. Denote by G its full automorphism group and suppose that $p \neq 2$. Then, the automorphism group G is liftable to characteristic 0 if and only if, up to isomorphism, G is one of the following groups:*

1. *$G = \mathbb{Z}/2p\mathbb{Z}$;*
2. *$G = D_{2p}$;*

with the exceptional possibilities:

1. *$G = \mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_5$ or $\mathrm{SL}_2(5)$ if $p = 5$;*
2. *$G = \mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_4, \mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_4, \mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_5, \mathrm{SL}_2(3)$, or $\mathrm{GL}_2(3)$ in the case when $p = 3$.*

In particular, the group G is liftable to characteristic 0 if and only if G is an Oort-group for k. We also observe that the order of G is divisible by p, but not by p^2.

Proof. Suppose that G is liftable to characteristic 0. Denote by σ the hyperelliptic involution of order 2 of the group G. Let X_0/K_0 be a good lifting of X/k such that $G_0 = \mathrm{Aut}_{k_0}(X_0) \simeq G$. The curve X_0 is also a hyperelliptic curve (by Proposition 3.2.8). The isomorphism between G_0 and G induces an isomorphism between $G_0/\langle\sigma\rangle$ and $H = G/\langle\sigma\rangle$. That is: Up to isomorphism, the group H which is a finite subgroup of $\mathrm{PGL}_2(k)$ can be embedded in $\mathrm{PGL}_2(k_0)$. So, let us first recall the list of possible groups that can occur as full automorphism groups of the hyperelliptic curve X_0/k_0. As far as we know, the list first appeared in [BGG93]:

H	G_0
$\mathbb{Z}/n\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/2n\mathbb{Z}$
D_n	$\mathbb{Z}/2\mathbb{Z} \times D_n, V_n, D_{2n}, H_n, U_n, G_n$
$\mathcal{A}_4$	$\mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_4, \mathrm{SL}_2(3)$
$\mathcal{S}_4$	$\mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_4, \mathrm{GL}_2(3), W_2, W_3$
$\mathcal{A}_5$	$\mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_5, \mathrm{SL}_2(5)$

where the groups V_n, H_n, U_n, G_n, W_2 and W_3 are defined as follows:

$$\begin{aligned}
V_n &= \langle x, y \mid x^4, y^n, (xy)^2, (x^{-1}y)^2\rangle;\\
H_n &= \langle x, y \mid x^4, (xy)^n, x^2y^2\rangle;\\
U_n &= \langle x, y \mid x^2, y^{2n}, xyxy^{n+1}\rangle;\\
G_n &= \langle x, y \mid x^2y^n, y^{2n}, x^{-1}yxy\rangle;\\
W_2 &= \langle x, y \mid x^4, y^3, yx^2y^{-1}x^2, (xy)^4\rangle;\\
W_3 &= \langle x, y \mid x^4, y^3, x^2(xy)^4, (xy)^8\rangle.
\end{aligned}$$

Now, following Lemma 5.1.5 and Theorem 5.2.1, we distinguish 4 cases:

1^{st}*case* : If $H \simeq \mathbb{Z}/p\mathbb{Z}$;

That is $G_0/\langle\sigma\rangle \simeq \mathbb{Z}/p\mathbb{Z}$. The abelian groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/2p\mathbb{Z}$ are isomorphic since p is an odd prime. According to the list we have above, we conclude that G_0 must be isomorphic to $\simeq \mathbb{Z}/2p\mathbb{Z}$.

2^{nd}*case* : If $H \simeq D_p$;

According to the list above, if $G_0/\langle\sigma\rangle \simeq D_n$, for a given integer n, then G_0 is isomorphic to one of the groups: $\mathbb{Z}/2\mathbb{Z}\times D_n, D_{2n}, H_n, U_nV_n$, and G_n. However, in the cases when G_0 would be isomorphic to V_n, H_n, U_n, G_n, or $\mathbb{Z}/2\mathbb{Z} \oplus D_n$, the integer n must be even ([Sha06] Remark 6.). Since p is assumed to be odd, then G_0 is isomorphic to D_{2p}.

3^{rd}*case* : If $p \leq 5$ and $H \simeq \mathcal{A}_5$;

Let $(\mathbb{F}_0|k_0, v)$ be the valued function field associated to X_0/k_0 where v is the valuation such that $\mathbb{F}_0 v = \mathbb{F}$ and $k_0 = k$. Let us consider the following polynomials:

$$\begin{aligned}
R(x) &= x^{30} + 522x^{25} - 10005x^{20} - 10005x^{15} - 522x^5 + 1\\
S(x) &= x^{20} - 228x^{15} + 494x^{10} + 228x^4 + 1\\
T(x) &= x^{10} + 10x + 1\\
G_i(x) &= (\lambda_i - 1)x^{60} - 36(19\lambda_i + 29)x^{55} + 6(26239\lambda_i - 42079)x^{50}\\
&\quad - 540(23199\lambda_i - 19343)x^{45} + 105(737719\lambda_i - 953143)x^{40}\\
&\quad - 72(1815127\lambda_i - 145087)x^{35} - 4(8302981\lambda_i + 49913771)x^{30}\\
&\quad + 72(1815127\lambda_i - 145087)x^{25} + 105(737719\lambda_i - 953143)x^{20}\\
&\quad + 540(23199\lambda_i - 19343)x^{15} + 6(26239\lambda_i - 42079)x^{10}\\
&\quad + 36(19\lambda_i + 29)x^5 + (\lambda_i - 1)\\
L &= \prod_{i=1}^{\delta} G_i.
\end{aligned}$$

Let x and y be residually transcendental elements in $\mathbb{F}_0$ such that $\mathbb{F}_0 = k_0(x, y)$ and $y^2 = F(x)$. According to [Sha03] § 4.5, we may assume that the polynomial F is one of the following forms:

$$F = L, SL, TL, STL, RL, RSL, RTL, RSTL$$

where the λ_i's, appearing in the G_i's, are in k_0 and δ is the dimension of the Hurwitz space $\mathcal{H}(G_0, \mathbf{C})$, the space of the family of covers

$$\varphi : \mathcal{X}_g \to \mathbb{P}^1$$

with fixed signature $\mathbf{C}$ and genus g (the genus of X_0). We recall that the space $\mathcal{H}(G_0, \mathbf{C})$ is a finite dimensional subspace of the moduli space of genus g hyperelliptic curves.

Note that, according to [Sha03] Table 1, if $F = L, SL, TL$ or STL, the group G_0 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_5$. In the other cases, G_0 must be isomorphic to $\mathrm{SL}_2(5)$.

For $p = 3$, the reduction modulo 3 of the polynomials $G_i(x), R(x), S(x)$ are respectively $(\lambda_i - 1)(\overline{x}^{10} + 1)^6, (\overline{x}^{10} + 1)^3, (\overline{x}^{10} + 1)^2$ and the polynomial T is irreducible in characteristic 3. So, if we assume that R or ST divides the polynomial F, then the genus of the residue function field $k(\overline{x}, \overline{y})$ defined by

$$\overline{y}^2 = \overline{F}(\overline{x})$$

is $\overline{g} \geq 1$. But, note that $g > \overline{g}$ where g denotes the genus of the function field $\mathbb{F}_0|k_0$. Furthermore, we have

$$[k(\overline{x}, \overline{y}) : k(\overline{x})] = 2$$

since the genus of $k(\overline{x}, \overline{y})$ is non-zero. On the other hand, we have

$$[\mathbb{F} : k(\overline{x})] = 2$$

and $\mathbb{F} \supseteq k(\overline{x}, \overline{y})$. Hence, $\mathbb{F} = k(\overline{x}, \overline{y})$. This is a contradiction. As, the valuation v is a good reduction, we must have

$$\overline{g} = g.$$

Therefore, the polynomials ST and R can not divide the polynomial F. We conclude that,

$$F = L, SL, T.$$

In these cases, the residue function field $k(\overline{x}, \overline{y})$ is of genus 0. That might be possible. So G could be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_5$.

Now, if p=5, the reduction modulo 5 of the polynomials $G_i(x)$, $R(x)$, $S(x)$ and $T(x)$ are respectively $(\lambda_i - 1)(\overline{x}^2 + \overline{x} - 1)^{30}$, $(\overline{x} + 2)^5(\overline{x} - 2)^{25}$, $(\overline{x}^2 + \overline{x} - 1)^{10}$ and $(\overline{x}^2 - 1)^5$. Using the same arguments as above, we must have,

$$F = L, SL, TL, STL, RL, RSG$$

and $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_5$ or $\mathrm{SL}_2(5)$.

$\underline{4^{\text{th}}\textit{case}}$: If $H \simeq \mathcal{A}_4$ or $\mathcal{S}_4$;

In both cases, we have $p = 3$. We shall use the same argument with the same notations as above.

First, suppose we have $H \simeq \mathcal{A}_4$. We consider the following polynomials:

$$\begin{aligned} G_i &= x^{12} - \lambda_i x^{10} - 33x^8 + 2\lambda_i x^6 - 33x^4 - \lambda_i x^2 + 1 \\ R &= x^4 + 2\sqrt{-3}x^2 + 1 \\ S &= x^8 + 14x^4 + 1 \\ T &= x(x^4 - 1) \\ L &= \prod_{i=1}^{\delta} G_i. \end{aligned}$$

According to T. Shaska in [Sha03], we may assume that the function field $\mathbb{F}_0 = k_0(x, y)$ is defined by

$$y^2 = F(x)$$

with

$$F(x) = L, RL, SL, TL, TRL, TSL.$$

In the cases when, $F = L, RL, SL$, the group G_0 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_4$. Otherwise, $G_0 \simeq \mathrm{SL}_2(3)$.

Among R, S and T, the polynomial S is the only reducible polynomial modulo 3. And we have $S \equiv (x^4 + 1)^2 \bmod 3$. Hence, S can not divide F. Otherwise, it will contradict the fact that v is a good reduction. So, the possible equations for $\mathbb{F}_0|k_0$ are the following:

$$y^2 = L, RL, TL, TRL.$$

Which means the group G_0 could be isomorphic to one of the possibilities which are $\mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_4$ and $\mathrm{SL}_2(3)$.

Now suppose $H \simeq \mathcal{S}_4$. In this case, the polynomials G_i, R, S and T become:

$$\begin{aligned} G_i &= x^{24} + \lambda_i x^{20} + (759 - 4\lambda)x^{16} + 2(3\lambda_i + 1288)x^{12} \\ &\quad + (759 - 4\lambda)x^8 + 2\lambda_i x^6 - 33x^4 + \lambda_i x^4 + 1 \\ R &= x^{12} - 33x^8 - 33x^4 + 1 \\ S &= x^8 + 14x^4 + 1 \\ T &= (x^4 - 1) \\ L &= \prod_{i=1}^{\delta} G_i. \end{aligned}$$

According to T. Shaska in [Sha03], we may assume that the function field $\mathbb{F}_0 = k_0(x, y)$ is defined by

$$y^2 = F(x)$$

with

$$F(x) = L, SL, TL, STL, RL, RSL, RTL, RSTL.$$

In the cases when, $F = L$ or SL, the group G_0 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_4$. If $F = TL$ or STL, we have $G_0 \simeq \mathrm{GL}_2(3)$. The group $G_0 \simeq W_2$ in the cases when $F = RL$ or RSL. And G_0 is isomorphic to W_3 for the rest of the possibilities.

Using the same reasoning again, the polynomials R and S are reducible modulo 3. We have $S \equiv (x^4 + 1)^2 \bmod 3$ and $R \equiv (x^4 + 1)^3 \bmod 3$. But, T is irreducible modulo 3. Which means R and S could not divide the polynomial F. Hence, we must have:

$$F = L, TL.$$

We conclude that G_0 could be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_4$ or $\mathrm{GL}_2(3)$.

For the converse, we shall use Lemma 5.1.2. We know that any cyclic group is an Oort group. So, the groups $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/2p\mathbb{Z}$ are liftable to characteristic 0.

The dihedral group D_{2p} is liftable to characteristic 0 for $p \neq 2$ since $D_{2p} \simeq \mathbb{Z}/2\mathbb{Z} \times D_p$ and D_p with $\mathbb{Z}/p\mathbb{Z}$ are the only cyclic-by-p subgroups which are Oort groups.

Finally, the groups $\mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_4, \mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_4, \mathbb{Z}/2\mathbb{Z} \times \mathcal{A}_5, \mathrm{SL}_2(3), \mathrm{GL}_2(3)$ and $\mathrm{SL}_2(5)$ are liftable to characteristic 0 using the fact that their cyclic-by-p subgroups are Oort groups for $p = 3$ or 5.

□

Remark 5.2.5. *One natural question to ask is the following: Does all the groups on the list above (Theorem 5.2.4) occur as full automorphisms groups of hyperelliptic curves? Sanjeewa, in [San09], gives a list of all finite groups that can occur as automorphisms groups of cyclic curves in any characteristic. All the groups on our list above appear in Sanjeewa's list in any prime characteristic, except, the group* $\mathrm{SL}_2(5)$ *in characteristic* 5 *and the group* $\mathrm{GL}_2(3)$ *in characteristic* 3.

However, there exists a hyperelliptic curve in characteristic 3 *which has* $\mathrm{GL}_2(3)$ *as full automorphism group. The curve is defined as follows:*

$$X/k: \ y^2 = x^6 + x^4 + x^2 + 1 \ (\textit{See}\ [\textit{KY00}]).$$

Moreover, according to Shaska in [Sha03] Example 5.2, in characteristic 0*, the curve defined by:*

$$y^2 = x^6 + a_1x^4 + a_2x^2 + 1$$

has $\mathrm{GL}_2(3)$ *as full automorphism group if and only if* $(u_1, u_2) = (-250, 50)$ *where*

$$u_1 = a_1^3 + a_2^3, \ u_2 = 2a_1a_2.$$

Therefore, the curve defined in characteristic 0 *by*

$$X_0: \ y^2 = x^6 - 5x^4 - 5x^2 + 1$$

has $\mathrm{GL}_2(3)$ *as full automorphism group. Since* $-5 \equiv 1 \mod 3$*, the automorphism group of* X/k *is liftable to characteristic* 0*. Hence, the group* $\mathrm{GL}_2(3)$ *should appear in the list of Sanjaeewa in characteristic* 3.

Remark 5.2.6. *Theorem 5.2.4 provides us with the list of the automorphism groups of hyperelliptic curves over* k*, of characteristic* $p \neq 2$*, that can be lifted to characteristic* 0*. In the case when the characteristic of* k *is equal to* 2*, our* *methods in the proof of the theorem do not seem to apply. The main reason is the fact that in characteristic* 2*, the minimal affine equation of the curve* X *is given by*

$$y^2 + P(x)y = F(x),\ \ P(x), F(x) \in k(x)$$

where $P(x)$ *is possibly a non-zero polynomial.*

For the rest of the chapter, we assume that the prime characteristic of the base field k is odd.

According to Shaska (See [Sha06]), determining the automorphism group G of a cyclic curve X/k in the case when $p > 2g+1$ is the same as in characteristic 0. Our next proposition gives a necessary and sufficient condition for G to be liftable to characteristic 0 in this case.

Proposition 5.2.7. *Let* X/k *be a smooth cyclic curve of genus* g *and denote by* G *its full automorphism group. Assume that* $p > 2g+1$*. Let* n *be a positive integer such that* $(n, p) = 1$ *and* n *is the order of the cyclic normal subgroup* N *of* G *such that the quotient space* X/N *has genus* 0*. Then, the group* G *is liftable to characteristic* 0 *if and only if* p *does not divide the order of* G*.*

Proof. Assume first that X/k is a hyperelliptic curve. Let us prove the proposition by contradiction.

Suppose that G is liftable to characteristic zero and p divides the order of G. We shall use the same notations we used in the proof of Theorem 5.2.4.

By hypothesis, since the genus of the curve X/k is always ≥ 2, we may assume that $p > 5$. According to Theorem 5.2.4, the group G_0 is isomorphic to $\mathbb{Z}/2p\mathbb{Z}$ or D_{2p}. If $G_0 \simeq \mathbb{Z}/2p\mathbb{Z}$, then the equation of the curve X_0/k_0 is one of the following (see [Sha06]):

$$\begin{aligned} y^2 &= x^{2g+2} + a_1 x^{p(t-1)} + \cdots + a_\delta x^p + 1, t = \frac{2g+2}{p} \\ &= x^{2g+2} + a_1 x^{p(t-1)} + \cdots + a_\delta x^p + 1, t = \frac{2g+1}{p}, \text{or} \\ &= x(x^{pt} + a_1 x^{p(t-1)} + \cdots + a_\delta x^p + 1), t = \frac{2g}{p}. \end{aligned}$$

In all cases, we have $p \geq 2g+2 \geq pt$. Since $2g+2$ is even, we conclude that $p > pt$ which is impossible. Thus, G is not isomorphic to $\mathbb{Z}/2p\mathbb{Z}$.

Now, if $G \simeq D_{2p}$, then the equation of the curve X_0/k_0 is of the form:

$$y^2 = x.\prod_{i=1}^{t}(x^{2p} + \lambda_i x^p + 1),\ \ t = \frac{g+1}{p}.$$

But, by hypothesis, we have $p \geq 2g+2$ which contradicts the fact that $pt = g+1$ for some integer t.

We use the same reasoning in the case when the cyclic curve is not necessarily hyperelliptic. Indeed, with the assumption $(n, p) = 1$, the genus of the corresponding function field is

$$g = \frac{n-1}{2}(-1+pt) \text{ or } (n-1)(-1+pt)$$

for some integer t. This contradicts the hypothesis, $p > 2g + 1$. □

Considering the results we have so far, we expect the following generalisation of Theorem 5.2.4:

Conjecture 5.2.8. *Let X be a smooth cyclic curve over k. Let n be a positive integer such that $(2n, p) = 1$ and n is the order of the cyclic normal subgroup of $G = \mathrm{Aut}_k(X)$ such that the quotient space X/N has genus 0. The group G is liftable to characteristic 0 if and only if G is an Oort-group for k.*

Note that if Conjecture 5.2.8 is true, using the results of Sanjeewa in [San09], we have a complete list of all liftable automorphism groups of cyclic curves with the same hypothesis as in the conjecture. In the case when p divides n, we might have an automorphism group which is liftable to characteristic 0 but not an Oort group for k.

Chapter 6

On the Tchebotarev Density Theorem for Function fields

The Tchebotarev Density Theorem for number fields, as well as for global function fields, is one the most important results in the study of class field theory. Extending this theorem to more general contexts such as arbitrary function fields is our main goal in this chapter. We attempt to use mainly our diagram in Lemma 3.2.8 and Theorem 4.3.5.

For this purpose, let us first recall some definitions and results in order to state the famous Tchebotarev Density Theorem for function fields properly.

6.1 Results on the Tchebotarev Density Theorem for function fields

Let $\mathbb{F}|\mathbb{E}$ be a finite Galois extension of function fields and denote by G its corresponding Galois group. To simplify, we assume that both of the function fields $\mathbb{F}$ and $\mathbb{E}$ have the same constant field k.

Let P be a place of $\mathbb{E}|k$. Consider a place B of $\mathbb{F}|k$ lying over P. Recall that, according to Proposition 2.1.6, the group G acts as a group permutations on the set of places above P. That is: the other places of $\mathbb{F}|k$ lying over P are of the form $\sigma(B)$ for some $\sigma \in G$.

Let us define two important subgroups of G associated to the place B : The `decomposition group`[1] of B over P

$$Z(B|P) := \{\sigma \in G \,|\, \sigma(B) = B\}$$

[1] In another case, the decomposition group has been used in Chapter 4, but for convenience we use this notation here.

and the `inertia group` of B over P

$$I(B|P){:=}\{\sigma \in G \,|\, \sigma(x) - x \equiv 0 \bmod B,\ \forall x \in \mathcal{O}_B\}$$

where $\mathcal{O}_B$ denotes the discrete valuation ring associated to the place B of $\mathbb{F}$.

Denote respectively by k_B and k_P the residue class fields of the discrete valuations $\mathcal{O}_B$ and $\mathcal{O}_P$. It is well known that the extension $k_B|k_P$ is also a Galois extension. Moreover, there is a natural homomorphism from $Z(B|P)$ onto $\mathrm{Gal}(k_B|k_P)$ and its kernel is the inertia group $I(B|P)$. Furthermore, the order of $Z(B|P)$ and $I(B|P)$ are $e(B/P) \cdot f(B/P)$ and $e(B/P)$ respectively. That is to say that the following sequence is exact:

$$1 \to I(B|P) \to Z(B|P) \to \mathrm{Gal}(k_B|k_P) \to 1.$$

See [Ros02] Chapter 9 for more details. So, in particular, if $B|P$ is unramified, then:

$$Z(B|P) \simeq \mathrm{Gal}(k_B|k_P).$$

Now, suppose that the constant field k is a finite field. In this case, the residue fields k_B and k_P are also finite fields. Thus, the Galois group $\mathrm{Gal}(k_B|k_P)$ is cyclic and generated by the Frobenius automorphism ϕ_P, which is defined by

$$\phi_P(x) = x^{NP}, \text{ for every } x \in k_B$$

where $N(P){:=}|k_P|$, the cardinality of the finite field k_P.

Let us assume that $B|P$ is unramified. Via the isomorphism from $Z(B|P)$ onto $\mathrm{Gal}(k_B|k_P)$, there exists a unique element $(B, \mathbb{F}|\mathbb{E}) \in Z(B|P)$ which corresponds to ϕ_P. We also call $(B, \mathbb{F}|\mathbb{E})$ the `Frobenius automorphism` of B for the extension $\mathbb{F}|\mathbb{E}$. By definition of the automorphism ϕ_P, the Frobenius automorphism of B can be characterized by

$$(B, \mathbb{F}|\mathbb{E})x \equiv w^{N(P)} \bmod B, \text{ for every } x \in \mathcal{O}_B.$$

Note that for any $\sigma \in G$, we have:

$$(\sigma(B), \mathbb{F}|\mathbb{E}) = \sigma(B, \mathbb{F}|\mathbb{E})\sigma^{-1}$$

since $\sigma(B)|P$ is also unramified and $\sigma(\mathcal{O}_B) = \mathcal{O}_{\sigma(B)}$. Furthermore, since the group G acts transitively on the set of places of $\mathbb{F}$ lying over P, we conclude that the Frobenius automorphisms $(B, \mathbb{F}|\mathbb{E})$, as B varies over the places above P, fill out a conjugacy class in G.

Definition 6.1.1. *Let $\mathbb{F}|\mathbb{E}$ be a Galois extension of function fields over the finite field k and P be a place of $\mathbb{E}$ which is unramified in $\mathbb{F}$. We call the set of all Frobenius automorphisms $(B, \mathbb{F}|\mathbb{E})$, as B varies over the places of $\mathbb{F}$ above P, **the Artin conjugacy class of** P.*

By abuse of notation, we will also denote by $(P, \mathbb{F}|\mathbb{E})$, the Artin conjugacy class of P. The map from $S(\mathbb{E}|k)$, the set of places of $\mathbb{E}|k$, to the conjugacy classes of Gal$(\mathbb{F}|\mathbb{E})$ *defined by*

$$P \mapsto (P, \mathbb{F}|\mathbb{E})$$

*is called **the Artin map**.*

Our aim is now to investigate the set of places of $\mathbb{E}$ which map to a given conjugacy class in G via the Artin map. For a given subset $\mathcal{M}$ of $S(\mathbb{E}|k)$, we introduce the `Dirichlet density` of $\mathcal{M}$ which is defined by

$$\delta(\mathcal{M}) = \lim_{s \to 1^+} \frac{\sum_{P \in \mathcal{M}} N(P)^{-s}}{\sum_{P \in S(\mathbb{E}|k)} N(P)^{-s}}$$

if the limit exists. In the case when the limit does not exist, we say that the set $\mathcal{M}$ does not have Dirichlet density. Note that s tends to 1 through real values and when the density $\delta(\mathcal{M})$ exists, we have

$$0 \leq \delta(\mathcal{M}) \leq 1.$$

For more details about the notion of Dirichlet density, the reader can use the book [Ros02].

We are now able to state the Tchebotarev Density Theorem for global functions fields.

Theorem 6.1.2. *Let $\mathbb{F}|\mathbb{E}$ be a Galois extension of function fields over the finite field k. Denote by G the Galois group of $\mathbb{F}|\mathbb{E}$. Let C be a conjugacy class in G and $S^{unr}(\mathbb{E}|k)$ be the set of places of $\mathbb{E}$ which are unramified in $\mathbb{F}$. then:*

1. ***First version:***

$$\delta\left(\{P \in S^{unr}(\mathbb{E}|k) \,|\, (P, \mathbb{F}|\mathbb{E}) = C\}\right) = \frac{|C|}{|G|}.$$

In particular, the conjugacy class C is of the form $(P, \mathbb{F}|\mathbb{E})$ for infinitely many places P of $\mathbb{K}$.

2. ***Second version:*** *For each positive integer n, we have*

$$\#\left\{P \in S^{unr}(\mathbb{E}|k) \,|\, \deg_{\mathbb{E}} P = n,\ (P, \mathbb{F}|\mathbb{E}) = C\right\} = \frac{|C|}{|G|}\frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n}\right)$$

where q is the cardinality of the base field k. In particular, for every sufficiently large integer n, there is a place P of degree n with the propriety $(P, \mathbb{F}|\mathbb{E}) = C$.

Proof. See [Ros02] Theorem 9.13A. and Theorem 9.13B. □

A natural question to ask is whether some form of Theorem 6.1.2 still holds in the case when k is no longer assumed to be finite. As far as we know, this is still an open problem. However, a weak partial answer can be deduced from the following theorem which can be found in [Sch34]:

Theorem 6.1.3 (F.K Schmidt)**.** *Let $\mathbb{F}|\mathbb{E}$ be a finite Galois extension of function fields over a Hilbertian field k. Then for any subgroup H of the Galois group* $\mathrm{Gal}(\mathbb{F}|\mathbb{E})$, *there are infinitely many valuations on $\mathbb{F}$ which are constant on k and have the group H as decomposition group.*

To end this introductory section, for convenience, let us make the following definition:

Definition 6.1.4. *Let $\mathbb{F}|\mathbb{E}$ be a Galois extension of function fields over the field k. If Theorem 6.1.2 holds for the extension $\mathbb{F}|\mathbb{E}$, we say that such extension has **the Tchebotarev Density Theorem property** or simply the TDT **property**.*

6.2 Lifting the Tchebotarev Density Property

Let $(\mathbb{F}|k, v)$ be a valued function field where the valuation v is a good reduction. Denote by $\overline{\mathbb{F}}|\overline{k}$ the corresponding residual function field.

Let us consider a sub-extension denoted by $\mathbb{E}$ of $\mathbb{F}|k$. We assume that $\mathbb{E}$ has k as constant field and the extension $\mathbb{F}|\mathbb{E}$ is finite and Galois. Denote by G the Galois group which corresponds to $\mathbb{F}|\mathbb{E}$. Then according to Theorem 4.3.5 and Theorem 3.2.7, we have:

1. $G \simeq \mathrm{Aut}(\overline{\mathbb{F}}|\overline{\mathbb{E}})$ and $[\mathbb{F} : \mathbb{E}] = \left[\overline{\mathbb{F}} : \overline{\mathbb{E}}\right]$;

2. $\mathbb{E}$ and $\overline{\mathbb{E}}$ have the same genus.

Denote by ϕ the natural isomorphism from G onto $\mathrm{Aut}(\overline{\mathbb{F}}|\overline{\mathbb{E}})$ we defined in Chapter 4. Note also that the extension $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ is also Galois.

Now, let us assume that $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ has the TDT property.

Definition 6.2.1. *Let $(\mathbb{F}|k, v)$ be a valued function field where v is assumed to be a good reduction. Let $\mathbb{E}|k$ be a subextension of $\mathbb{F}$ such that $\mathbb{F}|\mathbb{E}$ is finite and Galois extension. Suppose that the corresponding residual extension of function fields $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ has the Tchebotarev Density Theorem property. We say that the TDP property of $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ **lifts with respect to the valuation** v if* *for all conjugacy classes C in $\mathrm{Gal}(\mathbb{F}|\mathbb{E})$ and for all unramified places $\overline{P}$ of $\overline{\mathbb{E}}|\overline{k}$ with $(\overline{P}, \overline{\mathbb{F}}|\overline{\mathbb{E}}) = C$, there exists a place P of $\mathbb{E}|k$ such that*

$$\overline{P} = \mathbf{h}_{\mathbb{E}}(P)$$

where $\mathbf{h}_{\mathbb{E}}$ is the arithmetic divisor homomorphism from $\mathrm{Div}(\mathbb{E}|k)$ to $\mathrm{Div}(\overline{\mathbb{E}}|\overline{k})$ and

$$\phi\left[(P, \mathbb{F}|\mathbb{E})\right] = (\overline{P}, \overline{\mathbb{F}}|\overline{\mathbb{E}}).$$

Let us recall the valued function field $(\mathbb{F}|k, v)$ that we defined in the beginning of this section. Our main goal is to find necessary and sufficient conditions so that the TDT property of the extension $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ lifts with respect to v. By definition, a necessary condition is that the arithmetic divisor homomorphism $\mathbf{h}_{\mathbb{E}}$ from $\mathrm{Div}(\mathbb{E}|k)$ to $\mathrm{Div}(\overline{\mathbb{E}}|\overline{k})$ must be surjective. Note that this could happen. For instance, in the case when $\mathbb{E}$ is a rational function field. Thus, let us admit that $\mathbf{h}_{\mathbb{E}}$ is surjective.

Let $\overline{P}$ be a place of $\overline{\mathbb{E}}$ which is unramified in $\overline{\mathbb{F}}$. Since $\mathbf{h}_{\mathbb{E}}$ is surjective, then there exists a place P of $\mathbb{E}$ which corresponds to the place $\overline{P}$ via the homomorphism $\mathbf{h}_{\mathbb{E}}$. Then, using Lemma 3.2.8, we have:

Proposition 6.2.2. *The place P is also unramified in $\mathbb{F}$.*

Proof. Let us prove the proposition by contradiction. Denote by $\mathbf{h}$ the arithmetic divisor homomorphism from $\mathrm{Div}(\mathbb{F}|k)$ to $\mathrm{Div}(\overline{\mathbb{F}}|\overline{k})$. Suppose we have s places of $\mathbb{F}$ lying over P. Denote by $B_1, \cdots, B_s$ these places. Since, P is ramified in $\mathbb{F}$ and $\mathbb{F}|\mathbb{E}$ is Galois, then there exists an integers $e > 1$, such that

$$\mathbf{h}(c(P)) = e \cdot \sum_{1 \leq i \leq s} \mathbf{h}(B_i)$$

where $c(P)$ denotes the conorm of P with respect to $\mathbb{F}|\mathbb{E}$. On the other hand, since $\overline{P}$ is unramified in $\overline{\mathbb{F}}$, we have

$$\overline{c}(\overline{P}) = \sum_{1 \leq j \leq \overline{s}} \overline{B_j}$$

where $\overline{B_j}$, $1 \leq j \leq \overline{s}$, denote all the places of $\overline{\mathbb{F}}$ lying over $\overline{P}$. The notation $\overline{c}$ denotes the conorm map from $\mathrm{Div}(\overline{\mathbb{E}}|\overline{k})$ to $\mathrm{Div}(\overline{\mathbb{F}}|\overline{k})$.

By, using Lemma 3.2.8, we have:

$$\mathbf{h}(c(P)) = e \cdot \sum_{1 \leq i \leq s} \mathbf{h}(B_i) = \sum_{1 \leq j \leq \overline{s}} \overline{B_j} = \overline{c}(\overline{P}).$$

Since all of the places $\overline{B_j}$ are all distinct, we conclude that e must be equal to 1. □

Remark 6.2.3. *Let $\overline{P}$ be an arbitrary place of $\overline{\mathbb{E}}$ such that there exists a place P in $\mathbb{E}$ with $\mathbf{h}_{\mathbb{E}}(P) = \overline{P}$. Let B (resp. $\overline{B}$) be a place of $\mathbb{F}$ (resp. of $\overline{\mathbb{F}}$) lying over P (resp. $\overline{P}$). Observing the proof of Proprosition 6.2.2, we conclude that*

$$e(B|P) = e(\overline{B}|\overline{P}).$$

In particular, $\overline{P}$ is unramified in $\overline{\mathbb{F}}$ if and only if P is unramified in $\mathbb{F}$.

Let B be a place in $\mathbb{F}$ above P. Consider the set S_B which consists of places in the Supp $(\mathbf{h}(B))$. The extensions $\mathbb{F}|\mathbb{E}$ and $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ are Galois. Therefore, every place in $\mathbb{F}$ above P is of the form $\sigma(B)$ for some $\sigma \in G$. Now consider the decomposition group $Z(B|P)$. Then:

Lemma 6.2.4. *The group $Z(B|P)$ acts transitively on the set S_B. In particular, if S_B consists of only one place, then $Z(B|P) \simeq Z(\overline{B}|\overline{P})$ where $\overline{B} = \mathbf{h}(B)$. In this particular case, the TDT property of $\mathbb{F}|\mathbb{E}$ lifts with respect to the valuation v.*

Proof. Let $\overline{B}$ be an arbitrary place in S_B. Let us first prove that $Z(\overline{B}|\overline{P})$ is a subgroup of $Z(B|P)$.

Let $\sigma \in Z(\overline{B}|\overline{P})$. Denote $\sigma(B)$ by B_0. We have,

$$\mathbf{h}(\sigma(B)) = \sigma(\mathbf{h}(B)) = \mathbf{h}(B_0).$$

Thus, $\overline{B}$ is in S_{B_0}. Therefore, $\mathbf{h}(B) = \mathbf{h}(B_0)$ and $B = B_0$. Otherwise, the place $\overline{B}$ will have a ramification index at least 2 in $\overline{\mathbb{F}}$, contradicting the fact that $\overline{P}$ (resp. P) unramified in $\overline{\mathbb{F}}$ (resp. $\mathbb{F}$). Hence, $\sigma(B) = B$. We conclude also that if B and B_0 are two places lying above P, we have either $S_B = S_{B_0}$ or $S_B \cap S_{B_0} = \emptyset$.

Now let $\overline{B}_1$ and $\overline{B}_2$ be two places in S_B. We know that H acts transitively on the set of places lying above $\overline{P}$. By definition, $\overline{B}_1$ and $\overline{B}_2$ are places lying above $\overline{P}$. Thus, there exists $\sigma \in H$ such that $\sigma(\overline{B}_1) = \overline{B}_2$. We should prove that σ is indeed in $Z(B|P)$. Denote $\sigma(B)$ by B_0. Then, B and B_0 are places lying above P. Therefore, we have either $S_B = S_{B_0}$ or $S_B \cap S_{B_0} = \emptyset$. However, by definition of σ and B_0, the place $\overline{B}_2 \in S_{B_0}$. Hence, $S_B \cap S_{B_0} \neq \emptyset$. Thus, $S_B = S_{B_0}$ and $B = B_0$.

The rest of the lemma is straightforward. □

According to what we have done so far, we conclude:

Theorem 6.2.5. *Let $(\mathbb{F}|k, v)$ be a valued function field where v is assumed to be a good reduction. Let $\mathbb{E}|k$ be a subextension of $\mathbb{F}$ such that $\mathbb{F}|\mathbb{E}$ is a finite and Galois extension. Suppose that the corresponding residual extension of* *function fields* $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ *has the Tchebotarev Density Theorem property. The TDT property of* $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ *lifts with respect to the valuation* v *if and only if the arithmetic divisor homomorphism between* $\operatorname{Div}(\mathbb{E}|k)$ *and* $\operatorname{Div}(\overline{\mathbb{E}}|\overline{k})$ *is surjective and for all unramified places* $\overline{P}$ *of* $\overline{\mathbb{E}}$*, there exists a place* P *of* $\mathbb{E}$ *such that* $\mathbf{h}_{\mathbb{E}}(P) = \overline{P}$ *and the divisor* $\mathbf{h}(B)$ *is a place of* $\overline{\mathbb{F}}$ *for all places* B *of* $\mathbb{F}$ *lying over* P*.*

It is important to note that observing Theorem 6.1.2, if the TDT property of $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ lifts with respect to the valuation v, then:

- Every conjugacy class C in G is of the form $(P, \mathbb{F}|\mathbb{E})$ for infinitely many places P of $\mathbb{E}$;
- Furthermore, for a given conjugacy class C in G for every sufficiently large integer n, there is a place P of degree n with the property $(P, \mathbb{F}|\mathbb{E}) = C$.

We now give an example of a family of such function fields.

Theorem 6.2.6. *Let* $(\mathbb{F}|k, v)$ *be a valued hyperelliptic function field where* v *is assumed to be a good reduction. Let* $\mathbb{E}|k$ *be a subextension of* $\mathbb{F}$ *such that* $\mathbb{E} \subseteq k(x)$ *and* $\mathbb{F}|\mathbb{E}$ *is a finite Galois extension. The field* $k(x)$ *denotes the unique rational subfield of* $\mathbb{F}$ *with* $[\mathbb{F}{:}k(x)] = 2$*. If the corresponding residual extension of function fields* $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ *have the Tchebotarev Density Theorem property, then the TDT property of* $\overline{\mathbb{F}}|\overline{\mathbb{E}}$ *lifts with respect to the valuation* v*.*

Proof. Let $\overline{P}$ be a place of $\overline{\mathbb{E}}$ which is unramified in $\overline{\mathbb{F}}$. By hypothesis, we have $\overline{\mathbb{E}} \subseteq \overline{k}(\overline{x}) \subset \overline{\mathbb{F}}$. So, the place $\overline{P}$ of $\overline{\mathbb{E}}$ is also unramified in $\overline{k}(\overline{x})$. Let $\overline{P}_i$ be a place of $\overline{k}(\overline{x})$ lying over $\overline{P}$. Since the arithmetic divisor homomorphism $\mathbf{h}_{k(x)}$ from $\operatorname{Div}(k(x)|k)$ to $\operatorname{Div}(\overline{k}(\overline{x})|\overline{k})$ is surjective, there exists a place P_i of $k(x)$ such that

$$\mathbf{h}_{k(x)}(P_i) = \overline{P}_i.$$

Now consider the place $P{:=}P_i \cap \mathbb{E}$ of $\mathbb{E}$. By definition of P, we have

$$\mathbf{h}_{\mathbb{E}}(P) = \overline{P}.$$

However, by construction of the place P_i of $k(x)$, the set $\operatorname{Supp}\left(\mathbf{h}_{k(x)}(P_i)\right)$ consists of only one element (the place $\overline{P}_i$ of $\overline{k}(\overline{x})$).

Furthermore, by hypothesis, the place $\overline{P}$ is unramified in $\overline{\mathbb{F}}$. Therefore, P is also unramified in $\mathbb{F}$ as well as the place P_i of $k(x)$. Since

$$[\mathbb{F}{:}k(x)] = \left[\overline{\mathbb{F}}{:}\overline{k}(\overline{x})\right] = 2,$$

then the places P_i and $\overline{P}_i$ split completely in $\mathbb{F}$ and in $\overline{\mathbb{F}}$ respectively. Thus, if B is one of the 2 places of $\mathbb{F}$ lying over P_i, since

$$\deg_{\overline{k}(\overline{x})} \overline{P}_i = \deg_{k(x)} P_i = \deg_{\mathbb{F}} B,$$

the set $\mathrm{Supp}\,(\mathbf{h}_{\mathbb{F}}(B))$ consists of only one element which is a place of $\overline{\mathbb{F}}$ lying over the place $\overline{P}$ of $\overline{\mathbb{E}}$. The map $\mathbf{h}$ denotes the arithmetic divisor homomorphism from $\mathrm{Div}(\mathbb{F}|k)$ to $\mathrm{Div}(\overline{\mathbb{F}}|\overline{k})$. Finally, using Lemma 6.2.4, we conclude that

$$\phi\,[Z(B|P)] = Z(\mathbf{h}(B)|\overline{P})$$

for all place B of $\mathbb{F}$ lying over P. Hence, for any place $\overline{P}$ of $\overline{\mathbb{E}}$, which is unramified in $\overline{\mathbb{F}}$, there exist a place P of $\mathbb{E}$ such that:

$$\mathbf{h}_{\mathbb{E}}(P) = \overline{P}$$

and

$$\phi\,[(P, \mathbb{F}|\mathbb{E})] = (\overline{P}, \overline{\mathbb{F}}|\overline{\mathbb{E}}).$$

□

Remark 6.2.7. *Theorem 6.2.6 still holds for other types of cyclic function fields, not necessary hyperelliptic, such as the p-cyclic function fields (p is a prime number). For a given positive integer, a cyclic function field $\mathbb{F}|k$ is said to be n-cyclic if the cyclic normal subgroup N of* $\mathrm{Aut}(\mathbb{F}|k)$, *such that the subfunction field $\mathbb{F}^N$ of $\mathbb{F}$ has genus* 0, *is of order n. The proof is exactly the same as we did for hyperelliptic function field.*

Bibliography

[BGG93] E. Bujalance, J. Gamboa, and G. Gromadzki, *The full automorphism groups of hyperelliptic Riemann surfaces*, Manuscripta Math. **79** (1993), 267–282.

[CGH08] T. Chinburg, R. Guralnick, and D. Harbater, *Oort groups and Lifting problems*, Compositio Math. **144** (2008), 849–866.

[Deu42] M. Deuring, *Reduktion algebraischer Funktionenkorper nach Primdividoren des Konstankorpers*, Math.Z **47** (1942), 643–654.

[DM69] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Math. Inst. Hautes études Sci. **36** (1969), 75–109.

[End72] O. Endler, *Valuation theory*, Springer Verlag, Berlin-Heidelberg-New York, 1972.

[Fab12] X. Faber, *Finite p-irregular subgroups of* $\mathrm{PGL}_2(k)$, arXiv:1112.1999v2 [math.NT] 14 Mar 2012 (2012).

[GMP89] B. Green, M. Matignon, and F. Pop, *On valued function fields I*, Manuscripta Math. **65** (1989), 257–276.

[GMP90] ______, *On valued function fields II, Regular functions and elements with uniqueness property*, J. reine angew. Math. **412** (1990), 128–149.

[GMP92] ______, *On valued function fields III, Reduction of algebraic curves*, J. reine angew. Math. **432** (1992), 117–133.

[Gre96] B. Green, *The relative genus inequality for curves over valuation rings*, Journal of Algebra **181** (1996), 836–856.

[Gro71] A. Grothendieck, *SGA1: Exposé XIII*, arXiv:02062203v2 [math.AG] 4 Jan 2004 (1971), 275–293.

[Har10] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer Science+Business media, 2010.

[Hur93a] A. Hurwitz, *Uber algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1893), 403–442.

[Hur93b] ______, *Ueber Algebraische Gebilde mit eindeutigen Transformationen in sich.*, Math. Ann. **41** (1893), 403–442.

[Kas90] T. Kasser, *Reduktion von Differentialen algebraischer Funktionenkorper*, Diplomarbeit, Universitat Heidelberg (1990).

[Kna90] H. Knaf, *Reduktion von Funktionenkorpern und Automorphismengruppen*, Diplomarbeit, Universitat Heidelberg (1990).

[KY00] A. Kontogeorgis and Y. Yang, *Automorphisms of hyperelliptic modular curves $x_0(n)$ in positive characteristic*, LMS J. Comput. Math. **13** (2000), 144–163.

[Liu02] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics, Oxford University Press, 2002.

[OW14] A. Obus and S. Wewers, *Cyclic extensions and the local lifting problem*, Annals of Mathematics **180** (2014), 233–284.

[PD01] A. Prestel and C. N. Delzell, *Positive Polynomials*, Springer Monographs in Mathematics, Springer, 2001.

[Pop14] F. Pop, *The Oort Conjecture on lifting covers of curves*, Annals of Mathematics **180** (2014), 285–322.

[Roq] P. Roquette, *Abschatzung der Automorphismenanzahl von Funkyionenkorpern bei Primzahlcharakteristik*, math Z. **117**, 157–163.

[Roq87] ______, *Reciprocity in valued function fields*, J. reigne angew. Math. **375/376** (1987), 238–258.

[Ros02] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, Springer-Verlag New-York, 2002.

[Sal06] G. D. V. Salvador, *Topics in the theory of algebraic function fields*, Birkhauser Boston, 2006.

[San09] R. Sanjeewa, *Automorphism Groups of Cyclic curves defined over finite fields of any characteristics*, Albanian jornal of mathematics **3** (2009), 131–160.

[Sch34] F.K. Schmidt, *Uber die Kennzeichnung algebraischer Funktionenkorper durch ihren Regularitatsbreich*, J. Reine Angew. Math **171** (1934), 162–169.

[Sha03] T. Shaska, *Determining the automorphism group of hyperelliptic curve*, Symbolic and algebraic computation: Proceedings of the 2003 international symposium (2003), 248–254.

[Sha06] ______, *Subvarieties of the Hyperelliptic Moduli Determined by Group Actions*, Serdica Math. J. **32** (2006), 355–374.

[Sti73] H. Stichtenoth, *Uber die Automorphismengruppe eines algebraishen Funktionenkorpers von Primezahlcharakteristik. I. Eine Abschatzung der Ordnung der Automorphismengruppe*, Arch. Math. (Basel) **24** (1973), 527–544.

[Sti09] ______, *Algebraic function fields and codes*, Graduate Texts in Mathematics, Springer-Verlag, Berlin Heidelberg, 2009.

[You93] T. Youssefi, *Inegalite Relative des Genres*, Manuscripta mathematica **78** (1993), 111–128.