On a Link Between Towers of Function Fields and Group Theory

Author: Yujia Qiu

Supervisors: Prof. Tanja Lange
            Dr. Alp Bassa

Eindhoven, July 2010
I would like to dedicate this thesis to my loving mother
Acknowledgements

I am grateful to my supervisors Professor Tanja Lange and Alp Bassa, for their constant support and patience, who were indispensable for the completion of this thesis, for I knew next to nothing about the subject matter nine months ago.

My special thanks go to prof. Hendrik Lenstra, who introduced this interesting topic to me and provided me help during my work.

I also want to thank prof. Henk van Tilborg for his caring and support during my study in Technical University of Eindhoven, dr. Ruud Pellikaan for leading me to the beautiful world of algebraic geometric codes, and also dr. Aart Blokhuis, dr. Jan Draisma, prof. Peter Stevenhagen, prof. Bas Edixhoven, prof. Eduard Looijenga, prof. Ronald Cramer for offering lectures of very high quality and instructing me about algebraic geometry and number theory.

I also would like to thank the Technical University of Eindhoven for offering me a good chance to study here and to get a deeper look into the beauty of mathematics.

Last but not the least, I also want to thank all my friends who have offered so much help during my working on the thesis. I owe a lot to my boyfriend Heer Zhao, who spent lots of time on discussing with me on problems I encountered. Also I would like to thank all my friends who offered me lots of support, Shoumin Liu, Qixiao Yu, Jochem Berndsen, Jorn van der Pol, and so on. I want to thank whom has brought all of you into my life, and it makes my life here unforgettable to have friends as you all.
Abstract

The search for explicit equations of function fields over finite fields has attracted lots of attention, especially when the application of asymptotically good towers of function fields to coding theory and cryptography was discovered. When we restrict our view to the towers which are 'built' by finite Galois extensions, the question comes to the mind whether it is possible to translate the concepts in the towers to the properties of corresponding Galois groups so that we may apply some nice tools in group theory to understand the towers better, and if the answer is yes, how the properties of towers show up in terms of group theory. The main purpose of this project is to set up a dictionary linking the theory of towers of function fields to group theory.
# Contents

1 Introduction .................................................. 1
   1.1 Motivation ............................................... 1
   1.2 An Example of Applications .............................. 2
      1.2.1 Mathematical Background .......................... 2
      1.2.2 Algebraic Geometry Codes ......................... 5
   1.3 Sketch of this Thesis .................................... 8

2 Infinite Galois Theory ....................................... 11
   2.1 Galois Groups as Topological Groups .................. 11
   2.2 The Fundamental Theorem of Infinite Galois Theory .. 14

3 Function Fields and Towers of Function Fields ............ 21
   3.1 Algebraic Function Fields .............................. 21
   3.2 The Extensions of Function Fields ..................... 22
   3.3 Towers of Function Fields .............................. 32
   3.4 Two Examples of Towers of Function Fields ........... 37
1. Introduction

1.1 Motivation

To find curves with as many rational points as possible over a finite field is an interesting question in number theory. It has a quite long history. One of the biggest achievements in the last century on this question is the theorem of Hasse-Weil, which is in fact equivalent to the Riemann-Hypothesis for function fields. In the first few decades of the last century these topics have been widely studied, but then they were forgotten for quite some time, until in the beginning of the 80’s Goppa showed how curves over finite fields can be used in the construction of codes, which we will introduce in detail later in this chapter. This gave a new impetus to the area, and intense research has been done subsequently. These applications in coding theory also motivated the study of asymptotic properties of function fields over a fixed finite field and with increasing genus. This question was not only interesting because of applications, but since Ihara noticed that the Hasse-Weil bound cannot be attained for curves over a finite field of large genus (it is shown in [10] that the Hasse-Weil bound can be reached only when $q \leq q(q - 1)/2$ for $q$ the cardinality of the base field), Drinfeld and Vlăduţ (following Ihara’s idea) improved the Hasse-Weil bound in the asymptotic case, then it became interesting also as a purely number theoretic question: how many rational points can a curve of large genus over a finite field have? Using various techniques (class field theory, the theory of modular curves, explicit equations) various people constructed examples of large genus curves with many points. More precisely they constructed sequences of curves all over a fixed finite field with genus tending to infinity, such that each one of these curves has many points with respect to their genus (i.e. $N_1/g$ is large, for $N_1$ the number of rational points and $g$ the genus of the algebraic curve). Subsequently many other applications of such sequences have been found, among others in the
1. Introduction

construction of hash families, low discrepancy sequences, and authentication codes. Recently, a new important application of these construction has been found in secret sharing and secure multi-party computation (see among others [3]). Because of these applications, having explicit equations for these curves, or in other words, explicit towers of function fields which are involved, is important.

1.2 An Example of Applications

Algebraic geometry codes (AG codes) are introduced in detail as follows.

1.2.1 Mathematical Background

We are going to give some mathematical background for the construction of algebraic geometry codes, which will be divided into two parts: algebraic curves, Riemann-Roch theorem and coding theory.

We assume basic knowledge of algebraic varieties.

Definition 1.2.1. An algebraic curve \( C \) is a smooth projective variety of dimension 1.

Note that in [8, Chapter 1, Theorem 6.9], it is stated that up to isomorphism, there is a 1-1 correspondence between the function fields of dimension 1 and the algebraic curves.

Definition 1.2.2. Let \( C \) be an algebraic curve. A divisor \( D \) is an element of the free abelian group generated by the subvarieties of codimension one. For a divisor \( D = \sum P f_P P \), the degree of \( D \) is defined as \( \deg D := \sum f_P \).

For \( f \) a rational function over \( C \), we can define the divisor associated to \( f \) as follows: \( (f) := \sum P \text{ord}_P(f) P \), where the sum goes over all the subvarieties \( P \) of codimension 1 of the curve, and the function \( \text{ord}_P \) evaluates the order of \( P \) as a zero or a pole of \( f \). For \( f = g/h \) a rational function over \( C \), with \( g, h \) regular functions, we can define the divisor associated to \( f \) as \( (f) := (g) - (h) \). For a 1-form \( \omega \), we can define the divisor associated to \( \omega \) as \( (\omega) := \sum P \text{ord}_P(\omega) P \), where the sum goes over all the subvarieties of codimension 1, and the function \( \text{ord}_P \) is defined as \( \text{ord}_P(\omega) := \text{ord}_P(\omega/\text{d}t) \) with \( t \) a local uniformizer.

A divisor \( D \) is called a canonical divisor if there exists a differential \( \omega \) such that \( D = (\omega) \).
1.2. An Example of Applications

Note that the divisor associated to a differential is well defined by [12, Chapter 2, Proposition 4.3].

**Definition 1.2.3.** A divisor $D = \sum_P f_P P$ is called *effective* if $f_P \geq 0$ for all $P$.

Before we can state the Riemann-Roch theorem, we need to define the $\mathcal{L}$-space first.

**Definition 1.2.4.** Given a divisor $D$, we can define a space associated to it as follows:

$$\mathcal{L}(D) := \{ f \in K(C)^* | (f) + D \geq 0 \} \cup \{0\}.$$ 

Note that for any $D$, the set $\mathcal{L}(D)$ is a finite dimensional $k$-vector space, where $k$ is the base field of the curve, and we denote the dimension by $l(D)$.

**Theorem 1.2.5 (Riemann-Roch Theorem).** Let $C$ be an algebraic curve and $K_C$ be a canonical divisor. There is an integer $g \geq 0$, which is called the genus of $C$ such that for any divisor $D$, we have

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

There are a few remarks to the Riemann-Roch theorem.

**Remark 1.2.6.** We can derive from the Riemann-Roch theorem that for a canonical divisor $K_C$, we have that $\deg(K_C) = 2g - 2$, and $l(K_C) = g$.

**Remark 1.2.7.** By the definition of the $\mathcal{L}$-space, the dimension of $\mathcal{L}(D)$ is 0 when $\deg(D)$ is negative. Hence by Riemann-Roch, when $\deg(D) > 2g-2$, we have that $l(D) = \deg(D) - g + 1$.

Here come some definitions from coding theory.

A code is a rule for converting a piece of information into another form of representation. In mathematics, we usually take it as a set of vectors of length $n$, which are called codewords. And usually, we require the code to have some algebraic structure which helps us to encode and decode. To avoid the interruption by possible noises, we always add some redundancy to the original information, which could also help correct errors in some cases.

**Definition 1.2.8.** A $q$-ary linear code $C$ is a code which is a linear subspace of $\mathbb{F}_q^n$, where $n$ is called the length of the code. The *dimension* of the code is its dimension as a vector space over $\mathbb{F}_q$. 

---

3
Definition 1.2.9. For a code $C$, the distance of two codewords $x$ and $y$ are defined as

$$d(x, y) := |\{ i \in [1, n] | x_i \neq y_i \}|.$$  

And the weight of a codeword $x$ is defined as $w(x) := d(x, 0)$ The minimal distance $d$ of $C$ is defined as

$$d(C) := \min_{x,y \in C, x \neq y} \{d(x,y)\}.$$  

Note that if $C$ is a linear code, then the minimal distance is just the minimal weight of the code, since $d(x, y) = d(x - y, 0) = w(x - y)$, since $x, y \in C$ induces $x - y \in C$ for $C$ a linear code.

So we have introduced three important parameters of a linear code, namely the length of codewords $n$, the dimension of the code $k$ and the minimal distance $d$. We sometimes denote the code by $[n, k, d]_q$ or $[n, k, d]$ if it will not cause any confusion.

Definition 1.2.10. Let $C$ be a linear code, denoted by $[n, k, d]$. A generator matrix of $C$ is a $k$ by $n$ matrix whose rows form a basis of $C$.

Note that there are many generator matrices for a given linear code, but all of them are equivalent up to linear transformation. Note that a generator matrix is always of full rank, hence there always exists a generator matrix for any linear code $C$ of the form $(I_k \quad A_{k,n-k})$, where $I_k$ is the $k \times k$ identity matrix.

There are a few bounds on the relations of the parameters. We introduce the Singleton bound here. As we have seen, for a linear code $C = [n, k, d]$, all the codewords have minimum weight $d$ and any two of them have minimum distance $d > 0$, in particular, all codewords are distinct. If we delete the last $d - 1$ coordinates of all codewords, then the resulting codewords are still pairwise different. Hence the dimension of the code $C$ cannot exceed the length of the code after deleting coordinates, i.e.

$$k \leq n - d + 1.$$  

This is called Singelton bound, and we call those codes which attains Singelton bound maximum distance separable codes, or MDS codes for brief.
1.2.2 Algebraic Geometry Codes

For some basic notations in coding theory refer to [15]. Consider a geometric object $X$ with a subset $\mathcal{P}$ consisting of $n$ sub-objects which are enumerated as $P_1, P_2, \ldots, P_n$. Suppose that we have a vector space $\mathcal{L}$ over $\mathbb{F}_q$ of functions well-defined on $\mathcal{P}$ with values in $\mathbb{F}_q$, i.e. $f(P_i) \in \mathbb{F}_q$ for all $i$ and $f \in \mathcal{L}$. In this way one has an evaluation map with respect to $\mathcal{P}$:

$$\text{eva}_P : \mathcal{L} \rightarrow \mathbb{F}_q^n$$

$$f \mapsto (f(P_1), \ldots, f(P_n)).$$

This evaluation map is $\mathbb{F}_q$-linear, so its image is a linear subspace of $\mathbb{F}_q^n$. Moreover, the image can be viewed as a linear code.

To get an AG code, the same trick is used, where $X$ is taken as an algebraic curve, $P_i$’s are taken as distinct points on $X$, and the vector space $\mathcal{L}$ is taken as the space $\mathcal{L}(G)$ of a divisor $G$ whose support is disjoint from the set $\{P_1, P_2, \ldots, P_n\}$, where $\mathcal{L}(G)$ is defined as the set of all rational functions $f$ such that the divisor associated to it satisfies that $(f) + G$ is effective. Hence $\mathcal{L}$ is a finite dimensional vector space over $\mathbb{F}_q$ by Theorem 5.2 in Chapter 3 of [8], and by definition the functions in $\mathcal{L}$ are well-defined at all $P_i$’s. Let $D := P_1 + P_2 + \ldots + P_n$. This code is called algebraic geometry code, or AG code for short, and is denoted by $C_{\mathcal{L}}(D, G)$. Or equivalently, we can look at the function field corresponding to an algebraic curve, which means that we can take $X$ to be a function field, and $P_i$’s to be distinct rational places of $X$ (whose definition will be given in Definition 3.1.3). Now we are going to take a look at the parameters $[n, k, d]$ of this code. From algebraic geometry, it is well-known that $\mathcal{L}(G)$ is finite dimensional, and its dimension is denoted as $l(G)$. To get the dimension of the code $C_{\mathcal{L}}(D, G)$, we need to look at the kernel of the map $\text{eva}_D$, which is:

$$\text{Ker}(\text{eva}_D) = \{f \in \mathcal{L}(G) | f(P_i) = 0 \text{ for all } i = 1, 2, \ldots, n\}$$

$$= \{f \in \mathcal{L}(G) | P_i \in \text{Supp}((f)) \text{ for all } i = 1, 2, \ldots, n\}$$

$$= \{f \in X | (f) - G \geq D\}$$

where $(f)$ denotes the divisor associated to $f$. Then by definition, $\text{Ker}(\text{eva}_D) = \mathcal{L}(G - D)$. Hence the dimension of the code is

$$k = l(G) - l(G - D).$$

By the definition of the $\mathcal{L}(G)$, we can see that when the degree of $G$ is strictly smaller than that of $D$, we have that $l(G - D) = 0$, hence in this case, the dimension of the code is just
1. Introduction

the dimension of \( l(G) \). Moreover, suppose that \( f_j, j = 1, 2, \ldots, k \) form a basis of \( \mathcal{L}(G) \), a generator matrix of \( C_L(D, G) \) is given as follows:

\[
\begin{pmatrix}
  f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\
  f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\
  \vdots & \vdots & \cdots & \vdots \\
  f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n)
\end{pmatrix}
\]

In fact, the Riemann-Roch Theorem helps us go further. Recall that the statement of Riemann-Roch says that \( l(G) - l(K - G) = \deg(G) + 1 - g \) for \( K \) a canonical divisor. Hence in any case, the dimension of \( \mathcal{L}(G) \) is always larger than or equal to \( \deg(G) + 1 - g \), where \( g \) denotes the genus of the curve or the function field. In particular, when \( \deg(G) \) is larger than \( 2g - 2 \), which is the degree of a canonical divisor, \( l(G) = \deg(G) + 1 - g \). Thus for \( \deg(G) < n \), the dimension of the code \( k \geq \deg(G) + 1 - g \), hence if \( 2g - 2 < \deg(G) < n \), then \( k = \deg(G) + 1 - g \). Another important parameter of a code is the minimal distance \( d \), which gives us an idea about the maximal number of errors which could be detected or corrected. In a linear code, the minimal distance is just the minimal weight, where the weight of a codeword here means the number of nonzero coordinates. Let \( \omega \) be a codeword in \( C_L(D, G) \) with weight exactly \( d \), which means that we can find \( n - d \) coordinates, \( i_1, i_2, \ldots, i_{n-d} \), such that \( \omega \) is zero at exactly these coordinates. Let \( f_\omega \) be the corresponding function in \( \mathcal{L}(G) \), then \( f_\omega \in \mathcal{L}(G - (P_{i_1} + P_{i_2} + \ldots + P_{i_{n-d}})) \), hence

\[
0 \leq \deg(G - (P_{i_1} + P_{i_2} + \ldots + P_{i_{n-d}})) = \deg(G) - n + d,
\]

hence \( d \geq n - \deg G \). We can see that this bound makes sense only when the degree of \( G \) is smaller than \( n \), so we always assume this afterwards.

As an easy example, if we take \( X \) to be \( \mathbb{F}_q(x) \) the rational function field (whose definition will be given in Definition 3.1.1), \( p_i \)'s to be \( n \) distinct rational places of \( \mathbb{F}_q(x) \), which means that \( p_i = (x - i) \) for \( i \in \mathbb{F}_q \cup \{\infty\} \), and take \( G \) to be a divisor whose support is disjoint from the set \( \{p_i\} \), such that \( 0 \leq \deg G \leq n - 1 \), then we get the following properties:

(i) \( n \leq q + 1 \) since the number of rational places of \( \mathbb{F}_q(x) \) is \( q + 1 \);

(ii) \( k = \deg(G) + 1 \);

(iii) \( d = n - \deg(G) \).
Moreover, since \(d + k = n + 1\), this code is a MDS code, which by definition means that it attains the maximal distance under the given code length and dimension.

One of the main purposes of studying codes is to find codes to achieve reliable and effective transmission of information, i.e. the information rate \(R(C) := k/n\) of a code \(C\) is close to 1. We can think of it like this: the length of the code \(n\) means the space we need to store a codeword, and the dimension \(k\) tells the length of the significant part, or in other words, the part which carries the information. To make the limited storage be used as much as possible, we want to get codes with redundancy as small as possible with respect to the total length \(n\). As we have discussed above, when the divisor \(G\) has degree between 0 and \(n - 1\), we have the dimension of the code being \(\text{deg}(G) + 1\), hence the information rate \(R(C) = (\text{deg}(G) + 1)/n\). But some problems come up from this, given \(n\) distinct rational places of a function field, the first problem is to determine whether divisors satisfying the degree condition always exist for any \(n\), and the second problem is to determine whether we can find a nontrivial lower bound of the limit of the information rate and whether we can construct a code to attain it or not. The first problem is answered by [13, Chapter 8, Lemma 8.4.5], stating that for any choice of \(n\) distinct rational places, for any \(r \geq 0\), there exists a divisor \(G\) of degree \(r\) such that none of the places chosen is in the support of \(G\). To answer the second question, we introduce some new notations to simplify our discussion of the asymptotic performance of codes. We define the relative minimum distance as \(\delta(C) := d/n\), and consider \(V_q := \{(\delta(C), R(C)) \in [0,1]^2 | C\text{ is a code over } \mathbb{F}_q\}\), denote by \(U_q\) the set of limit points of \(V_q\). According to [13, Chapter 8, Proposition 8.4.2], there always exists a continuous function \(\alpha_q : [0,1] \rightarrow [0,1]\) such that

\[
U_q = \{(\delta, R)|0 \leq \delta \leq 1 \text{ and } 0 \leq R \leq \alpha_q(\delta)\},
\]

and it satisfies that \(\alpha_q(0) = 1\), \(\alpha_q(\delta) = 0\) for all \(1 - q^{-1} \leq \delta \leq 1\), and \(\alpha_q\) is decreasing in the interval \([0,1 - q^{-1}]\). Thus we can safely say that \(\alpha_q(\delta)\) is a good bound of the information rate and we can analyze it instead of the information rate. Moreover, the \(q\)-ary entropy function \(H_q(x) : [0,1 - q^{-1}] \rightarrow \mathbb{R}\) is defined by \(H_q(0) = 0\) and for \(x \neq 0\),

\[
H_q(x) := x \log_q(q - 1) - x \log_q(x) - (1 - x) \log_q(1 - x).
\]

Then by some classical results from coding theory, we have a good lower bound for \(\alpha_q(\delta)\), namely the Gilbert-Varshamov bound, which says that for \(0 \leq \delta \leq 1 - q^{-1}\), we have \(\alpha_q(\delta) \geq 1 - H_q(\delta)\). It was considered as the best possible lower bound. But when the towers of function fields are taken into account for of the construction of algebraic geometry codes, it is shown in [13, Chapter 8, Proposition 8.4.6] that if Ihara’s constant of a tower \(A(q)\) for some \(q\) is larger than 1, then
1. Introduction

\( \alpha_q(\delta) \geq (1 - A(q)) - \delta. \) In particular, when we take \( q \) to be a square, then \( A(q) = \sqrt{q} - 1, \) hence \( \alpha_q(\delta) \geq (1 - 1/(\sqrt{q} - 1)) - \delta, \) which is the Tsfasman-Vlăduț-Zink bound. And it is really an improvement of Gilbert-Varshamov bound in some interval of \([0, 1]\), see Figure 1.1.

![Comparison of GV bound and TVZ bound](image)

Figure 1.1: A comparison of GV bound and TVZ bound when \( q = 64 \) (left) and \( q = 49 \) (right)

1.3 Sketch of this Thesis

In this thesis we will be mainly concerned with such sequences (towers) over finite fields which are given by explicit equations. These have been intensively studied by various authors, most notably Garcia and Stichtenoth. In fact, Garcia and Stichtenoth gave the first example of a tower of functions fields, which attained the Drinfeld-Vlăduț bound (see [4]). In these constructions, the same suitably chosen equation is iterated repeatedly, hence these towers are also called recursive towers. Because of this repeated nature, the towers obtained have strong symmetry and very interesting structures. It is extremely difficult to come up with equations, which give good towers when iterated. Hence various negative criteria have been found, that exploit in a disguised way this symmetry, and that help to exclude bad candidates. It is crucial to better understand these negative results and hopefully to come up with new necessary criteria for the iterated equation. The hope is to gain a better understanding of various results, among others [9], [2] and [6], and to come up with new necessary conditions. And, as was pointed out by Prof. Lenstra to me, a promising way to achieve this is by exploiting the symmetry involved (hence
using some group theory). This thesis is a first step towards this goal. We try to give a reinterpretation of various concepts from the domain of towers in terms of the groups that are involved, developing, in some sense, a dictionary to pass from one world to the other. So, in chapter 2, we start by introducing basic concepts from Infinite Galois theory, and then show the antiequivalence of two categories, $\pi$-SET and $K$-FEA. In Chapter 3, some definitions and properties of the function fields, the extensions of function fields, and the towers are introduced, while in Chapter 4, decomposition groups, inertia groups and higher ramification groups as well as their properties are introduced. Then last but not the least comes Chapter 5, where the link between these two are shown, which forms the heart of this thesis.
2. Infinite Galois Theory

In the finite Galois theory, there is a beautiful theorem stating that each subgroup of the Galois group of a finite Galois extension corresponds to an intermediate field. But when we look at infinite field extensions, this does not always hold. For an example to this, one can look at the extension $\mathbb{F}_q/\mathbb{F}_q$, which is an infinite Galois extension, with the Galois group being $\hat{\mathbb{Z}}$. As a subgroup of $\hat{\mathbb{Z}}$, $\mathbb{Z}$ also corresponds to $\mathbb{F}_q$, which violates the $1-1$ correspondence, and in the following, we will see that the reason for this is that $\mathbb{Z}$ is not closed in $\hat{\mathbb{Z}}$.

In order to recover a similar correspondence which is true for infinite Galois extensions, we introduce a topology, the Krull topology, to the Galois group. This allows us to establish a $1-1$ correspondence between the closed subgroups and the intermediate fields.

2.1 Galois Groups as Topological Groups

The Krull topology, named after Wolfgang Krull, provides us a nice view of the Galois groups. First we give the definition of a Galois extension.

Definition 2.1.1. Let $L$ be an algebraic field extension of a field $K$. Then we can define a subgroup of the group of automorphisms of $L$, say $G$, as follows. An automorphism $\sigma \in \text{Aut}(L)$ is in $G$ if the restriction of $\sigma$ to $K$ is the identity map. We call this extension Galois if $K$ is the fixed field of $G$, i.e. for any element $x$ in $L\setminus K$, there exists an automorphism $\sigma \in G$ such that $\sigma(x) \neq x$, and we call $G$ the Galois group of $L$ over $K$, with notation $\text{Gal}(L/K)$.

Then we give the definition of the Krull topology on the Galois groups.
**Definition 2.1.2.** Let a field $L$ be a Galois extension of a field $K$, with Galois group $G = \text{Gal}(L/K)$, and let $N$ be the set of subgroups of $G$ which are the Galois groups $\text{Gal}(L/M)$, where $M$ is a finite Galois subextension of $L$ over $K$, i.e. $K \subseteq M \subseteq L$, $[M : K]$ is finite, and $M$ is Galois over $K$. The Krull topology is defined as taking $N$ as a basis of the topology, i.e. a subset $X$ of $G$ is open if it is $\emptyset$, or a union of arbitrary many $\sigma N$ for some $\sigma$ in $G$ and $N$ in $N$.

Recall some definitions from topology, which are those of **Hausdorff**, **compact** and **totally disconnected**.

**Definition 2.1.3.** Let $X$ be a topological space.

(a) $X$ is **Hausdorff** if any two distinct points of $X$ can be separated by neighborhoods, i.e. for any two distinct points $x, y \in X$, there exist $U$ and $V$ which are nonempty open subsets of $X$ and $x \in U$, $y \in V$, such that $U \cap V = \emptyset$.

(b) $X$ is **compact** if for any open covering of $X$, i.e. a set of open sets $X := \{X_i\}_{i \in I}$ for an index set $I$ which may be infinite or even uncountable, and $\bigcup_{i \in I} X_i \supset X$, there always exists a finite subcovering $\{X_i\}_{i=1}^n \subset X$ for $n$ a positive integer.

(c) $X$ is **totally disconnected** if any nonempty subset of $X$ is disconnected.

**Proposition 2.1.4.** Under the Krull topology, $G = \text{Gal}(L/K)$, as a topological space, is Hausdorff, compact and totally disconnected.

**Proof.** To show that $G$ is totally disconnected, we need to show that any subset of $G$ is disconnected. Let $X$ be a subset of $G$ and $\sigma$ and $\tau$ be distinct elements in $X$. Let $\sigma N$ be an open neighborhood of $\sigma$ which does not contain $\tau$. The existence of this $N$ follows from that

$$\bigcap_{N \in N} N = \{\text{id}\}.$$  \hfill (2.1)

The proof to (2.1) is quite straightforward. Let $\tau \in \bigcap_{N \in N} N$ and let $a \in L$. Then let $E$ be the splitting field of the minimal polynomial of $a$ over $K$. Hence $E$ is finite Galois over $K$, and denote the Galois group $\text{Gal}(L/E)$ by $N'$, hence $N' \in N$. Since the automorphism $\tau$ is in $N'$, it fixes $E$, and in particular $\tau(a) = a$. Thus for any $a \in L$, $\tau$ maps $a$ to itself, hence $\tau = \text{id}$, which means that $\bigcap_{N \in N} N = \{\text{id}\}$, hence $\bigcap_{N \in N} \sigma N = \{\sigma\}$. Then we can write $X$ as

$$X = (\sigma N \cap X) \cup ((G - \sigma N) \cap X).$$
which is a union of two disjoint open subsets of $X$ with induced topology, and both sets are nonempty since $\sigma \in \sigma N \cap X$ and $\tau \in (G - \sigma N) \cap X$.

To show that $G$ is Hausdorff, we need to find disjoint open neighborhoods of $\sigma$ and $\tau$, which are distinct elements of $G$. As shown above, $\cap_{N \in \mathbb{N}} \sigma N = \{\sigma\}$, then we can find $N \in \mathbb{N}$ such that $\tau \notin \sigma N$. As we discussed above, $N$ is not only open but also closed. So $G - \sigma N$ is an open subset of $G$ and $\tau \in G - \sigma N$. Hence we have already found disjoint open neighborhoods of $\sigma$ and $\tau$, namely $\sigma N$ and $G - \sigma N$.

We need to do a bit more work to show that $G$ is compact. Consider the mapping:

$$h : G \rightarrow \prod_E \text{Gal}(E/K)$$

$$\sigma \mapsto \prod_E \sigma |_E,$$

where $E$ varies over all the finite Galois subextensions. Each $\text{Gal}(E/K)$, equipped with the discrete topology, can be viewed as a disconnected compact topological space, hence by Tychonoff’s theorem, the product of all $\text{Gal}(E/K)$’s is compact with respect to the product topology. On the other hand, the homomorphism $h$ is injective, since for any $\sigma$ and $\tau$ in $G$, $h(\sigma) = h(\tau)$ induces that $\sigma |_E = \tau |_E$ holds for any finite Galois subextension $E$. Any $a \in L$, it lies in a finite Galois subextension, say $E'$, hence we have that $\sigma(a) = \tau(a)$, and thus $\sigma = \tau$. The homomorphism $h$ is continuous, since the sets $U_{E'} = \prod_{E \neq E'} \text{Gal}(E/K) \times \{\tilde{\sigma}\}$, where $\tilde{\sigma} \in \text{Gal}(E'/K)$, form a subbasis of open sets of the product $\prod_E \text{Gal}(E/K)$, where $E'$ varies over the finite Galois subextensions. If $\sigma$ is a preimage of $\tilde{\sigma}$ under the map $G \rightarrow \text{Gal}(E'/K)$, then $h^{-1}(U) = \sigma \text{Gal}(L/E)$, which is open in $G$. Therefore, it suffices to show that $h(G)$ is closed in the compact set $\prod_E \text{Gal}(E/K)$. Let us consider the set $M_{E'/E} := \{\prod_E \sigma_F \in \text{Gal}(F/K) | \sigma_{E'} |_E = \sigma_E \}$, for each pair $E' \supseteq E$ of finite Galois subextensions. It is clear that $h(G) = \bigcap_{E',E} M_{E'/E}$. We can show that $M_{E'/E}$ is closed, since if $\text{Gal}(E/K) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, and $S_i$ is the set of the extensions of $\sigma_i$ to $E'$, then

$$M_{E'/E} = \bigcup_{i=1,2,\ldots,n} \left( \prod_{F \neq E',E} \text{Gal}(F/K) \times S_i \times \{\sigma_i\} \right).$$

We can easily see that a nonempty subgroup is open under the Krull topology if and only if it is closed and of finite index, i.e. there exist only finitely many pairwise disjoint cosets of the given subgroup. The proof of this just follows from the definition and the
compactness of the topological group $G$. If $H$ is a nonempty open subgroup of $G$, we can see that $\{\sigma H\}_{\sigma \in G}$ forms an open covering of $G$. By the compactness of $G$, there exists a finite subcovering, say $\{\sigma_i H\}_{i=1,2,\ldots,t}$, where $t < \infty$, $\sigma_1 = \text{id}$ and $\sigma_i \neq \sigma_j$ for $i \neq j$. Hence for any $i \neq j$, $\sigma_i H \cap \sigma_j H = \emptyset$. In particular, $\sigma_i H \cap H = \emptyset$ for any $i \neq 0$, so we have $H = G \setminus \bigcup_{i=0}^{t} \sigma_i H$. From this we conclude that $H$ is closed and $[G : H] = t$, which is finite. Conversely, if $H$ is closed and of finite index in $G$, say $[G : H] = t$, then we can find $\sigma_i$ for $i = 1,2,\ldots,t-1$, such that $G = \bigcup_{i=1}^{t} \sigma_i H$, where $\sigma_t = \text{id}$. As $t$ is finite, the union $\bigcup_{i=1}^{t} \sigma_i H \cup H$ is also closed, hence as its complement, $H$ is open.

It is easy to see that any $N \in \mathcal{N}$ is both open and closed.

*Remark* 2.1.5. As we can see, if $L$ is a finite Galois extension of $K$, any subgroup of $\text{Gal}(L/K)$ is open, since the Krull topology on $\text{Gal}(L/K)$ is just the discrete topology.

### 2.2 The Fundamental Theorem of Infinite Galois Theory

Suppose that $K$ is a field. We can define the algebraic closure of $K$, denoted as $\bar{K}$. The existence of the algebraic closure for an arbitrary field is shown by Zorn’s lemma, and the algebraic closure of a field is unique up to isomorphism which fixes the base field $K$. Suppose we have fixed $\bar{K}$ and an embedding of $K$ into $\bar{K}$, then we can define the separable closure of $K$ as a subfield of $\bar{K}$:

$$K_s = \{\alpha \in \bar{K}| \alpha \text{ is separable over } K\}.$$  

Note that sometimes, the separable closure of $K$ is also denoted as $K^{sep}$. It is unique up to isomorphism. In most situations, the separable closure of a field $K$ is strictly contained in the algebraic closure, but if $K$ is a perfect field, then the separable closure is the same as the algebraic closure.

*Claim:* If $K$ is a field, for any separable closure $K_s$ of $K$, we have that $K_s/K$ is Galois.

*Proof.* We only need to show that $K_s^{\text{Aut}_{K}(K_s)} = K$. The $\supseteq$ part is trivial. So we only need to show that $K_s^{\text{Aut}_{K}(K_s)} \subseteq K$. Let $x$ be an element of $K_s \setminus K$, then as $K_s$ is separable over $K$, there exists an irreducible separable polynomial $f(t)$ in $K[t]$ which is the minimal
2.2. The Fundamental Theorem of Infinite Galois Theory

polynomial of $x$ over $K$. Let $L$ be the splitting field of $f(t)$, hence it is Galois, hence there exists some $\sigma'$ in $\text{Gal}(L/K)$ which maps $x$ to some other element in $L$. We can extend $\sigma'$ to an automorphism of the field $K_s$, say $\sigma$, then we obtain an element which is identity when restricted on $K$, while it maps $x$ to some element other than $x$. Hence $x$ does not lie in $K_{\text{Aut}_K(K_s)}$, thus $K_{\text{Aut}_K(K_s)} \subseteq K$ and we are done. \hfill \Box

We call the Galois group of $K_s/K$ the absolute Galois group of $K$, denoted by $\pi$, which is also known as the étale fundamental group of $K$. Then we can define $\pi$-sets as follows: a $\pi$-set is a finite set $X$ equipped with a $\pi$-action on $X$, i.e. id · $x$ = $x$ for any $x$ in $X$, and $(\sigma\tau) \cdot x = \sigma \cdot (\tau \cdot x)$ holds for any $\sigma$ and $\tau \in \pi$, and the action of $\pi$ is continuous, in the sense that the map $\pi \times X \to X$ is continuous when $X$ is equipped with the discrete topology, $\pi$ is equipped with the Krull topology, and $\pi \times X$ is equipped with the product topology. We can define a category $\pi$-SET with the objects being the $\pi$-sets and the morphisms between $X$ and $X'$ defined as $f$ is a map from $X$ to $X'$ satisfying $f(\sigma \cdot x) = \sigma \cdot f(x)$ for any $\sigma \in \pi$ and $x \in X$. Denote the set of morphisms from a $\pi$-set $X$ to $X'$ by $\text{Mor}_{\pi\text{-SET}}(X,X')$.

The category $K\text{-FEA}$ of the finite étale $K$-algebras defined as follows.

**Definition 2.2.1.** We call $E$ a finite étale $K$-algebra if the following conditions are satisfied:

(a) $E$ is a commutative ring with 1;

(b) we can write $E$ as a direct product of $L_1, L_2, \ldots, L_t$, where $t$ is a nonnegative integer and each $L_i$ is a finite separable field extension of $K$.

The category is defined with the objects being finite étale $K$-algebras and the morphisms being the natural $K$-algebra homomorphisms. Similar as above, the set of morphisms from $E$ to $E'$ is denoted by $\text{Mor}_{K\text{-FEA}}(E,E')$.

We are going to prove that these two categories are anti-equivalent. Consider the following functors: $S$ and $M$. The functor $S$ sends a finite étale $K$-algebra $E$ to the set $S(E) := \text{Hom}(E, K_s)$, where the homomorphisms are defined between $K$-algebras, and we define the action of $\pi$ on $S(E)$ as $\sigma \cdot g := \sigma \circ g$ for any $\sigma \in \pi$ and $g \in S(E)$. It maps a morphism $g$ in $\text{Mor}_{K\text{-FEA}}(E_1, E_2)$ to $S(g)$ such that $S(g)(f) := f \circ g$ for any $f \in \text{Hom}(E_2, K_s)$.

On the other hand, the functor $M$ sends a $\pi$-set $X$ to the set $M(X)$ which is defined to be the set of $\pi$-respecting maps from $X$ to $K_s$, i.e. $M(X) = \{ f : X \to K_s | \sigma \cdot f(x) = \}$
2. Infinite Galois Theory

\[ f(\sigma \cdot x), \forall \sigma \in \pi, x \in X \} \]. It maps a morphism \( h \) in \( \text{Mor}_{\pi-\text{SET}}(X_1, X_2) \) to \( \mathbb{M}(h) \) such that \( \mathbb{M}(h)(f) := f \circ h \) for any \( f \in \mathbb{M}(X_2) \).

The very first question that arises is whether these two functors are well-defined as functors between these two categories.

Let us look at \( S \) first. Let \( E \) be a finite étale \( K \)-algebra, then by definition, it can be written as a finite product of finite extension fields of \( K \), say \( E = \prod_{i=1}^{t}L_i \), hence the set of \( K \)-algebra homomorphisms from \( E \) to \( K_s \) is the product of \( \text{Hom}(L_i, K_s) \) for \( i = 1, 2, \cdots, t \), and for each \( i \), since \( L_i \) is a finite separable extension of \( K \), it can be viewed as \( K[t]/(f_i(t)) \) for some irreducible polynomial \( f_i \), where \( f_i \) is chosen as the minimal polynomial of a primitive element for \( L_i \) over \( K \). Hence the set of \( K \)-homomorphisms from \( L_i \) to \( K_s \), which are defined as the embeddings of \( L_i \) into \( K_s \) which are identity when restricted to \( K \), is isomorphic to the set of the roots of \( f_i \) in \( K_s \). Recall that the action of \( \pi \) on this set is defined as: \( \sigma \cdot f(x) = \sigma(f(x)) \), for any \( \sigma \in \pi \), \( f \in \text{Hom}(L_i, K_s) \), and \( x \in L_i \). So the set \( S(X) \) is isomorphic to the disjoint union of sets of zeros of \( f_i \)'s where \( f_i \) is the minimal polynomial of a primitive element of \( L_i \) over \( K \), as argued before. Thus it is finite, and the action of \( \pi \) on \( S(X) \) can be canonically defined as left composition. So the functor \( S \) does send finite étale \( k \)-algebras to \( \pi \)-sets. What about the morphisms? To see this, we prove that for an \( g \in \text{Mor}_{K-\text{FEA}}(E_1, E_2) \), \( \phi := S(g) \) is indeed in \( \text{Mor}_{\pi-\text{SET}}(S(E_2), S(E_1)) \). To be precise, for a \( K \)-algebra homomorphism, say \( g \), from \( E_1 \) to \( E_2 \), we want to show that for any \( f \in S(E_2) = \text{Hom}(E_2, K_s) \), \( \sigma \in \pi \), we have \( \phi(f) \in S(E_1) = \text{Hom}(E_1, K_s) \), satisfying \( \phi(\sigma \cdot f) = \sigma \cdot (\phi(f)) \). Moreover, as we discussed above, we reduce the problem to when both \( E_1 \) and \( E_2 \) are fields. To show that \( \phi(f) = f \circ g \in \text{Hom}(E_1, K_s) \), for any \( x_1, x_2 \in E_1 \), \( a \in K_s \), we need to check:

- for the scalar multiplication:
  \[ (\phi(f))(ax_1) = f(g(ax_1)) = f(ag(x_1)) \] (since \( g \) is a \( k \)-algebra homomorphism from \( E_1 \) to \( E_2 \))
  \[ = af(g(x_1)) \] (since \( f \) is a \( k \)-algebra homomorphism from \( E_2 \) to \( K_s \))
  \[ = a(\phi(f))(x_1); \]

- for the sum of two elements in \( E_1 \):
  \[ (\phi(f))(x_1 + x_2) = f(g(x_1 + x_2)) = f(g(x_1) + f(x_2)) = f(g(x_1)) + f(g(x_2)) = (\phi(f))(x_1) + (\phi(f))(x_2); \]
2.2. The Fundamental Theorem of Infinite Galois Theory

- for the product of two elements in \( E_1 \):
  
  \[
  (\phi(f))(x_1x_2) = f(g(x_1x_2)) \\
  = f(g(x_1)g(x_2)) = f(g(x_1))f(g(x_2)) \\
  = (\phi(f))(x_1)(\phi(f))(x_2).
  \]

For any \( \sigma \in \pi \), and any \( x \in E_1 \), then

\[
(\phi(\sigma \cdot g))(x) = (\sigma \cdot g)(f(x)) \\
= \sigma(g(f(x))) = \sigma((\phi(g))(x)) \\
= \sigma \cdot (\phi(g))(x),
\]

since \( \pi \) acts on \( \text{Hom}(E_1, K_s) \) by left composition.

Then let us look at \( \mathbb{M} \). Let \( X \) be a \( \pi \)-set, then we can decompose \( X \) as the disjoint union of its \( \pi \)-orbits, say \( X_1, X_2 \cdots X_i \), hence \( \mathbb{M}(X) = \prod_{i=1}^{\infty} \mathbb{M}(X_i) \). We prove that for each \( i \), \( \mathbb{M}(X_i) \) is a finite extension field of \( K \). Let \( f_a \) be the constant function from \( X_i \) to \( K \), mapping every element in \( X_i \) to \( a \), for \( a \in K \). For any \( \sigma \in \pi = \text{Gal}(K_s/K) \), \( a \) lies in the fixed field of \( \pi \), so \( \sigma(f_a(x)) = \sigma(a) = a = f_a(\sigma \cdot x) \) for any \( x \in X_i \) since \( X_i \) is a \( \pi \)-orbit. So \( K \) can be embedded into \( \mathbb{M}(X_i) \). Let \( d_i \) be the cardinality of \( X_i \) which is finite since the \( \pi \)-sets are defined to be finite, and let \( h_i(x) \) be an irreducible separable polynomial in \( K[x] \) of degree \( d_i \), then we can show that \( \mathbb{M}(X_i) \) is isomorphic to the field \( K[x]/(h_i(x)) \), since \( X_i \) is transitive, which means that for any \( x \) and \( y \) in \( X_i \), we can find a \( \sigma \in \pi \) such that \( y = \sigma \cdot x \), hence to define a map \( f : X_i \to K_s \), we can choose \( f(x) \) freely, then define \( f(y) \) as \( \sigma(f(x)) \) where \( \sigma \) is chosen as above. Since \( X_i \) has the same size as the set of all the roots to \( h_i(x) \in K_s \), \( \mathbb{M}(X_i) \) is isomorphic to \( K[x]/(h_i(x)) \), hence a finite extension field of \( K \). Therefore \( \mathbb{M}(X) \) is a product of finitely many finite extension fields over \( K \). So the functor \( \mathbb{M} \) does send \( \pi \)-sets to \emph{finite étale} \( K \)-algebras. Then what about the morphisms? That is, we want to prove that for an \( h \in \text{Mor}_{\pi-\text{SET}}(X_1, X_2) \), \( \varphi := \mathbb{M}(h) \) is indeed in \( \text{Mor}_{K-\text{FÉA}}(\mathbb{M}(X_2), \mathbb{M}(X_1)) \). To be precise, \( h \) is a morphism from \( X_1 \) to \( X_2 \), satisfying \( h(\sigma \cdot x) = \sigma \cdot h(x) \) for any \( \sigma \in \pi, x \in X \), and we need to show that \( \varphi \) is a \( K \)-algebra homomorphism from \( \mathbb{M}(X_2) \) to \( \mathbb{M}(X_1) \). As shown above, we can reduce the problem to the case that \( X_1 \) and \( X_2 \) are transitive \( \pi \)-sets, then both \( \mathbb{M}(X_1) \) and \( \mathbb{M}(X_2) \) are finite extension fields over \( K \). Firstly, \( \varphi(f) \in \mathbb{M}(X_1) \) for any \( f \in \mathbb{M}(X_2) \), i.e. \( \varphi(f) \) is a \( \pi \)-respecting map from \( X_1 \) to \( K_s \). This is easy to see since for any \( \sigma \in \pi \) and \( x \in X_1 \),

\[
(\varphi(f))(\sigma \cdot x) = f(h(\sigma \cdot x)) = f(\sigma \cdot h(x)) = f(\sigma \cdot f(h(x))) = \sigma \cdot \varphi(f)(x),
\]
since $f$ and $h$ are both $\pi$-respecting maps. Secondly, for any $f_1, f_2 \in M(X_2)$, $a \in K_s$, we have:

- for the scalar multiplication:
  \[
  (\varphi(a f_1))(x) = (a f_1)(f(x)) = a(f_1(h(x))) = a(\varphi(f_1))(x);
  \]

- for the sum of two elements,
  \[
  (\varphi(f_1 + f_2))(x) = (f_1 + f_2)(h(x)) = f_1(h(x)) + f_2(h(x)) = (\text{var}(f_1))(x) + (\varphi(f_2))(x) = ((\varphi(f_1)) + (\varphi(f_2)))(x);
  \]

- for the multiplication of two elements,
  \[
  (\varphi(f_1 f_2))(x) = (f_1 f_2)(h(x)) = f_1(h(x)) f_2(h(x)) = \varphi(f_1)(x) \varphi(f_2)(x) = (\varphi(f_1)\varphi(fg_2))(x).
  \]

so $\varphi$ is a $K$-algebra homomorphism from $M(X_2)$ to $M(X_1)$.

Thus, we have two functors and there are canonical isomorphisms such that
\[
E \cong M(\mathcal{S}(E)) \\
X \cong \mathcal{S}(M(X)).
\]

The following are a few remarks before the end of this section.

**Remark 2.2.2.** Suppose $E$ is a finite Galois field extension over $K$. Since $\mathcal{S}(E)$ is isomorphic to the $\pi$-set $\pi/\rho$ where $\rho$ is the Galois group of the extension $K_s/E$, then $\mathcal{S}(E)$ is isomorphic to the Galois group $\text{Gal}(E/K)$.

**Remark 2.2.3.** If the action of $\pi$ on $X$ is transitive, then $X$ is isomorphic to the $\pi$-set $\pi/\rho$, where $\rho$ is the stabilizer of some $x \in X$. The action of $\pi$ on $X$ is continuous, hence $\rho$ is open and $M(X)$ is a finite field extension over $K$. If moreover, $\rho$ is normal in $\pi$, then $M(X)/K$ is Galois.

**Remark 2.2.4.** In the fundamental theorem of Galois theory for finite extensions, there is a 1-1 correspondence between the subfields containing the base field and the subgroups of the
2.2. The Fundamental Theorem of Infinite Galois Theory

Galois group, but in the infinite case, the 1-1 correspondence is between the subextensions and the closed subgroups of the Galois group. This was shown by Krull, but for a proof to it, see [14, Chapter 1, Theorem 1.3.11]. As in Remark 2.1.5, in the finite case, any subgroup of $G$ is a closed subgroup of $G$, so in this case, we recover the fundamental theorem of Galois theory for finite extension.

Remark 2.2.5. Moreover, there is something more in the fundamental theorem than the 1-1 correspondence, which says that for a finite extension $L/K$, a sub-extension $M/K$ is Galois if and only if the corresponding subgroup $H$ of the Galois group $G$ is a normal subgroup of $G$. In the infinite case, $M/K$ is finite Galois if and only if the corresponding $\rho$, where $S(M)$ is isomorphic to $\pi/\rho$, is an open normal subgroup of $\pi$. Thus we can safely say that this is the general case of the fundamental theorem of Galois theory.
3. Function Fields and Towers of Function Fields

We introduce some notations, definitions and some properties which are important and used throughout the thesis.

3.1 Algebraic Function Fields

In this section, we will introduce the algebraic function field, and its place.

Definition 3.1.1. Given a field \( k \), an algebraic function field \( K \) over \( k \) of one variable is an extension field of \( k \) such that \( K \) is a finite algebraic extension of \( k(x) \) with \( x \) transcendental over \( k \). And \( K \) is called a rational function field if \( K \) can be written as \( k(x) \) for some \( x \) transcendental over \( k \).

In this case, \( k \) is called the constant field of \( K \), and in particular, if \( k \) is algebraically closed in \( K \), then it is called the full constant field or exact constant field.

Definition 3.1.2. Given a function field \( K/k \), with \( k \) its full constant field, one can construct a smooth absolutely irreducible projective curve \( C \) over \( k \) such that \( K \) is the function field of \( C \). The genus of \( K \) is defined as the genus of \( C \), and we denote it as \( g(K) \).

Note that this is well-defined since the curve mentioned in the definition is unique up to birational equivalence, hence the genus is uniquely determined. There are other definitions of the genus, which can be found in [13] or [8]. As a special case, observe that \( k(x) \) is the function field of the projective line, hence \( g(k(x)) \) is 0, then the genus of a rational function field is always 0.
Definition 3.1.3. A place $p$ of the function field $K/k$ is the maximal ideal of some discrete valuation ring $\mathcal{O}$ of $K/k$. Since the valuation ring is determined uniquely by the place $p$, it can also be denoted by $\mathcal{O}_{p,K}$, and the valuation corresponding to $\mathcal{O}_{p,K}$ is denoted by $v_p$. We denote the set of all places of $K$ by $\mathbb{P}_K$.

Note that it is easy to show (proof can be found in [1]) that $p$ is the only maximal ideal of $\mathcal{O}_{p,K}$, and it is a principal ideal, then there exists a $t \in \mathcal{O}_{p,K}$ such that $p = t\mathcal{O}_{p,K}$, and we call any element $t$ satisfying this a local parameter. Sometimes we also call a place of $K$ a prime.

Definition 3.1.4. Since $p$ is the maximal ideal of $\mathcal{O}_{p,K}$, the ring $\kappa_p = \mathcal{O}_{p,K}/p$ is a field. The field $\kappa_p$ is called the residue class field. Also, we can define the degree of $p$ as

$$\deg p = [\kappa_p : k].$$

And in particular, a place is called rational if it is of degree 1.

Note that $\kappa_p$ is a finite extension of $k$. To see this, observe the map from $k$ to $\kappa_p$, sending $a$ to $a + p$. This is an embedding of $k$ into $\kappa_p$ since the kernel is trivial, otherwise, there exists $a, b \in k$ such that $a - b \in p$, which contradicts to the fact that both $a$ and $b$ are units of $\mathcal{O}_{p,K}$.

The degree of a place is always finite. And we denote the cardinality of set of places of degree $r$ as $N_r(K)$.

### 3.2 The Extensions of Function Fields

In this section, we will give some properties of extensions of function fields.

First we define what an algebraic extension of function fields is.

Definition 3.2.1. An algebraic function field $L/l$ is called an algebraic extension of $K/k$ if $L \supseteq K$ is an algebraic field extension and $l \supseteq k$. A place $q \in \mathbb{P}_L$ is said to lie over $p \in \mathbb{P}_K$ if $p \subseteq q$, denoted by $q|p$.

Note that it is shown in [13, Chapter 3, Proposition 3.1.7] that any place $p$ has at least one but only finitely many places lying over the same place.
Proposition 3.2.2. Let $L/K$ be an algebraic extension of function fields. Let $p$ be a place of $K$ and $q$ be a place of $L$. Let $\mathcal{O}_{p,K}$ and $\mathcal{O}_{q,L}$ denote the valuation rings corresponding to $p$ and $q$, respectively. Then the following are equivalent:

1. $q|p$;
2. $\mathcal{O}_{q,L} \supseteq \mathcal{O}_{p,K}$;
3. there exists an integer $e \geq 1$ such that

\[ v_q(x) = e \cdot v_p(x) \]

for all $x \in K$.

Moreover, if $q$ lies over $p$, then $p$ is the intersection of $q$ and $K$, and $\mathcal{O}_{p,K}$ is the intersection of $\mathcal{O}_{q,L}$ and $K$. In this case, we also call $p$ the restriction of $q$ to $K$, or $q$ an extension of $p$ to $L$.

For a proof to this proposition refer to [13, Chapter 3, Proposition 3.1.4].

Now we can define the ramification index and the inertia degree of an extension of a place.

Definition 3.2.3. Let $L/K$ be an algebraic extension of function fields. Let $q$ be a place of $L$ lying over $p$, which is a place of $K$. We define the ramification index and inertia degree as follows:

(a) the ramification index is defined as:

\[ e(q|p) = e \text{ for which } v_q(x) = e \cdot v_p(x) \text{ for all } x \in K; \]

(b) the inertia degree is defined as:

\[ f(q|p) = [\kappa_q : \kappa_p]. \]

Note that the existence of the ramification index is shown by Proposition 3.2.2, and the inertia degree is just $\deg q$ divided by $\deg p$ if both function fields have the same constant field (if not, then it is just $[l : k] \deg q / \deg p$). For any element $a$ in $K$, we have that $v_q(a) = e(q|p)v_p(a)$. 


3. Function Fields and Towers of Function Fields

**Definition 3.2.4.** Let $p$ be a place of $K$ and $q$ be a place $L$, where $L/K$ is an algebraic extension and $q$ lies over $p$. Let $\mathcal{O}_{p,K}'$ be the integral closure of $\mathcal{O}_{p,K}$ in $L$. Then we can define the complementary module as $C_p = \{z \in L | \text{Tr}_{L/K}(z \cdot \mathcal{O}_{p,K}') \subseteq \mathcal{O}_{p,K}\}$.

It is shown in [13, Chapter 3, Proposition 3.4.2] that

1. $C_p$ is trivial for almost all $p$;
2. there is an element $t \in L$ which depends on $p$ such that $C_p = t \cdot \mathcal{O}_{p,K}'$, moreover, $v_q(t) \leq 0$ for all $q | p$ where $q$ is a place of $L$ lying over $p$;
3. for $t' \in L$, $C_p = t' \cdot \mathcal{O}_{p,K}'$ if and only if $v_q(t') = v_p(t)$ for all $q | p$ where $q$ is a place of $L$ lying over $p$.

**Definition 3.2.5.** Let $L/K$ be an algebraic extension of function fields, and $p$ (resp. $q$) be a place of $K$ (resp. $L$), such that $q | p$. The different exponent $d(q | p)$ is defined as

$$d(q | p) = -v_q(t),$$

with $t$ satisfying $C_p = t \cdot \mathcal{O}_{p,K}'$ as above.

The different of this extension is defined as:

$$\mathcal{D}_{L/K} = \sum_{p \in \mathcal{P}_K} \sum_{q | p} d(q | p) \cdot q.$$

Note that the properties of the complementary module guarantee that the different exponent is well-defined and that it is always non-negative.

Back to algebraic geometry, a divisor is defined as a formal sum of subvarieties of codimension 1. We call a divisor effective if the "coefficients" are all nonnegative. So when we treat the function field as a variety, the places are the subvarieties of codimension one. Since $C_p$ is trivial for almost all $p$, the different exponent is zero for almost all $p$ and $q | p$, hence the different is a formal sum of places, hence a well-defined divisor of $L$. Moreover, the different exponent is defined to be nonnegative, hence the different is an effective divisor.

**Remark 3.2.6.** Let $L/K$ be an algebraic extension of function fields. Suppose that $p$ is a place of $K$ and $q$ is a place of $L$ lying over $p$. Then we can have completions of $K$ and $L$ with respect to $p$ and $q$, respectively. A good result is that the ramification index $e(q | p)$,
the inertia degree \( f(q|p) \), and the different exponent \( d(q|p) \) are invariant. Hence we can look at the completions of function fields which are local fields and are easier to be dealt with in some sense.

Then we give the fundamental equation of extensions of function fields.

**Theorem 3.2.7.** Let \( L/K \) be an algebraic extension of function fields, and \( n = [L : K] \). Let \( p \) be a place of \( K \), and \( q_1, q_2, \ldots, q_r \) be the places of \( L \) which lie over \( p \). Denote \( e_i = e(q_i|p) \) and \( f_i = f(q_i|p) \). Then we have:

\[
\sum_{i=1}^{r} e_if_i = n.
\]

**Definition 3.2.8.** Let \( L/K \) be an algebraic extension of function fields, with extension degree \( n = [L : K] \). Suppose \( p \) is a place of \( K \) and \( q \) a place of \( L \), satisfying \( q|p \).

(a) A place \( p \) is said to be **unramified** if for any place \( q \) lying over \( p \), we have \( e(q|p) = 1 \); it is called **ramified** otherwise.

(b) A place \( p \) is said to be **splitting completely** if there are exactly \( n \) places of \( L \) lying over \( p \). By the fundamental equation, it splits completely if and only if \( e(q|p) = f(q|p) = 1 \).

(c) A place \( p \) is **totally ramified** if \( e(q|p) = n \). By the fundamental equation, it is clear that when a place \( p \) is totally ramified, there is only one place lying over \( p \) and \( f(p|q) = 1 \).

(d) If a place \( p \) is ramified, then it is said to be **tamely ramified** if for any place \( q \) lying over \( p \), the ramification index \( e(q|p) \) is not divisible by the characteristic of \( K \); it is called **wildly ramified** otherwise.

(e) An algebraic extension \( L/K \) of function fields is called **unramified** if all the places of \( K \) are unramified in the extension; the extension is called **ramified** otherwise.

(f) If an algebraic extension \( L/K \) is ramified, then it is called **tamely ramified** if all places of \( K \) are unramified or tamely ramified in the extension; it is called **wildly ramified** otherwise.

We denote the set of places of \( K \) which is ramified in the extension \( L/K \) by \( \text{Ram}(L/K) \). Note that according to the fundamental equation, a place \( p \) splits completely if and only \( e(q|p) = f(q|p) = 1 \) for all \( q \) lying over \( p \), and it is totally ramified if and only if \( e(q|p) = n \), which induces \( f(q|p) = 1 \).
Remark 3.2.9. If $L/l$ is a constant field extension of $K/k$, i.e. $L = Kl$, then the extension is unramified, by [13, Chapter 3, Theorem 3.6.3].

In the following, there are some properties of the ramification index, inertia degree and the different exponent.

Proposition 3.2.10. Let $M/L/K$ be algebraic extensions of function fields over $k$. Let $p$ be a place of $K$, $t$ be a place of $M$ lying over $p$, and $q$ be a place of $L$ which is the restriction of $t$ to $L$, hence $q$ also lies over $p$, as in the following diagram.

\[
\begin{array}{ccc}
M & \rightarrow & t \\
\downarrow & & \downarrow \\
L & \rightarrow & q \\
\downarrow & & \downarrow \\
K & \rightarrow & p
\end{array}
\]

There are a few properties of the ramification index, the inertia degree and the different exponent:

(1) the transitivity of the ramification index:

\[
e(t|p) = e(t|q) \cdot e(q|p);
\]

(2) the transitivity of the inertia degree:

\[
f(t|p) = f(t|q) \cdot f(q|p);
\]

(3) the transitivity of the different exponent:

\[
d(t|p) = e(t|q) \cdot d(q|p) + d(t|q).
\]

Moreover, in the particular case that the extension $L/K$ is Galois, then we have some beautiful results for ramification index and inertia degree.

Proposition 3.2.11. Let $L/K$ be a Galois extension of function fields over $k$. Let $p$ be a place of $K$, and $q_1, \ldots, q_r$ be all the places lying over $p$. 
Then we have

\[ e(q_1|p) = e(q_2|p) = \ldots = e(q_r|p), \]
\[ f(q_1|p) = f(q_2|p) = \ldots = f(q_r|p), \]
\[ d(q_1|p) = d(q_2|p) = \ldots = d(q_r|p). \]

In this case, the ramification index, the inertia degree and the different exponent only depend on the place \( p \), so we denote them by \( e_p \), \( f_p \) and \( d_p \), respectively.

Moreover, the fundamental equation becomes

\[ n = [L : K] = r \cdot e_p \cdot f_p. \]

This is just a consequence of the fact that if the extension \( L/K \) is Galois with Galois group \( G \), then the set of extensions of a fixed place of \( K \) is transitive under the action of \( G \), where the action of \( G \) on the places is defined as applying the automorphism of \( L \) to the places as subrings of \( L \).

In particular, if the extension is of prime degree, then we can conclude that a place in \( K \) can only split completely (which means that \( e_p = f_p = 1 \) and \( r = n \)), be totally ramified (which means that \( e_p = n \) and \( f_p = r = 1 \)), or be unramified to exactly one place of degree \( n \).

There is also a theorem called "Abhyankar’s Lemma" which helps to determine the ramification index for the compositum of function fields.

**Theorem 3.2.12. (Abhyankar’s Lemma)** Let \( L/K \) be a finite separable extension of function fields. Suppose that \( L = L_1 L_2 \) is the compositum of two intermediate fields. Let \( p \) and \( q \) be places of \( K \) and \( L \), respectively, such that \( q \) lies over \( p \). Denote \( q_i \) be the restriction
of $q$ to $L_i$ for $i = 1, 2$.

If at least one of the extensions $q_1|p$ and $q_2|p$ is tame, then

$$e(q|p) = \text{lcm}\{e(q_1|p), e(q_2|p)\}.$$ 

The following is an important theorem stating the relation between the ramification index and the different exponent, which is called the "Dedekind’s Different Theorem".

**Theorem 3.2.13.** (Dedekind’s Different Theorem) We use the notations defined as above, then

$$d(q|p) \geq e(q|p) - 1$$

where the equality holds if and only if $e(q|p)$ is coprime to the characteristic of the constant field $k$.

When $q|p$ is unramified, the ramification index is 1, hence is always coprime to the characteristic of the constant field, hence the different exponent for an unramified place is always 0. Also by the definition of tame ramification, the equality holds if and only if the extension of place is either unramified or tamely ramified.

**Remark 3.2.14.** In the particular case that the extension $L/K$ is Galois of degree $\text{Char}(k)$ with $k$ the constant field, it can be shown that the different exponent should always be $d_p = c_p \cdot (e_p - 1)$ with $c_p$ a positive integer. We call $p$ weakly ramified if $c_p = 2$.

The Hurwitz formula, which will be given below, is a useful formula to compute the genus of an algebraic extension of a function field.

**Proposition 3.2.15.** Let $L/l$ be a separable algebraic extension of $K/k$. Then we can compute the genus of $L$ as follows:

$$2(g(L) - 1) = \frac{[L : K]}{[l : k]} \cdot 2(g(K) - 1) + \deg \mathcal{O}_{L/K}.$$
3.2. The Extensions of Function Fields

Remark 3.2.16. We can write the formula explicitly as follows:

\[
2(g(L) - 1) = \frac{[L : K]}{[l : k]} 2(g(K) - 1) + \deg \mathcal{D}_{L/K}
\]

\[
= \frac{[L : K]}{[l : k]} 2(g(K) - 1) + \sum_{p \in \mathcal{P}_K} \sum_{q \mid p} d(q \mid p) \deg q
\]

since the different exponent \(d(q \mid p)\) is zero for a place \(p\) which is unramified.

Moreover, by Theorem 3.2.13, we can conclude that

\[
2(g(L) - 1) \geq \frac{[L : K]}{[l : k]} 2(g(K) - 1) + \sum_{p \in \text{Ram}(L/K)} \sum_{q \mid p} (e(q \mid p) - 1) \deg q,
\]

and the equality holds if and only if all the ramified places of \(K\) are all tame, i.e. the extension \(L/K\) is tamely ramified.

Remark 3.2.17. There are several special cases which will be useful in the following chapters.

(i) when both function fields have the same exact constant field, i.e. we have \(l = k\), then

\[
g(L) = 1 + \frac{[L : K]}{[l : k]} (g(K) - 1) + \frac{1}{2} \sum_{p \in \text{Ram}(L/K)} \sum_{q \mid p} d(q \mid p) \deg q;
\]

(ii) when \(K\) is a rational function field, then we have \(g(K) = 0\), hence

\[
g(L) = 1 - 2 \frac{[L : K]}{[l : k]} + \frac{1}{2} \sum_{p \in \text{Ram}(L/K)} \sum_{q \mid p} d(q \mid p) \deg q.
\]

At the end of this section, we introduce two special kinds of extensions, which will be important for the towers.

Proposition 3.2.18. (Kummer Extensions) Let \(K/k\) be an algebraic function field with \(k\) as full constant field of characteristic \(p\). Assume that \(k\) contains a primitive \(n\)-th root of unity, where \(n > 1\) and \(n\) is not divisible by \(p\). Suppose that \(u \in K\) is an element satisfying \(u \neq w^d\) for all \(w \in K\) and all \(d > 1\) dividing \(n\). Let \(L = K(y)\) with \(y\) satisfying \(y^n = u\). Such an extension \(L/K\) is called a Kummer extension. And we have:

(1) the polynomial \(f(T) = T^n - u\) is the minimal polynomial of \(y\) over \(K\);
3. Function Fields and Towers of Function Fields

(2) the extension \( L/K \) is cyclic Galois of degree \( n \). The elements of \( \text{Gal}(L/K) \) acts as \( y \mapsto \zeta y \), where \( \zeta \in k \) is a primitive \( n \)-th root of unity;

(3) let \( p \in \mathbb{P}_K \) and \( q \in \mathbb{P}_L \) which lies over \( p \). Then we have the ramification index and different exponent as

\[
e(q|p) = \frac{n}{r_p} \quad \text{and} \quad d(q|p) = \frac{n}{r_p} - 1,
\]

where \( r_p := \gcd(n, v_p(u)) > 0 \).

(4) if \( k \) is algebraically closed in \( L \), then the genus of \( L \) is:

\[
g(L) = 1 + n(g(K) - 1 + \frac{1}{2} \sum_{p \in \mathbb{P}_K} (1 - \frac{r_p}{n}) \cdot \deg p).
\]

Note that from Galois theory, every cyclic field extension \( L/K \) of degree \( n \) is a Kummer extension, provided that \( n \) is not divisible by the characteristic of \( K \) and \( K \) contains all \( n \)-th roots of unity.

**Proposition 3.2.19.** (Artin-Schreier Extensions) Let \( K/k \) be a function field of characteristic \( p > 0 \) with \( k \) as its full constant field. Suppose that \( u \in K \) is an element which satisfies that \( u \neq \omega^p + \omega \) for all \( \omega \in K \). Let \( L = K(y) \) with \( y \) satisfying \( y^p + y = u \). Such a extension \( L/K \) is called an Artin-Schreier extension. For \( p \in \mathbb{P}_K \), we can define the integer \( m_p \) as

\[
m_p := \begin{cases} 
  m & \text{if there is an element } z \in K \text{ satisfying that } v_p(u - z^p - z) = -m < 0 \text{ and } m \text{ is not divisible by } p; \\
  -1 & \text{otherwise.}
\end{cases}
\]

Then we have:

(a) the extension \( L/K \) is cyclic Galois of degree \( p \). The elements of \( \text{Gal}(L/K) \) acts as \( y \mapsto y + \nu \) with \( \nu = 0, 1, \ldots, p - 1 \);

(b) a place \( p \) is unramified in \( L/K \) if and only if \( m_p = -1 \);

(c) a place \( p \) is totally ramified in \( L/K \) if and only if \( m_p > 0 \). Denote the place lying over \( p \) by \( q \), then the different exponent is give by \( d(q|p) = (m_p + 1)(p - 1) \);
(d) if at least one place \( p \) of \( K \) satisfies \( m_p > 0 \), then \( k \) is algebraically closed in \( L \), and

\[
g(L) = p \cdot g(K) + \frac{p-1}{2}(-2 + \sum_{p \in P_K} (m_p + 1) \cdot \deg p).
\]

Note that in [13, Appendix A], it is shown that all cyclic field extensions \( L/K \) of degree \( p \) (the characteristic of \( K \)) are Artin-Schreier extensions. When we look at the left hand side of the defining equation of the extension, it turns out to be an additive polynomial over \( k \), i.e. of the form

\[
f(T) = a_n T^p + a_{n-1} T^{p-1} + \ldots + a_1 T + a_0 T
\]

with all the coefficients in \( k \) and \( a_0 \neq 0 \). Observe that \( f(T) \) is separable since \( f'(T) = a_0 \) and obviously it cannot have any common zero with \( f(T) \). Note that it is called additive since it has the property \( f(u + v) = f(u) + f(v) \), which follows from the property of Frobenius map. Hence if all the roots of \( f(T) \) are in \( k \), then they form a subgroup of the additive group of \( k \) of order \( p^n \).

So we give a more general definition of Artin-Schreier extension as follows.

**Proposition 3.2.20.** Let \( K/k \) be an algebraic function field with \( k \) as full constant field. Denote by \( p \) the characteristic of \( k \). Assume that \( p > 0 \). Let \( f(T) \) be an additive polynomial of degree \( p^n \) as defined above, which has all its roots in \( k \). Let \( u \in K \), satisfying that for each \( p \in \mathbb{P}_K \), there exists an element \( z_p \in K \) such that

\[
v_p(u - f(z_p)) \geq 0
\]

or

\[
v_p(u - f(z_p)) = -m \text{ with } m > 0 \text{ and } m \text{ not divisible by } p.
\]

Define \( m_p := -1 \) in the first case and \( m_p := m \) in the second case. Consider the extension field \( L = K(y) \) of \( K \) where \( y \) satisfies the equation \( f(y) = u \). Then the following holds:

1. the extension \( L/K \) is Galois of degree \( p^n \) and its Galois group is the product of \( n \) cyclic groups. To be precise, \( \text{Gal}(L/K) \) is isomorphic to \( (\mathbb{Z}/p\mathbb{Z})^n \);

2. a place \( p \in \mathbb{P}_K \) is unramified in \( L/K \) if and only if \( m_p = -1 \);

3. a place \( p \) is totally ramified in \( L/K \) if and only if \( m_p > 0 \). Denote the place lying over \( p \) by \( q \), then the different exponent is give by \( d(q|p) = (m_p + 1)(p^n - 1) \);
(4) if at least one place \( p \) of \( K \) satisfies \( m_p > 0 \), then \( k \) is algebraically closed in \( L \), and

\[
g(L) = p^n \cdot g(K) + \frac{p^n - 1}{2} (-2 + \sum_{p \in \mathcal{P}_K} (m_p + 1) \cdot \deg p).
\]

### 3.3 Towers of Function Fields

Now let us move to towers of function fields, which are basically sequences of function fields satisfying certain properties.

**Definition 3.3.1.** Let \( \mathcal{F} = (F_0, F_1, \ldots) \) be an infinite sequence of function fields. We call \( \mathcal{F} \) a tower if it satisfies the following conditions:

(a) \( F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_n \subsetneq \ldots \), and all \( F_n \) for \( n \geq 0 \) have the same full constant field;

(b) for each \( i \geq 0 \), the extension \( F_{i+1}/F_i \) is algebraic, finite and separable;

(c) the genus \( g(F_i) \) tends to infinity when \( i \) goes to infinity.

Note that there is an equivalent condition to the third one, stating that \( g(F_j) \geq 2 \) for some \( j > 0 \), and a proof to the equivalence can be found in [13, Chapter 7, Section 7.2]. We always assume that \( F_i \) has \( \mathbb{F}_q \) as its full constant field for \( i = 1, 2, \ldots \).

The research into towers began from the search for curves with many points, which could be used widely in coding theory and cryptography. So one of the main purposes of the investigation into the tower is to look for towers which have as many rational places with respect to the genus as possible. Thus we are going to give the definitions of Ihara’s constant, asymptotically good or bad towers.

**Definition 3.3.2.** The *Ihara’s constant* is defined as:

\[
A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g},
\]

where \( N_q(g) := \max\{N_1(K) \text{ for } K \text{ a function field over } \mathbb{F}_q \text{ of genus } g\} \).
There are several upper bounds of Ihara’s constant. By the Hasse-Weil bound, we know that $A(q) \leq 2q^{\frac{1}{2}}$. But unfortunately, it is shown that this bound cannot be attained for function fields with large genus. As an improvement to the Hasse-Weil bound, Serre’s bound induces that $A(q) \leq 2\sqrt{q}$. A further improvement to this is called the Drinfeld-Vlăduţ bound, stating that $A(q) \leq q^{1/2} - 1$, and it is shown that it could be attained when $q$ is a square.

**Definition 3.3.3.** Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a tower of function fields over $\mathbb{F}_q$, then

(a) the splitting rate of the tower over $F_0$ is defined as:

$$\nu(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{N_1(F_i)}{[F_i : F_0]}.$$  

(b) the genus of the tower over $F_0$ is defined as:

$$\gamma(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]}.$$  

(c) the limit of the tower is defined as:

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N_1(F_i)}{g(F_i)}.$$  

Note that these limits do exists in towers, because

- the sequence $\{N_1(F_i)/[F_i : F_0]\}_{i}$ is decreasing and is bounded by 0 and $N_1(F_0)$, since a place in $F_0$ cannot have more than $[F_i : F_0]$ places lying over it, otherwise it contradicts to the fundamental equation;

- the sequence $\{g(F_i)/[F_i : F_0]\}_{i}$ is increasing by Hurwitz formula,

hence we have that

(i) the splitting rate

$$0 \leq \nu(\mathcal{F}/F_0) \leq N_1(F_0) < \infty;$$

(ii) the genus

$$0 < \gamma(\mathcal{F}/F_0) \leq \infty;$$
3. Function Fields and Towers of Function Fields

(iii) the limit can also be obtained by $\lambda(\mathcal{F}) = \nu(\mathcal{F}/F_0)/\gamma(\mathcal{F}/F_0)$, and it is bounded by Ihara’s constant:

$$0 \leq \lambda(\mathcal{F}) \leq A(q) < \infty.$$ 

**Remark 3.3.4.** Note that when we consider a tower of function fields, say $\mathcal{F} = (F_0, F_1, \ldots)$, by definition, all the extensions $F_{i+1}/F_i$ for $i \geq 0$ are finite and separable. If $F_0$ is also a separable finite extension field of $k(x)$ (of which being a finite extension is satisfied by definition), then we can always add a ’basement’ to the tower, hence we can change the tower a little bit to $\mathcal{F}' = (k(x), F_0, F_1, \ldots)$. It is clear that the properties we care about of the tower do not change when we move from $\mathcal{F}$ to $\mathcal{F}'$. So in the following context, we always assume that $F_0 = k(x)$.

**Definition 3.3.5.** Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a tower of function fields over $\mathbb{F}_q$, then it is called asymptotically good if the limit of the tower $\lambda(\mathcal{F})$ is positive; it is called asymptotically bad otherwise. In particular, if $\lambda(\mathcal{F}/F_0)$ reaches $A(q)$, then the tower is said to be asymptotically optimal.

In most cases, $\lambda(\mathcal{F})$ of a tower $\mathcal{F}$ is strictly less than the Ihara’s constant $A(q)$. So those towers with large limits are interesting for us, since they can provide nontrivial lower bounds for $A(q)$.

**Definition 3.3.6.** Let $\mathcal{F} = (F_0, F_1, \ldots)$ and $\mathcal{E} = (E_0, E_1, \ldots)$ be two towers of function fields over $\mathbb{F}_q$. Then $\mathcal{E}$ is said to be a subtower of $\mathcal{F}$ if for each $i \geq 0$, there exists an index $j$ depending on $i$ such that $E_i$ can be embedded into $F_j$ over $\mathbb{F}_q$.

The introduction of subtowers gives a way to estimate the limit of a tower, since suppose $\mathcal{E}$ is a subtower of $\mathcal{F}$, then $\lambda(\mathcal{E}) \geq \lambda(\mathcal{F})$, hence $\mathcal{F}$ being asymptotically good induces that $\mathcal{E}$ is asymptotically good, and $\mathcal{E}$ being asymptotically bad induces that $\mathcal{F}$ is asymptotically bad too.

**Remark 3.3.7.** Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a tower of function fields over $\mathbb{F}_q$. Then we can build another tower $\mathcal{E} = (E_0, E_1, \ldots)$ where for each $i \geq 0$, the function field $E_i$ is defined as the Galois closure of $F_i$ over $F_0$. Then we call $\mathcal{E}$ the Galois closure of the tower $\mathcal{F}$ over $F_0$. We can see that $\mathcal{F}$ is a subtower of $\mathcal{E}$, hence if $\mathcal{E}$ is asymptotically good, so is $\mathcal{F}$. Moreover, if $\mathcal{E}$ is optimal, so is $\mathcal{F}$.

Now we define two sets of places which will help us to determine whether the tower is asymptotically good or bad.
Definition 3.3.8. Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a tower of function fields over $\mathbb{F}_q$.

(a) The splitting locus of $\mathcal{F}$ over $F_0$ is defined as:

$$\text{Split}(\mathcal{F}/F_0) := \{ p \in \mathbb{P}_{F_0} \mid \deg p = 1 \text{ and } p \text{ splits completely in all extensions } F_n/F_0 \}.$$ 

(b) The ramification locus of $\mathcal{F}$ over $F_0$ is defined as:

$$\text{Ram}(\mathcal{F}/F_0) := \{ p \in \mathbb{P}_{F_0} \mid p \text{ is ramified in } F_n/F_0 \text{ for some } n \geq 1 \}.$$ 

Note that the splitting locus is always a finite set, and even may be empty.

Proposition 3.3.9. Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_q$, and $\text{Split}(\mathcal{F}/F_0)$ and $\text{Ram}(\mathcal{F}/F_0)$ are defined as above.

(1) The splitting rate satisfies:

$$\nu(\mathcal{F}/F_0) \geq |\text{Split}(\mathcal{F}/F_0)|.$$ 

(2) Assume that the ramification locus is finite and for each place $p \in \text{Ram}(\mathcal{F}/F_0)$ there is a constant $c_p$ such that $d(q \mid p) \leq c_p \cdot e(q \mid p)$ holds for all $n \geq 1$ and $q \in \mathbb{P}_{F_n}$ lying over $p$. Then by Hurwitz formula, the genus of the tower satisfies:

$$\gamma(\mathcal{F}) \leq g(F_0) - 1 + \frac{1}{2} \cdot \sum_{p \in \text{Ram}(\mathcal{F}/F_0)} c_p \cdot \deg p.$$ 

These are quite straightforward from the definitions of splitting locus and ramification locus. In particular, if the tower is tame, i.e. all the extensions $F_{n+1}/F_n$ are tame, then we can choose $c_p = 1$ for all the places ramified, and get:

$$\gamma(\mathcal{F}) \leq g(F_0) - 1 + \frac{1}{2} \cdot \sum_{p \in \text{Ram}(\mathcal{F}/F_0)} \deg p.$$ 

Now the question goes to how to determine the splitting locus and ramification locus. Unfortunately, it is usually difficult. But when dealing with explicit towers, we have some ways to give estimations to them, which will be given as Proposition 3.3.11 and Proposition 3.3.12.

The towers which attract a lot of attention nowadays are the explicit towers, which are the towers whose function fields are given by explicit equations. We introduce a special kind of explicit towers in the following.
Definition 3.3.10. Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a tower of function fields over $\mathbb{F}_q$. We call it a recursive tower if there exists a polynomial $f(X, Y)$ with coefficients in $\mathbb{F}_q$, and functions $x_n \in F_n$ such that the following conditions are satisfied:

(a) the polynomial $f(X, Y)$ is separable in both variables $X$ and $Y$;
(b) $F_{n+1} = F_n(x_{n+1})$ with $f(x_n, x_{n+1}) = 0$ for all $n \geq 0$;
(c) $[F_{n+1} : F_n] = \deg_Y f(X, Y)$ for all $n \geq 0$.

Sometimes we also say that the tower $\mathcal{F}$ is defined by $f(X, Y) = 0$.

As said before, there are some ways to give estimations to the splitting locus and ramification locus of explicit towers. The proofs to Proposition 3.3.11 and Proposition 3.3.12 can be found in [7, Section 3].

Proposition 3.3.11. Let $\mathcal{F} = (F_0 = \mathbb{F}_q(x), F_1, \ldots)$ be a recursive tower over $\mathbb{F}_q$ which is defined by the equation $f(Y) = g(X)$, with $f(Y)$ and $g(X)$ rational functions over $\mathbb{F}_q$. Let $F$ be the function field $\mathbb{F}_q(x, y)$ with $f(y) = g(x)$. Assume that there exists a nonempty subset $S$ of $\mathbb{F}_q \cup \{\infty\}$ which satisfies that for all $\alpha \in S$, the equation $f(\beta) = g(\alpha)$ has $m = \deg f$ distinct roots in $S$.

Then for all $\alpha \in S$, the place $(x_0 = \alpha)$ splits completely in $\mathcal{F}/F_0$, hence is in the splitting locus of the tower. So we have

$$\nu(\mathcal{F}) \geq |S|.$$ 

Proposition 3.3.12. Let $\mathcal{F} = (F_0 = \mathbb{F}_q(x), F_1, \ldots)$ be a recursive tower over $\mathbb{F}_q$ which is defined by the equation $f(Y) = g(X)$, with $f(Y)$ and $g(X)$ rational functions over $\mathbb{F}_q$. Let $F$ be the function field $\mathbb{F}_q(x, y)$ with $f(y) = g(x)$. Assume that there exists a finite subset $R \subseteq \overline{\mathbb{F}}_q \cup \{\infty\}$ such that the following two conditions hold:

(1) the set $R$ contains $R_0 := \{x(\mathfrak{p})| \mathfrak{p} \in \mathbb{F}_{F_0} \text{ which ramifies in } F/F_0\}$;
(2) if $\beta \in R$ and $\alpha \in \overline{\mathbb{F}}_q \cup \{\infty\}$ such that $f(\beta) = g(\alpha)$, then $\alpha$ is also in $R$.

Then the ramification locus of the tower $\mathcal{F}$ satisfies:

$$\text{Ram}(\mathcal{F}/F_0) \subseteq \{\mathfrak{p}| \mathfrak{p} \in \mathbb{P}_{F_0} \text{ with } x_0(\mathfrak{p}) \in R\},$$
where \( x_0(p) \) is the value of function \( x_0 \) at \( p \). In particular, the ramification locus is finite and

\[
\sum_{p \in \text{Ram}(F/F_0)} \deg p \leq |R|
\]

So what will we do when given a polynomial and a ‘tower’ defined by the polynomial? The very first problem is to determine whether this ‘tower’ is well-defined or not, of course, only after which we can start to look into the properties of that tower, for example the genus, the number of rational places, the limit, and so on. The next proposition gives sufficient conditions for an answer to this question.

**Proposition 3.3.13.** Consider a sequence of function fields \( F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \), where \( F_0 \) is a function field with exact constant field \( \mathbb{F}_q \) and the extension \( F_{n+1}/F_n \) is finite for all \( n \geq 0 \). Suppose that for all \( n \) there exist places \( p_n \in \mathbb{P}_{F_n} \) and \( q_n \in \mathbb{P}_{F_{n+1}} \) which lies over \( p_n \), and has the ramification index \( e(q_n|p_n) > 1 \). Then it follows that \( F_{n+1} \supseteq F_n \). Moreover, if we have that \( e(q_n|p_n) = [F_{n+1}:F_n] \) for all \( n \geq 0 \), then \( \mathbb{F}_q \) is also the full constant field of \( F_n \) for all \( n \geq 0 \).

The proof of this proposition mainly uses the fundamental equation and Remark 3.2.9.

### 3.4 Two Examples of Towers of Function Fields

#### 3.4.1 The Tame Tower \( \mathcal{T} \)

Here we give an example of a tame tower of function fields. Consider the tower over the field \( \mathbb{F}_4 \) with four elements, which is given recursively by the polynomial

\[
f(X,Y) = Y^3(X^2 + X + 1) - X^3.
\]

First we need to show that this tower is well-defined, which means that we need to show the following:

(i) for any \( n \geq 0 \), \( F_n \subseteq F_{n+1} \), and \( F_{n+1}/F_n \) is separable for all \( n \geq 0 \);

(ii) all the function fields \( F_i \)’s have the same full constant field \( \mathbb{F}_4 \);
(iii) the genus of a function field \( F_j \) is at least 2 for some \( n \geq 1 \).

The first one is easy to see, since \( x_n^2 + x_n + 1 \) could not have a third root in \( F_n = F_{n-1}(x_n) \), and the extension \( F_{n+1}/F_n \) is inseparable if and only if there exists a common zero of \( f(X,Y) \) and \( f'_Y(X,Y) \) as functions of \( Y \), where the only zero of \( f'_Y(X,Y) \) is \( Y = 0 \), which is not a zero of \( f(X,Y) \).

We prove the second one using Proposition 3.3.13. Let \( p_0 = (x_0 = \infty) \) be the place at infinity of the function field \( F_0 = \mathbb{F}_4(x_0) \), and let \( q_0 \) be a place of the field \( F_1 = \mathbb{F}_4(x_0, x_1) \) which lies over \( p_0 \). The place \( p_0 \) is a single pole of the function \( x_0^3/(x_0^2 + x_0 + 1) \), and hence we have

\[
3v_{q_0}(x_1) = v_{q_0}(x_1^3) = e(q_0|p_0)v_{p_0}(\frac{x_0^3}{x_0^2 + x_0 + 1}) = -e(q_0|p_0).
\]

Since the extension degree can not exceed the degree of the defining function \( f(X,Y) \) in \( Y \), i.e. \( [F_1 : F_0] \leq 3 \), we have that \( e(q_0|p_0) \leq [F_1 : F_0] \leq 3 \) by fundamental equation, hence \( e(q_0|p_0) = 3 \) and \( v_{q_0}(x_1) = -1 \), thus we conclude that \( [F_1 : F_0] = e(q_0|p_0) = 3 \), \( q_0 \) is a single pole of \( x_1 \), and \( p_0 \) is totally ramified in \( F_1/F_0 \). In the next step, take \( p_1 = q_0 \) and let \( q_1 \) be a place of \( F_2 \) lying over \( p_1 \). Similar as the discussion above, it is easy to show that \( e(q_1|p_1) = 3 = [F_2 : F_1] \). Iterate the procedure and we can get places \( p_n \in \mathbb{P}_{F_n} \) and \( q_n \in \mathbb{P}_{F_{n+1}} \), with \( q_n|p_n \) and \( e(q_n|p_n) = [F_{n+1} : F_n] = 3 \), thus by Proposition 3.3.13, we get the conclusion that \( \mathbb{F}_4 \) is the exact constant field of \( F_n \) for all \( n \geq 0 \).

It still remains to prove that \( g(F_j) \geq 2 \) for some \( j \geq 1 \). From the equation \( x_1^3 = x_0^3/(x_0^2 + x_0 + 1) \), we can see that only the following places are ramified in \( F_1/F_0 \):

- the pole of \( x_0 \);
- the place of degree 2 corresponding to \( x_0^2 + x_0 + 1 \).

Hence by the Hurwitz formula, the genus of \( F_1 \) is

\[
g(F_1) = 1 + [F_1 : F_0](g(F_0) - 1) + \frac{1}{2} \sum_{p \in \mathbb{P}_{F_0}} \sum_{q|p} d(q|p) \deg q \\
\geq 1 - 3 + \frac{1}{2}(2 + 4) \\
= 1,
\]
and as shown above, the place $p_1$ is totally ramified in $F_2/F_1$, hence $\deg D \geq 2$, thus $g(F_2) \geq 2$.

Thus this is a well-defined tower, denote it by $\mathcal{T}$. Since by Proposition 3.2.18, the extension $F_{n+1}/F_n$ is Galois of degree 3 for $n \geq 0$, the ramification index $e(q|p)$ for any $p \in \mathbb{P}_{F_2}$ and $q|p$ can only be 1 or 3, which is not divisible by 2, the characteristic of the constant field. Therefore, this is a tame tower.

In fact this is an optimal tower, which we will show next. As discussed above, the place $p_0$ of $F_0$ is totally ramified in $F_1/F_0$, and the place of $F_1$ lying over $p_0$ is also totally ramified in $F_2/F_1$, and so on, hence by the transitivity of the ramification index, $p_0$ is totally ramified in $F_n/F_0$, for all $n \geq 1$. Therefore $p_0$ lies in the ramification locus of $\mathcal{T}/F_0$.

Next we will show that the place $p' = (x_0 = 0)$ of $F_0$ splits completely in all the extensions $F_n/F_0$ for $n \geq 1$. Let $q'$ be a place of $F_1$ which lies over $p'$. We can change the definition of the function field a little bit to be $F_1 = F_0(x_1/x_0)$, and the defining equation to be $(x_1/x_0)^3 = 1/(x_0^2 + x_0 + 1)$. Since $v_{p'}(x_0) = 1$, the valuation of the right hand side with respect to $p'$ is 0, hence $p'$ splits completely in the extension $F_1/F_0$. Moreover, from the defining equation, we can also see that $q'$ is a zero of the function $x_1$, and similar as above, it splits completely in $F_2/F_1$. Therefore, $p'$ splits completely in the extension $F_n/F_0$ for all $n \geq 1$, hence it lies in the splitting locus of $\mathcal{T}$ over $F_0$.

To show the tower is in fact optimal, we use Proposition 3.3.12. Let $R_0$ be the set $(\mathbb{F}_4 \setminus \mathbb{F}_2) \cup \{\infty\}$, hence it is just the set of all poles of $X^3/(X^2 + X + 1)$ all of which are single poles. We then show that the set $R := \mathbb{F}_4^* \cup \{\infty\}$ satisfies the two conditions in Proposition 3.3.12 which are:

(i) the set $R$ contains $R_0 := \{x(q)|p \in \mathbb{P}_{F_0}$ which ramifies in $F/F_0\}$;

(ii) if $\beta \in R$ and $\alpha \in \mathbb{F}_q \cup \{\infty\}$ such that $f(\beta) = g(\alpha)$, then $\alpha$ is also in $R$.

Condition (i) is satisfied in an obvious manner, and the second one is satisfied since for $\beta \in \mathbb{F}_4^*$, then $\beta^3 = 1 = \alpha^3/(\alpha^2 + \alpha + 1)$, which turns out that $\alpha$ should satisfy $0 = \alpha^3 + \alpha^2 + \alpha + 1 = (\alpha + 1)^3$, hence $\alpha = 1 \in R$, and for $\beta = \infty$, then $\alpha^3/(\alpha^2 + \alpha + 1) = \infty$ and hence $\alpha = \infty$ or $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$, thus $\alpha \in R$. Therefore, the ramification locus of $\mathcal{T}$ is
contained in the set of places of $F_0$ with $x_0(p) \in R$. Hence we have
\[
g(F_n) = 1 + 3^n \cdot (-1) + \frac{1}{2}(3^n - 1) \cdot \sum_{p \in \text{Ram}(F_n/F_0)} \text{deg } p
\leq 1 - 3^n + 2 \cdot (3^n - 1) = 3^n - 1,
\]
hence
\[
\gamma(J) = \lim_{n \to \infty} \frac{g(F_n)}{[F_n : F_0]} = \lim_{n \to \infty} \frac{3^n - 1}{3^n} = 1.
\]
For the number of rational places, as $p'$ splits completely in the extension $F_n/F_0$, the number of rational places of $F_n$ satisfies
\[
N_1(F_n) \geq [F_n : F_0] = 3^n,
\]
hence
\[
\nu(J) = \lim_{n \to \infty} \frac{N_1(F_n)}{[F_n : F_0]} \geq 1.
\]
Therefore we have the limit of the tower to be
\[
\lambda(J) = \frac{\nu(J)}{\gamma(J)} \geq 1.
\]
The Drinfeld-Vlăduţ bound tells that
\[
\lambda(J) \leq \sqrt{q} - 1 = 1,
\]
so $\lambda(J) = 1$. The tower attains the Drinfeld-Vlăduţ bound, hence it is asymptotically optimal.

### 3.4.2 The Wild Tower $W$

Here we give an example of wild tower of function fields. Consider the tower over the field $\mathbb{F}_q$ with $q = p^2$ and $p$ an odd prime, which is given recursively by the polynomial
\[
f(X, Y) = (X^{p-1} + 1)(Y^p + Y) - X^p.
\]
First we need to show that this tower is well-defined, which means that we need to show the following:
(i) for any $n \geq 0$, $F_n \subseteq F_{n+1}$, and $F_{n+1}/F_n$ is separable for all $n \geq 0$;

(ii) all the function fields $F_i$'s have the same full constant field $\mathbb{F}_{p^2}$;

(iii) the genus of a function field $F_j$ is at least 2 for some $j \geq 1$.

We prove the first two using Proposition 3.3.13. Let $p_0 = (x_0 = \infty)$ be the place at infinity of the function field $F_0 = \mathbb{F}_q(x_0)$, and let $q_0$ be a place of the field $F_1 = \mathbb{F}_q(x_0, x_1)$ which lies over $p_0$. The place $p_0$ is a single pole of the function $x_0^p/(x_0^{p-1} + 1)$, and hence we have

$$p \cdot v_{q_0}(x_1) = v_{q_0}(x_1 + x_1) = e(q_0|p_0)v_{p_0}(\frac{x_0^p}{x_0^{p-1} + 1}) = -e_{q_0|p_0}.$$ 

Thus $e(q_0|p_0) = p$ and $v_{q_0}(x_1) = -1$, which means that $[F_1 : F_0] \geq e(q_0|p_0) = p$ and $q_0$ is a single pole of $x_1$. Since the extension degree can not exceed the degree of the defining function $f(X, Y)$ in $Y$, i.e. $[F_1 : F_0] \leq p$, we get $[F_1 : F_0] = p$ and $p_0$ is totally ramified in $F_1/F_0$. In the next step, take $p_1 = q_0$ and let $q_1$ be a place of $F_2$ lying over $p_1$. Similar as the discussion above, it is easy to show that $e(q_1|p_1) = p = [F_2 : F_1]$. Iterate the procedure and we can get places $p_n \in \mathbb{P}_{F_n}$ and $q_n \in \mathbb{P}_{F_{n+1}}$, with $q_n|p_n$ and $e(q_n|p_n) = [F_{n+1} : F_n] = p$, thus by Proposition 3.3.13, we get the conclusion that $\mathbb{F}_q$ is the exact constant field of $F_n$ for all $n \geq 0$.

It still remains to prove that $g(F_j) \geq 2$ for some $j \geq 1$. From the equation $x_1^p + x_1 = x_0^p/(x_0^{p-1} + 1)$, we can see that only the following places are ramified:

- the pole of $x_0$;
- the places corresponding to the irreducible divisors of $x_0^{p-1} + 1$.

Clearly this is an Artin-Schreier extension, so by Proposition 3.2.19, the genus of $F_1$ is

$$g(F_1) = p \cdot g(F_0) + \frac{p-1}{2}(-2 + \sum_{p \in \text{Ram}(F_1/F_0)} (m_q + 1) \deg q) \geq (p - 1)^2,$$

since $m_p$ is always positive for $p$ which ramifies in the extension $F_1/F_0$. And as $p > 2$, the genus of $F_1$ is larger than 2.
3. Function Fields and Towers of Function Fields

Thus this is a well-defined tower, denote by $W$. Since the place $p_0$ above is wildly ramified in $F_1/F_0$, this is a wild tower.

In fact this is an optimal tower, which we will show next. As discussed above, the place $p_0$ of $F_0$ is totally ramified in $F_1/F_0$, and the place of $F_1$ lying over $p_0$ is also totally ramified in $F_2/F_1$, and so on, hence by the transitivity of the ramification index, $p_0$ is totally ramified in $F_n/F_0$, for all $n \geq 1$. Therefore $p_0$ lies in the ramification locus of $T/F_0$. To identify the ramification locus, we use Proposition 3.3.12. Let $R_0$ be the set $\{a|a^{p-1} + 1 = 0\} \cup \{\infty\}$, hence it is just the set of all poles of $X^p/X^{p-1} + 1$, all of which are single poles. We then show that the set $R := \{a|a^p + a = 0\} \cup \{\infty\}$ satisfies the two conditions in Proposition 3.3.12 which are:

(i) the set $R$ contains $R_0 := \{x(q)|p \in \mathbb{F}_{F_0} \text{ which ramifies in } F/F_0\}$;

(ii) if $\beta \in R$ and $\alpha \in \mathbb{F}_q \cup \{\infty\}$ such that $f(\beta) = g(\alpha)$, then $\alpha$ is also in $R$.

Condition (i) is satisfied in an obvious manner, and the second one is satisfied since for $\beta \in \{a|a^p + a = 0\}$, then $\beta^p + \beta = 0 = a^p/(a^{p-1} + 1)$, hence $\alpha = 0 \in R$, and for $\beta = \infty$, then $a^p/(a^{p-1} + 1) = \infty$ and hence $\alpha = \infty$ or $\alpha^{p-1} + 1 = 0$, thus $\alpha \in R$. Therefore, the ramification locus of $T$ is contained in the set of places of $F_0$ with $x_0(p) \in R$. In fact, the ramification locus is just $\{(x_0 = a)|a \in R\}$, since we have checked that the places $(x_0 = \infty)$ and $(x_0 = a)$ for $a^{p-1} + 1 = 0$ ramify in $F_1/F_0$, and the place $(x_0 = 0)$ ramifies in $F_2/F_0$.

Next we will show that the splitting locus of the tower is given by

$$\text{Split}(W/F_0) = \{(x_0 = a)|a \in \mathbb{F}_q \text{ and } a^p + a \neq 0\}.$$

For any $\alpha \in S := \{a \in \mathbb{F}_q|a^{p} + a \neq 0\}$, we have that $\alpha^p/(\alpha^{p-1} + 1)$ is in $\mathbb{F}_q^*$, hence the equation $\beta^p + \beta = \alpha^p/(\alpha^{p-1} + 1)$ has $p$ distinct roots in $S$. Then it follows from Proposition 3.3.11 that

$$\text{Split}(W/F_0) \supseteq S.$$

The equality holds since $S \cup \text{Ram}(W/F_0) = \mathbb{F}_q \cup \{(x_0 = \infty)\}$ and $\text{Split}(W/F_0) \cap \text{Ram}(W/F_0) = \emptyset$. 


3.4. Two Examples of Towers of Function Fields

Therefore, for the genus of the tower, we first claim that if \( p \), a place of \( F_0 \), ramifies in the tower, and \( q \) lies over \( p \), then the different exponent is \( d(q|p) = 2(e(q|p) - 1) \), which is proven in \([5]\). According to Remark 3.2.14, \( p \) is weakly ramified in the extension \( F_1/F_0 \). Since the ramification locus is \( \{a|a^p + a = 0\} \cup \{\infty\} \), we have

\[
g(F_n) = 1 + p^n \cdot (-1) + \frac{1}{2} \cdot 2(p^n - 1) \cdot \sum_{p \in \text{Ram}(W/F_0)} \deg p
\]

\[
\leq 1 - p^n + (p^n - 1) \cdot (p + 1)
\]

\[
= p(p^n - 1),
\]

hence

\[
\gamma(W) = \lim_{n \to \infty} \frac{g(F_n)}{[F_n : F_0]} = \lim_{n \to \infty} \frac{p(p^n - 1)}{p^n} = p.
\]

For the number of rational places, as the splitting locus is \( \{(x_0 = a)|a \in \mathbb{F}_q \text{ and } a^p + a \not= 0\} \), the number of rational places of \( F_n \) satisfies

\[
N_1(F_n) \geq (q - p)[F_n : F_0] = p^n(p^2 - p),
\]

hence

\[
\nu(W) = \lim_{n \to \infty} \frac{N_1(F_n)}{[F_n : F_0]} \geq p^2 - p.
\]

Therefore we have the limit of the tower to be

\[
\lambda(W) = \frac{\nu(W)}{\gamma(W)} \geq p - 1.
\]

The Drinfel-Vlăduţ bound tells that

\[
\lambda(W) \leq \sqrt{q} - 1 = p - 1,
\]

so \( \lambda(W) = p - 1 \). The tower \( W \) attains the Drinfeld-Vlăduţ bound, hence it is asymptotically optimal.

Remark 3.4.1. In fact the prime \( p \) in the defining polynomial can be replaced by any power of \( p \), as long as \( p \) is the characteristic of the constant field. The resulting tower is also wild and optimal.
4. The Decomposition Group and Higher Ramification Groups

Let $K$ be an algebraic function field and $p$ be a place of it. Then we have a discrete valuation of $K$ corresponding to the place, say $v_p$, and the discrete valuation ring $\mathcal{O}_{p,K}$. Let $L/K$ be an algebraic extension of function fields, and $q$ be a place of $L$, lying above $p$, which gives rise to the valuation $v_q$ and the corresponding discrete valuation ring $\mathcal{O}_{q,L}$. In this section, we always assume that $L/K$ is Galois, and denote the Galois group by $G$.

4.1 The Decomposition Group and the Higher Ramification Groups

In this section, we mainly introduce the definitions of decomposition groups, inertia groups and higher ramification groups.

**Definition 4.1.1.** Let $K$, $L$, $G$, $p$ and $q$ be defined as above. Then we can define the *decomposition group* $G_q$ associated to $q$ as follows:

$$G_q := \{ \sigma \in G | \sigma(q) = q \}.$$

As a subgroup of the decomposition group, the *inertia group* $I_q$ is defined as follows:

$$I_q := \{ \sigma \in G_q | v_q(\sigma(a) - a) \geq 1 \text{ for all } a \in \mathcal{O}_{q,L} \}.$$

Note that it is unique by definition.
Or equivalently, it can also be defined as the kernel of the map:

\[ G_q \twoheadrightarrow \text{Gal}(\kappa_q/\kappa_p) \]

\[ \sigma \mapsto \bar{\sigma}, \]

with \( \kappa_q := \mathcal{O}_{q,L}/q \) and \( \kappa_p := \mathcal{O}_{p,K}/p \), the residue class fields, and \( \bar{\sigma}(\bar{a}) = \sigma(a) \) for \( \bar{a} \in \kappa_q \) and \( a \) some lifting of \( \bar{a} \) to \( L \).

Note that the decomposition group is just the Galois group of \( L_q \) over \( K_p \), where \( L_q \) (resp. \( K_p \)) denotes the completion of \( L \) (resp. \( K \)) at the place \( q \) (resp. \( p \)), then we have the following diagram:

\[ \begin{array}{ccc}
L_q & \longrightarrow & L \\
\downarrow & & \downarrow \sigma \\
G_q & \longrightarrow & K_p \\
\end{array} \]

**Proposition 4.1.2.** Let \( K, L, G, p \) and \( q \) be defined as above. Let \( q' \) be a place of \( L \) which is different from \( q \) but also lies above \( p \). Denote the decomposition group corresponding to \( q \) (resp. \( q' \)) by \( G_q \) (resp. \( G_{q'} \)). Then we have:

1. the decomposition group \( G_q \) is a subgroup of \( G \);
2. there exists an automorphism \( \sigma \in G \) such that \( \sigma G_q \sigma^{-1} = G_{q'} \).

Following from [11, Chapter 3, Proposition 12], the discrete valuation ring \( \mathcal{O}_{q,L} \) is generated as an \( \mathcal{O}_{p,K} \)-algebra by a single element, say \( x \).

**Proposition 4.1.3.** Let \( \sigma \in G_q \), and \( i \) be an integer which is larger than or equal to -1. Then the following conditions are equivalent:

1. \( \sigma \) operates trivially in the quotient ring \( \mathcal{O}_{q,L}/q^{i+1} \);
2. for all \( a \in \mathcal{O}_{q,L} \), \( v_q(\sigma(a) - a) \geq i + 1 \);
3. \( v_q(\sigma(x) - x) \geq i + 1 \).
4.1. The Decomposition Group and the Higher Ramification Groups

The proof to the equivalences are not too difficult. \((1) \iff (2)\) is quite straightforward, and \((2) \iff (3)\) just follows from the fact that \(x\) generates \(\mathcal{O}_{q,L}\) as an \(\mathcal{O}_{p,K}\)-algebra.

Then we can define the higher ramification groups as follows:

**Definition 4.1.4.** For each rational number \(i \geq -1\), define the \(i\)-th *ramification group* 
\((G_q)_i\) corresponding to \(q\) as follows:

\[
(G_q)_i := \{ \sigma \in G_q | v_q(\sigma(a) - a) \geq i + 1 \text{ for all } a \in \mathcal{O}_{q,L} \}.
\]

By Proposition 4.1.3, there is an alternative definition to the \(i\)-th ramification group:

\[
(G_q)_i := \{ \sigma \in G_q | v_q(\sigma(x) - x) \geq i + 1 \},
\]

where \(x\) generates \(\mathcal{O}_{q,L}\) as an \(\mathcal{O}_{p,K}\)-algebra.

Since the valuation takes values in the integers, for any \(i \geq -1\), \((G_q)_i\) is the same as \((G_q)_{\lfloor i \rfloor}\), where \(\lfloor i \rfloor\) refers to the biggest integer which is smaller than or equal to \(i\). Hence we mainly talk about integral indexes afterwards.

**Proposition 4.1.5.** Let \((G_q)_i\) be defined as above. Then the \((G_q)_i\)'s form a decreasing chain of subgroups of \(G_q\). Moreover, \((G_q)_i\) is \(G_q\) itself for \(i = -1\), \((G_q)_i\) is the inertia group of \(G_q\) for \(i = 0\), and for \(i\) sufficiently large, \((G_q)_i\) is trivial.

The reason to that \(\{(G_q)_i\}_i\) is a decreasing chain is the way to construct the higher ramification groups. And the existence of an \(i\) such that \((G_q)_i\) is trivial is guaranteed by the alternative definition of the higher ramification groups. To be precise, let \(x\) generate \(\mathcal{O}_{q,L}\) as an \(\mathcal{O}_{p,K}\)-algebra, and \(i\) be the biggest valuation of \(\sigma(x) - x\) for \(\sigma \in G_q\) (it exists since \(G_q\) is a finite group). Then \((G_q)_{i+1}\) is trivial by definition.

When \(i \geq 0\), we call \((G_q)_i\) a higher ramification group.

**Remark 4.1.6.** As a special case, if the Galois group \(G\) is isomorphic to some \(\mathbb{Z}/q\mathbb{Z}\) for \(q\) a prime, then the subgroups for \(G\) are either trivial or \(G\) itself. Hence if for some \(q|p\), \(G_q\) is not trivial, then we can find an \(i\) such that

\[
G_q = (G_q)_{-1} = \ldots = (G_q)_i \supset (G_q)_{i+1} = \{\text{id}\} = (G_q)_{i+2} = \ldots
\]
4.2 Some Properties of Ramification Groups

There are some important properties of the higher ramification groups which could help us a lot when trying to compute them.

**Proposition 4.2.1.** Let the higher ramification group \((G_q)_i\) be defined as above, and let \(p\) be the characteristic of \(K\), then we have:

1. the quotient \((G_q)_0/(G_q)_1\) is cyclic of order relatively prime to \(p\);
2. the quotient \((G_q)_i/(G_q)_{i+1}\) for \(i > 0\) can be written as a product of groups which are of order powers of \(p\).

A direct result from this proposition is that \((G_q)_1\) is a Sylow \(p\)-subgroup of \((G_q)_0\). In the case of Remark 4.1.6, if \(q\) is prime to \(p\), then \((G_q)_0\) is either \(G_q\) or trivial, and \((G_q)_i\) is always trivial for any \(i > 0\).

**Corollary 4.2.2.** If the characteristic of \(K\) is positive, say \(p\), then the inertia group \((G_q)_0\) is the semi-direct product of a cyclic group of order prime to \(p\) with a normal subgroup whose order is a power of \(p\).

A proof to Proposition 4.2.1 and this corollary refers to [11, Chapter 4, Corollary 1 and 2 to Proposition 7].

4.3 The Different of a Field Extension

In this section, we mainly talk about the different of a field extension and the relation between the different and the ramification groups.

First, let us give a definition of the different.

**Definition 4.3.1.** Let \(A\) be a Dedekind domain, and \(K\) be its field of fractions. Suppose \(L\) is a finite separable extension of \(K\), then denote by \(B\) the integral closure of \(A\) in \(L\). We can define the **codifferent** as follows:

\[
B^* := \{ y \in L | \text{Tr}_{L/K}(xy) \in A \text{ for all } x \in B \}.
\]
Then $B^*$ is a finitely generated $B$-submodule of $L$. Hence following from [11, Chapter 3, Section 3], $B^*$ is a fractional ideal of $L$. And we can define the different of the extension as follows:

**Definition 4.3.2.** Let $A$, $B$, $K$, $L$ and $B^*$ defined as above, then we can define the different of $L$ over $K$ as the inverse ideal of $B^*$. It is denoted as $\mathfrak{D}_{L/K}$.

**Remark 4.3.3.** One may notice that we use the same notation as for the different defined in Definition 3.2.5, which is just because that these two definitions are equivalent. Let $A$ be a Dedekind domain. For a fractional ideal $I$ of $A$, we can define the divisor corresponding to $I$ as follows:

$$\text{Div}(I) := \sum_p v_p(I)p,$$

where it sums over all the prime factors $p$ of $I$. To be precise, if $I$ can be factored as

$$I = p_1^{d_1} \cdots p_r^{d_r},$$

the divisor of $I$ is

$$\text{Div}(I) = d_1p_1 + \cdots + d_rp_r.$$ 

For the different of the extension, by the definition of $d(q|p)$, we can see that $B^*$ can be written as the product of $q^{-d(q|p)}$ over all primes $p$ in $K$ and primes $q$ in $L$ which lie over $p$. Hence

$$\mathfrak{D}_{L/K} = \prod_p \prod_q q^{d(q|p)},$$

whose divisor is just what we defined in Definition 3.2.5.

Moreover, the different behaves well in the completions, which follows from [11, Chapter 3, Proposition 10]:

**Proposition 4.3.4.** Let $q$ be a place of $L$ lying over $p$, a place of $K$. Denote the different of $L$ over $K$ by $\mathfrak{D}_{L/K}$. Let $L_q$ (resp. $K_p$) be the completion of $L$ (resp. $K$) with respect to $q$ (resp. $p$). Denote the ideal generated by $\mathfrak{D}_{L/K}$ in the completion by $\hat{\mathfrak{D}}_{L/K}$. Then we have

$$\hat{\mathfrak{D}}_{L/K} = \mathfrak{D}_{L_q/K_p}.$$ 

Therefore, we can compute the different of $L/K$ by

$$\mathfrak{D}_{L/K} = \prod_p \prod_{q|p} \mathfrak{D}_{L_q/K_p}.$$
We can define a function $i_{G_q}$ on $G_q$ by sending $\sigma$ to $v_q(\sigma(x) - x)$ for $x$ generating $O_{q,L}$ as an $O_{p,K}$-algebra. Observe that $i_{G_q}$ is a map from $G_q$ to $\mathbb{Z}$ with its zero locus being $G_q \setminus (G_q)_0$. If $\sigma$ is not the identity map, then $i_{G_q}(\sigma)$ is always a non-negative integer, and it has the following properties:

\begin{align*}
    i_{G_q}(\sigma) &\geq i + 1 \iff \sigma \in (G_q)_i, \\
    i_{G_q}(\eta\sigma\eta^{-1}) &= i_{G_q}(\sigma), \\
    i_{G_q}(\eta\sigma) &\geq \min(i_{G_q}(\eta), i_{G_q}(\sigma)).
\end{align*}

The first one comes from the definition of the higher ramification groups. The second property follows from the fact that $(G_q)_i$ is normal in $G_q$, and the last property holds because:

\begin{align*}
    i_{G_q}(\eta\sigma) &= v_q(\eta\sigma(x) - x) \\
    &= v_q(\eta(\sigma(x)) - \sigma(x) + \sigma(x) - x) \\
    &\geq \min\{v_q(\eta(\sigma(x)) - \sigma(x)), v_q(\sigma(x) - x)\} \\
    &\geq \min\{i_{G_q}(\eta), i_{G_q}(\sigma)\}
\end{align*}

where the first inequality follows from the strong triangular inequality and the second one follows from the definition of $i_{G_q}$.

The following proposition shows that this function behaves well in the subextensions.

**Proposition 4.3.5.** Let $L/K$ be a finite Galois extension with Galois group $G$. Let $p$ be a place of $K$ and $q$ be a place of $L$ which lies over $p$. Suppose $K'$ is a subextension of $L$ over $K$, then $L$ is Galois over $K'$ with Galois group $H$, hence $H$ is a subgroup of $G$. Let $t$ be the restriction of $q$ into $K'$, and $i_{H_t}$ and $i_{G_q}$ be defined as above. Then for any $\sigma \in H_t$, we have that $i_{H_t}(\sigma) = i_{G_q}(\sigma)$, and $(H_t)_i = (G_q)_i \cap H_t$ for all $i \geq 0$.

There is a corollary to it which is important when dealing with the towers in the next chapter.

**Corollary 4.3.6.** Let $L/K$ be a finite Galois extension with Galois group $G$. Let $p$ be a place of $K$ and $q$ be a place of $L$ which lies over $p$. Let $K_p$ and $L_q$ be the corresponding local fields. Suppose $(K_p)_r$ is the largest subextension of $L_q$ over $K_p$ with $p$ unramified. Denote by $H$ the Galois group of $L_q$ over $(K_p)_r$. Then $H$ is the inertia group $(G_q)_0$, and
the ramification groups of \( G_q \) of nonnegative index are equal to those of \( H_t \) where \( t \) is the restriction of \( q \) into \( (K_p)_r \).

Note that the place \( t \) is totally ramified in the extension \( L_q/(K_p)_r \), and by the transitivity of ramification index, \( e(q|t) = e(q|p) \). We will discuss this in the next chapter.

In addition, if we assume that \( (K_p)_r/K_p \) is Galois, we will see that the ramification groups of \( G_q \) determine those of \( G_q/H_t \), and we have the following diagram:

\[
\begin{align*}
L_q & \quad \downarrow^{(G_q)_{0}} \\
(K_q)_r & \quad \downarrow \\
K_p & 
\end{align*}
\]

**Proposition 4.3.7.** Let notations be defined as above. For any \( \eta \in G_q/H_t \), we have

\[
i_{G_q/H_t}(\eta) = \frac{1}{e(q|t)} \sum_{\sigma \in R_\eta} i_{G_q}(\sigma),
\]

where \( R_\eta \) is defined as the set of preimages of \( \eta \) under the map \( G_q \to G_q/H_t \).

The following is an important proposition stating the relation between the different of an extension and the higher ramification groups.

**Proposition 4.3.8.** Let notations be defined as above. Denote the different of \( L/K \) by \( \mathfrak{D}_{L/K} \), then

\[
v_q(\mathfrak{D}_{L/K}) = \sum_{\sigma \neq id} i_{G_q}(\sigma) = \sum_{i=0}^{\infty} \left( |(G_q)_i| - 1 \right).
\]

Observe that the infinite sum makes sense since for \( i \) sufficiently large, \( (G_q)_i \) is trivial. A proof to this proposition can be found in [11, Chapter 3, Section 1].
5. The Link Between Towers of Function Fields and Group Theory

5.1 A Special Case: Galois Extension

Let us look at a special case first, where the extensions of function fields are Galois. Recall that in Remark 2.2.2, it is shown that when the extension is Galois, we can just take $X$ to be the Galois group $\text{Gal}(L/K)$, denoted by $G$.

5.1.1 The Full Constant Field of a Function Field

As we have seen in Chapter 2, a $\pi$-set $X$ which is transitive under the action of $\pi$ corresponds to a field which is defined by an irreducible polynomial. Let us look at an example now.

Let $K$ be a rational function field over $\mathbb{F}_q$, i.e. $K = \mathbb{F}_q(x)$ for some $x$ transcendental over $\mathbb{F}_q$, and let $L$ be a finite Galois extension of $K$. From Remark 2.2.2, the field $L$ corresponds to a $\pi$-set $X$ which is isomorphic to $\text{Gal}(L/K)$. Then we can look at the following diagram:

\[
\begin{array}{ccc}
K_s = (\mathbb{F}_q(x))_s & \text{\rotatebox[origin=c]{90}{$\cong$}} & \mathbb{F}_q(x) \otimes_K L \\
\text{\rotatebox[origin=c]{90}{$\cong$}} & & \text{\rotatebox[origin=c]{90}{$\cong$}} \\
\mathbb{F}_q(x) & \text{\rotatebox[origin=c]{90}{$\cong$}} & L \\
\text{\rotatebox[origin=c]{90}{$\cong$}} & & \text{\rotatebox[origin=c]{90}{$\cong$}} \\
2 & \text{\rotatebox[origin=c]{90}{$\cong$}} & \text{Gal}(L/K) \\
\text{\rotatebox[origin=c]{90}{$\cong$}} & & \text{\rotatebox[origin=c]{90}{$\cong$}} \\
K = \mathbb{F}_q(x) & \text{\rotatebox[origin=c]{90}{$\cong$}} & \\
\end{array}
\]
Let us look at a subset of $\pi$, namely $\pi'$, which is defined as a subset of $\pi$ such that the following sequence

$$0 \to \pi' \to \pi \to \hat{\mathbb{Z}} \to 0$$

is a short exact sequence. If we choose the set $X$ such that it is transitive under the action of $\pi'$, then we can show that $L$ is defined by an absolutely irreducible polynomial, which by definition implies that $L \cap \overline{F_q} = F_q$, which means that $F_q$ is the full constant field of $L$.

**Proof.** Since $X$ is defined as transitive under the action of $\pi'$, for each pair of elements in $X$, $x$ and $y$, there exists a $\gamma' \in \pi' \subset \pi$, which maps $x$ to $y$, hence $X$ is transitive under the action of $\pi$, which implies that $M(X) = L$ is a field. Let $f(t)$ be the defining polynomial of $L$ over $K$.

If we look at the extension

$$K_s = (\overline{F_q(x)})_s$$

As $\pi'$ is defined to be the kernel of the map from $\pi$ to $\hat{\mathbb{Z}}$, the action of $\pi'$ is trivial in the sub-extension $\overline{F_q(x)}/K$, thus the roots of $f(t)$ are not in $\overline{F_q(x)}$, i.e. $f$ is absolutely irreducible. The same holds in the opposite direction. 

Moreover, if $X$ is not transitive under $\pi'$, we can write $X$ as a disjoint union of the orbits, hence $L$ can be written as a product of absolutely irreducible fields, thus $L \cap \overline{F_q} = F_q^m$, where $m$ is the number of $\pi'$-orbits.

**Proposition 5.1.1.** Let $L/K$ be an algebraic extension of function fields, where $K$ is a rational function field over $\mathbb{F}_q$. Suppose that $L/K$ is finite Galois with Galois group $G$. Let $\pi'$ be defined as above. Then the full constant field of $K$ is $\mathbb{F}_q$ if and only if $G$ is transitive under the action of $\pi'$. 

5.1.2 The Extension of Places

What if we want to look at the behavior of a place in the extension? Let $K$ and $L$ be algebraic function fields such that $L/K$ is a finite Galois extension. Let $p$ be a place of $K$, which lies below $q$, a place of $L$. Denote by $K_p$ and $L_q$ the completion of $K$ and $L$ at places $p$ and $q$, respectively. We would define $\pi_p$ as in the following diagram:

\[
\begin{array}{c}
\pi_p \\
\downarrow \\
K_p \cap K_s \\
\downarrow \\
K
\end{array}
\]

Note that the intersection of $K_p$ and $K_s$ here refers to the largest subfield of $K_p$ which is algebraic separable over $K$. It is easy to see that $\pi_p$ is a closed subgroup of $\pi$. Similar to what we have done with $\pi$ above, we define a subgroup of $\pi_p$, namely $\pi_p'$, which makes the following sequence

\[
0 \rightarrow \pi_p' \rightarrow \pi_p \rightarrow \hat{m}\hat{\mathbb{Z}} \rightarrow 0
\]

a short exact sequence, where $m = \text{deg } p$. Or equivalently, we can define $\pi_p'$ in the following diagram:
where \((K_p)_r\) refers to the largest unramified subextension of \((K_p)_s\) over \(K_p\), and \(m = \deg p\). Note that \(\text{Gal}((K_p)_r/K_p) = m\hat{\mathbb{Z}}\) by the definition of the degree of a place. In this sense, \(\pi'_p\) is equal to the inertia group of \(\pi_p\), according to the Corollary 4.3.6, and the extension \((K_p)_s/(K_p)_r\) is totally ramified.

Denote the decomposition group associated to \(q\) by \(G_q\) and the higher ramification groups by \((G_q)_i\) for \(i = 0, 1, \ldots\). To investigate the ramification of \(p\), we first complete \(L\) at \(q\) and \(K\) at \(p\) to get \(L_q\) and \(K_p\), respectively. Then the extension \(L_q/K_p\) is Galois and with Galois group \(G_q\). Let \((K_p)_r\) be the largest unramified subextension of \(L_q/K_p\). By Corollary 4.3.6, the Galois group \(\text{Gal}(L_q/(K_p)_r)\) is the inertia group, i.e. under our notation, is \((G_q)_0\). Let \(t = q \cap (K_p)_r\), i.e. \(t\) is the restriction of \(q\) in \((K_p)_r\), hence it lies over \(p\). Then we have the following diagram of function fields and the corresponding Galois groups, as well as the places:

Now let us go back to the global field \(L\) and \(K\). Suppose that \(q_1, \ldots, q_m\) be all the places of \(L\) lying over \(p\), then for each \(q_i\), we have the restricts of \(q_i\) to the corresponding \((K_p)_r\) (which is dependent on the choice of \(q_i\)), say \(t_i\), for \(i = 1, 2, \ldots, m\). Then for each \(q_i\) and \(t_i\), we have the following diagram of field extensions and places:

where we have
5.1. A Special Case: Galois Extension

\[ e(q_i|t_i) = \left| (G_{q_i})_0 \right|, f(q_i|t_i) = 1 \]
\[ e(t_i|p) = 1, f(t_i|p) = \left| G_{q_i}/(G_{q_i})_0 \right| \]

for \( i = 1, 2, \ldots, m \).

The following proposition gives an interpretation of the ramification index, the inertia degree and the different exponent.

**Proposition 5.1.2.** The ramification index and inertia degree of \( q \) over \( p \) can be shown as follows:

\[
\begin{align*}
  e(q|p) &= \left| (G_q)_0 \right| \\
  f(q|p) &= \left| G_q/(G_q)_0 \right| = \left| G_q \right| / \left| (G_q)_0 \right| \\
  d(q|p) &= \sum_{i=0}^{\infty} \left( \left| (G_q)_i \right| - 1 \right)
\end{align*}
\]

**Proof.** The formula for different exponent is a direct result from the Proposition 4.3.8.

We can look at the ramification index and inertia degree at each step of the tower:

\[ \begin{array}{c}
L_q \\
(K_p)_r \\
K_p
\end{array} \]

then

(a) in the extension \( (K_p)_r/K_p \), since \( (K_p)_r \) by definition is an unramified extension of \( K_p \), we have

\[ e(p_r|p) = 1, \quad f(p_r|p) = \left| G_q/(G_q)_0 \right|, \]

since \( p_r \) is the only place in \( (K_p)_r \), hence the only place lying over \( p \), then we can compute \( f(p_r|p) \) by the fundamental equality \( \sum_i e_i f_i = [L : K] \);
(b) in the extension $L_q/(K_p)_r$, the extension is totally ramified by Corollary 4.3.6, then we have

$$e(q|p_r) = |(G_q)_0|, \quad f(q|p_r) = 1.$$ 

Hence by the transitivity of the ramification index and inertia degree, we have the following:

$$e(q|p) = e(p_r|p) \cdot e(q|p_r) = |(G_q)_0|, \quad f(q|p) = f(p_r|p) \cdot f(q|p_r) = |G_q/(G_q)_0|.$$ 

From this the result in Remark 3.2.14 is quite straightforward, since the only possible subgroups of $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$ are the trivial group and $\mathbb{Z}/p\mathbb{Z}$ itself.

In Proposition 4.1.2, we have shown that for different places lying over a same place, the decomposition groups associated to them are conjugate.

**Proposition 5.1.3.** Use notations as defined above. We can calculate the number of the places lying over $p$ as

$$m = |\{q \in \mathfrak{P}_L| q \text{ lies over } p\}| = |G/G_q| = \frac{|G|}{|G_q|},$$

where on the right hand side, $q$ is any place of $L$ lying over $p$.

This proposition just follows from the fundamental equation and Proposition 5.1.2.

The following is an interpretation of the Dedekind’s different theorem.

**Theorem 5.1.4.** *(Dedekind’s Different Theorem)* With the notations as above, we have that:

$$d(q|p) \geq e(q|p) - 1.$$ 

The equality holds if and only if $e(q|p)$ is not divisible by the characteristic of $K$, i.e. $p$ is unramified or tamely ramified.
5.1. A Special Case: Galois Extension

We get the expressions of \( e(q|p) \) and \( d(q|p) \) in terms of groups as discussed above:

\[
d(q|p) = \sum_{i=0}^{\infty} \left| (G_q)_i \right| - 1
\]

\[
= \left| (G_q)_0 \right| - 1 + \sum_{i=1}^{\infty} \left( \left| (G_q)_i \right| - 1 \right) \\
\geq e(q|p) - 1,
\]

since all the ramification groups are nonempty.

In the theorem, the equality holds if and only if each \((G_q)_i\) is trivial for \(i = 1, 2, \ldots\). When \(p\) is unramified or tamely ramified, \(e(q|p)\) is not divisible by the characteristic of \(K\), say \(p\), i.e. \(\left| (G_q)_0 \right|\) is not divisible by \(p\). By Proposition 4.2.1, we have that all the \((G_q)_i\) for \(i = 1, 2, \ldots\) are \(p\)-subgroups of \((G_q)_0\). Therefore, \((G_q)_i\) can only be trivial for \(i = 1, 2, \ldots\).

On the other hand, when \((G_q)_i\) is trivial for \(i = 1, 2, \ldots\), \((G_q)_0 / (G_q)_1 = (G_q)_0\) is cyclic of order prime to \(p\) by Proposition 4.2.1, hence \(e(q|p)\) is not divisible by \(p\), which means that \(p\) is unramified or tamely ramified. Therefore, as a conclusion, the equality holds if and only if \(p\) is unramified or tamely ramified.

Note that as shown in Proposition 3.2.11, under the assumption that the extension is always Galois, \(e(q|p)\), as well as \(f(q|p)\), is independent of the choice of \(q\) lying over \(p\). Thus we use \(e_p\) and \(f_p\) for brief in the following.

Then, we look at some special cases of \(e_p\) and \(f_p\).

(i) the ramification index \(e_p\) is 1 if and only if \(\left| (G_q)_0 \right| = 1\), i.e. \((G_q)_0\) is trivial, which is equivalent to that for each \(\sigma \in G_q\), \(\sigma \neq \text{id}\), \(v_q(\sigma x - x) = 0\) for some \(x \in \mathcal{O}_{q,L}\). If \(x \in q\), then \(\sigma x \in q\) since \(\sigma \in G_q\), hence \(v_q(\sigma x - x) \geq 1\). So such \(x\) can only exist in \(\mathcal{O}^*_{q,L}\), such that \(x\) and \(\sigma x\) are not in the same equivalence class of \(\kappa_q\);

(ii) the inertia degree \(f_p\) is 1 if and only if \(G_q = (G_q)_0\), i.e. for each \(\sigma \in G_q\), there is \(v_q(\sigma x - x) \geq 1\) for any \(x \in \mathcal{O}_{q,L}\). For \(x \in q\), similar as above, this always holds; for \(x \in \mathcal{O}^*_{q,L}\), it implies that \(\sigma x\) and \(x\) lie in the same equivalence class of \(\kappa_q\), which is the residue field at \(q\), or, in other words, if we define the action of \(G_q\) on \(\kappa_q\) as \((\sigma, \bar{x}) \mapsto \bar{\sigma x}\) (it is well defined since \(\sigma\) preserves \(q\)), hence \(G_q\) acts transitively on the equivalence class of trivially on \(\kappa_q\).
5. The Link Between Towers of Function Fields and Group Theory

Now we can take a look at the different kinds of ramifications defined in Definition 3.2.8.

(i) A place $p$ is tamely ramified if and only if $e_p$ is not divisible by the characteristic of $K$, i.e. $|(G_q)_0|$ is coprime to $\text{Char}(K)$, which holds if and only if all the $(G_q)_i$ are trivial for $i \geq 1$.

(ii) A place $p$ is totally ramified if and only if $e_p = |G|$ and $f_p = 1$ (we could omit the last condition since it holds when $e_p = |G|$ by the fundamental equality), which holds if and only if $(G_q)_0 = G_q = G$. As we discussed above, the first equality holds if and only if each equivalence class of $\kappa_q$ is stable under the action of $G_q$, which is in fact $G$ here. And the second equality holds if and only if for each $\sigma \in G$, $v_q(\sigma x) \geq 1$ holds for all $x \in q$.

(iii) A place $p$ splits completely if and only if $e_p = f_p = 1$, which holds if and only if $G_q$ is trivial.

Now we are going to look at two important numbers when discussing the property of a tower, which are the number of rational places and the degree of the different (let $n = [L : K]$):

$$N_1(L) = \sum_{p \in \mathcal{P}_K, \deg p = 1, f_p = 1} \frac{n}{e_p \cdot f_p}$$

$$\deg \mathfrak{D}(L/K) = \sum_{p \in \mathcal{P}_K} \sum_{q | p} d(q | p) \cdot \deg q$$

$$= \sum_{p \in \mathcal{P}_K} |G/G_q| \cdot d(q | p) \cdot f_p \cdot \deg p$$

$$= \sum_{p \in \mathcal{P}_K} \sum_{i = 0}^{\infty} |G/G_q| \cdot |(G_q)_i| - 1 \cdot |G_q/(G_q)_0| \cdot \deg p$$

$$= \sum_{p \in \mathcal{P}_K} \sum_{i = 0}^{\infty} |G/(G_q)_0| \cdot |(G_q)_i| - 1 \cdot \deg p.$$
5.1.3 The Splitting Locus and the Ramification Locus of a Tower

Recall that there are two important sets of places when we talk about whether the tower is asymptotically good or bad, which are the splitting locus and the ramification locus:

\[
\text{Split}(\mathcal{F}/F_0) = \{ p \in \mathcal{P}_{F_0} | \deg p = 1 \text{ and } p \text{ splits completely in } F_n/F_0, \text{ for all } n \geq 1 \},
\]

\[
\text{Ram}(\mathcal{F}/F_0) = \{ p \in \mathcal{P}_{F_0} | p \text{ is ramified in } F_n/F_0 \text{ for some } n \geq 1 \}.
\]

From the definition of a tower, the function fields in a tower always have a finite field as full constant field, say \( k \). By Remark 3.3.4, we can assume that \( F_0 = k(x) \) for some \( x \) transcendental over \( k \), then a place in \( F_0 \) is of degree 1 if and only if \( p = (x - \alpha) \), which is denoted as \( p_\alpha \) for some \( \alpha \in k \), hence

\[
\text{Split}(\mathcal{F}/k(x)) = \{ p \in \mathcal{P}_{k(x)} | \deg p = 1 \text{ and } p \text{ splits completely in } F_n/k(x), \text{ for all } n \geq 1 \}
\]

\[
\cong \{ \alpha \in k | e_{p_\alpha} = f_{p_\alpha} = 1 \text{ in } F_n/k(x), \text{ for all } n \geq 1 \}
\]

\[
= \{ \alpha \in k | G_q = \{ \text{id} \} \text{ for all } q|p_\alpha, q \in \mathcal{P}_{F_n}, \text{ for all } n \geq 1 \},
\]

\[
\text{Ram}(\mathcal{F}/k(x)) = \{ p \in \mathcal{P}_{k(x)} | p \text{ is ramified in } F_n/k(x) \text{ for some } n \geq 1 \}
\]

\[
= \{ p \in \mathcal{P}_{k(x)} | e_p \neq 1 \text{ in } F_n/k(x) \text{ for some } n \geq 1 \}
\]

\[
= \{ p \in \mathcal{P}_{k(x)} | (G_q)_0 \neq \{ \text{id} \} \text{ for some } q|p \text{ with } q \in \mathcal{P}_{F_n}, \text{ for some } n \}
\]

\[
= \{ p \in \mathcal{P}_{k(x)} | \exists \sigma \in G_q \text{ for some } q|p \text{ with } q \in \mathcal{P}_{F_n}, \text{ for some } n, \text{ such that each equivalence class in } \kappa_q \text{ is preserved by } \sigma \}.
\]

5.2 The General Case

Here we give an interpretation of Galois closure of a function field.

Let \( L/K \) be an algebraic extension of function fields, where \( K = \mathbb{F}_q(x) \) and \( L \) has \( \mathbb{F}_q \) as its full constant field. Let \( X = S(L) \), with \( K \) set to be the base field. Then as discussed before, there is a normal open subgroup \( \rho \) of \( \pi \) such that \( X = \pi/\rho \). A Galois closure of \( L \) over \( K \) is defined as a Galois extension of \( K \) which contains \( L \), which is minimal in the respect that no proper subextension of it containing \( L \) is normal over \( K \). Hence we can
obtain a Galois closure of $L$ by $L' = \prod_{\sigma \in X} \sigma(L)$. Suppose that the $\pi$-set corresponding to $L'$ is $X'$, and $X' = \pi/\rho'$, then we have the following diagram:

where the extension $L'/K$ is Galois by the construction of $L'$. Thus $X'$ is isomorphic to the Galois group of $L'$ over $K$. So we have an interpretation of Galois closure in terms of groups as follows: a $\pi$-set $X' = \pi/\rho'$ corresponds to the Galois closure of $L$ over $K$, where $L$ corresponds to another $\pi$-set $X = \pi/\rho$, if $\rho'$ is the biggest subgroup of $\rho$ such that $\rho'$ is open normal in $\pi$ and the restriction to $L'$ of any element in $\pi/\rho'$ is an automorphism on $L'$.

Let $p$ be a place of $K$ and $q'$ be a place of $L'$ lying over $p$. Let $q$ be the restriction of $q'$ to $L$, then it lies over $p$. Since $L'$ is the compositum of all the conjugates of $L$, we first look at the compositum of $L$ and one conjugate of $L$, say $\sigma L$ with $\sigma$ nontrivial. Denote the restriction of $q'$ to $\sigma L$ by $\tilde{q}$, then $\tilde{q} = \sigma q$. If $p$ is tamely ramified in $L/K$, then by Abhyankar’s lemma, the ramification index $e(q'|p) = \text{lcm}(e(q|p), e(\sigma q|p))$. But unfortunately, it is usually not easy to compute $e(\sigma q|p)$ when given $e(q|p)$.

5.3 Examples

In this section, we use the tools presented in this chapter to deal with some problems of the towers in subsections 3.4.1 and 3.4.2.

5.3.1 The Tame Tower $T$

Let the tower $T$ be defined as the tame tower presented in subsection 3.4.1.
From the defining equation, it is clear that the extension \( F_{n+1}/F_n \) is a Kummer extension for all \( n \geq 0 \). So \( F_{n+1}/F_n \) for \( n \geq 0 \) is Galois and the Galois group is:

\[
G^{n+1} := \text{Gal}(F_{n+1}/F_n) = \{ \text{id}, x_{n+1} \mapsto \omega x_{n+1}, x_{n+1} \mapsto \omega^2 x_{n+1} \}
\]

\[\cong C_3, \text{ for any } n \geq 0,\]

where \( \omega \) here is a primitive 3-rd root of unity and \( C_3 \) is the cyclic group of order 3.

Let us give an interpretation of the result that \( p_0 = (x_0 = \infty) \) is totally ramified in all the extensions \( F_n/F_0 \), for all \( n \geq 0 \). In \( F_1/F_0 \), let \( p_1 \) be a place of \( F_1 \) lying over \( p_0 \), then by Proposition 5.1.2, we need to compute the decomposition group and the inertia group corresponding to \( p_1 \). By Proposition 4.2.1, the first ramification group is always a Sylow \( p \)-subgroup of the inertia group for \( p \) the characteristic of the constant field. In this case, the decomposition group \( G_{p_1} \) as well as the inertia group \( (G_{p_1})_0 \) is either trivial or \( C_3 \), and the higher ramification groups \( (G_{p_1})_i \) for all \( i \geq 1 \) can only be trivial. Now we compute the inertia group. We have shown in 3.4.1 that \( p_1 \) is a single pole of the function \( x_1 \), and the function \( 1/x_1 \) is a generator of \( O_{p_0,F_1} \) as an \( O_{p_0,F_0} \)-algebra. When \( \sigma = \text{id} \), then \( v_{p_1}(\sigma(x_1) - x_1) = \infty \); when \( \sigma(x_1) = \omega x_1 \) or \( \omega^2 x_1 \), then \( v_{p_1}(\sigma(1/x_1) - 1/x_1) = -v_{p_1}(x_1) = 1 \), hence:

\[
(G_{p_1})_0 = \{ \sigma \in G^1 | v_{p_1}\left(\sigma\left(\frac{1}{x_1}\right) - \frac{1}{x_1}\right) \geq 1 \} = G^1,
\]

since \( (G_{p_1})_0 = G^1 \subseteq G_{p_1} \subseteq G^1 \), we have that \( G_{p_1} = G^1 \). Thus by Proposition 5.1.2, the ramification index and the inertia degree are:

\[
e(p_1|p_0) = |(G_{p_1})_0| = |C_3| = 3,
\]

\[
f(p_1|p_0) = \frac{|G_{p_1}|}{|(G_{p_1})_0|} = 1,
\]

\[
d(p_1|p_0) = \sum_{i=0}^{\infty} |(G_{p_1})_i| - 1 = 2.
\]

Now let us move on to the place \( p' = (x_0 = 0) \) of \( F_0 \) and the place \( q' \) of \( F_1 \) lying over \( p' \). Since the function \( x_1/x_0 \) generates \( O_{q',F_1} \) as an \( O_{p,F_0} \)-algebra as shown in subsection 3.4.1, the decomposition group corresponding to \( q' \) is:
5. The Link Between Towers of Function Fields and Group Theory

\[ G_{q'} = \{ \sigma \in G^1 | \sigma(q') = q' \} = \{ \text{id} \}, \]

since for \( \sigma(x_1) = \omega x_1 \), we have

\[
v_{q'} \left( \sigma \left( \frac{x_1}{x_0} \right) - \frac{x_1}{x_0} \right) = v_{q'} \left( (\omega - 1) \frac{x_1}{x_0} \right) = v_{q'}(\omega - 1) + v_{q'}(x_1) - v_{p'}(x_0) = 1 - e(q'|p')v_{p'}(x_0)
\]

\[
= 1 - e(q'|p') < 1
\]

since the ramification index is always positive; similar considerations apply to \( \sigma(x_1) = \omega^2 x_1 \).

Hence the inertia group is also trivial and we have the ramification index and inertia degree both 1, which means that \( p' \) splits completely in \( F_1/F_0 \).

5.3.2 The Wild Tower \( \mathcal{W} \)

Let the tower \( \mathcal{W} \) be defined as the wild tower presented in subsection 3.4.2.

From the defining equation, it is clear that the extension \( F_{n+1}/F_n \) is an Artin-Schreier extension for all \( n \geq 0 \). So all the extensions \( F_{n+1}/F_n \) for \( n \geq 0 \) are Galois and the Galois groups are:

\[
G^{n+1} : = \text{Gal}(F_{n+1}/F_n) = \{ \text{id}, x_{n+1} \mapsto 1 + x_{n+1}, x_{n+1} \mapsto 2 + x_{n+1}, \ldots, x_{n+1} \mapsto p - 1 + x_{n+1} \} \\
\cong C_p, \text{ for any } n \geq 0,
\]

where \( C_p \) is the cyclic group of order \( p \).

Let us give an interpretation of that \( p_0 = (x_0 = \infty) \) is totally ramified in all the extensions \( F_n/F_0 \), for all \( n \geq 0 \). In \( F_1/F_0 \), let \( p_1 \) be a place of \( F_1 \) lying over \( p_0 \), then by Remark 4.1.6, we need to compute the decomposition group and the inertia group corresponding to \( p_1 \). By Proposition 4.2.1, if \( G_{p_1} \) is not trivial, then we can find an integer \( j \) such that \( G^1 = G_{p_1} = (G_{p_1})_0 = \ldots = (G_{p_1})_j \supseteq \{ \text{id} \} = (G_{p_1})_{j+1} = \ldots \). In fact, the index \( j \) is determined by \( \min_{\sigma \in G^1} v_{p_1}(\sigma(x) - x) \) for \( x \) which generates \( \mathcal{O}_{p_1,F_1} \) as an \( \mathcal{O}_{p_0,F_0} \)-algebra. As the function \( 1/x_1 \) is a generator we need, we have that:
5.3. Examples

\[
\min_{\sigma \in G^1} \{ v_{p_1} \left( \sigma \left( \frac{1}{x_1} \right) - \frac{1}{x_1} \right) \} = \min_{i=0,1,...,p-1} \{ v_{p_1} \left( \frac{1}{i + x_1} \right) - \frac{1}{x_1} \} = \min_{i=0,1,...,p-1} \{ v_{p_1} \left( \frac{i}{x_1(x_1 + i)} \right) \} = 2.
\]

Thus we have that \( j = 1 \) and then the ramification index, the inertia degree and the different exponent are as follows:

\[
e(p_1|p_0) = |(G_q)_0| = p;
\]
\[
f(p_1|p_0) = |G_q/(G_q)_0| = |G_q|/|(G_q)_0| = 1;
\]
\[
d(p_1|p_0) = \sum_{i=0}^{\infty} |(G_q)_i| - 1) = 2(p - 1).
\]

For \( n \geq 2 \), let \( p_n \) be a place of \( F_n \) lying over \( p_0 \). We have shown in subsection 3.4.2 that \( p_1 \) is the only place of \( F_1 \) lying over \( p_0 \), and from the defining equation, \( p_1 \) corresponds to the single pole of \( x_1 \). Hence using the same trick, we can show that \( p_1 \) is totally ramified in the extension \( F_2/F_1 \), and \( p_2 \) is the only place of \( F_2 \) lying over \( p_1 \), hence also the only place of \( F_2 \) lying over \( p_0 \). Moreover, by the transitivity of the ramification index, the inertia degree and the different exponent in Proposition 3.2.10, we have the following:

\[
e(p_2|p_0) = e(p_2|p_1) \cdot e(p_1|p_0) = p^2
\]
\[
f(p_2|p_0) = f(p_2|p_1) \cdot f(p_1|p_0) = 1
\]
\[
d(p_2|p_0) = e(p_2|p_1) \cdot d(p_1|p_0) + d(p_2|p_1) = 2(p^2 - 1)
\]

Thus \( p_0 \) is totally ramified in the extension \( F_2/F_0 \). Similarly as above, we have that \( p_0 \) is totally ramified in the extension \( F_n/F_0 \), and have the following:

\[
e(p_n|p_0) = p^n, \quad f(p_n|p_0) = 1
\]
\[
d(p_n|p_0) = 2(p^n - 1)
\]

Similarly, when looking at the place \( p' = (x_0 = \alpha) \) of \( F_0 \) with \( \alpha^{l-1} + 1 = 0 \), and the place \( q' \) of \( F_1 \) lying over \( p' \), the place \( q' \) is a pole of \( x_1 \) following from the defining equation of \( F_1/F_0 \). Hence \( 1/x_1 \) is a generator of \( \mathcal{O}_{q', F_1} \) as an \( \mathcal{O}_{p', F_0} \)-algebra. Similar considerations hold as above, so we only need to identify the \( j \) as above by determining the minimal value of
5. The Link Between Towers of Function Fields and Group Theory

$v_p(\sigma(1/x_1) - 1/x_1)$ over all $\sigma \in G^1$, i.e.

$$\min_{\sigma \in G^1} \{ v_{p_1} \left( \sigma \left( \frac{1}{x_1} \right) - \frac{1}{x_1} \right) \} = \min_{i=0,1,\ldots,p-1} \{ v_{p_1} \left( \frac{i}{x_1 + x_1} \right) \} = 2.$$ 

Thus we also have $e(q'|p') = p$, $f(q'|p') = 1$ and $d(q'|p') = 2(p - 1)$.

5.4 Conclusions

5.4.1 Conclusions

In this chapter, we established a link between the towers of function fields and the group theory. To be specific, one can find the interpretations of the full constant field, the ramification index, the inertia degree and the different exponent of an extension of a place of some function field, and also the splitting locus and the ramification locus of a tower. Moreover, two examples of towers are given along with the computations of the ramification index, inertia degree and different exponent of the extensions of some special places. Compare the computations in Section 3.4.1 and Section 5.3.1, as well as in Section 3.4.2 and Section 5.3.2, we can see that it is simplified when we turn to the Galois group and its subgroups. And this holds for the explicit towers when the extensions are Galois and the corresponding Galois groups are easy to represent. Although the examples given are quite easy to compute, we can use computer algebra packages, for example MAGMA, to compute the orders decomposition group, the inertia group and the higher ramification groups of given places when dealing with more complicated cases.

5.4.2 What’s Next

This topic is interesting, not only because it bridged up two different theories, but also because we can have a lot more to ask and to do, among which I only present below two questions which appears most interesting for me.

The first question is to give some criteria for asymptotic properties of towers. As shown in Chapter 3, the asymptotic property of a tower is very important in the research of towers.
5.4. Conclusions

of function fields, which could give a lower bound of the Ihara’s constant. But due to the limit of time, I have not looked into that part yet.

The second question is the one I am most interested in, which is about whether it is possible or not to generalize these considerations to the general case, i.e. when the extension is not Galois. From Remark 3.3.7 and Section 5.2, one can see that for such a tower, we can always look at the Galois closure of it, which is actually a subtower of it and give some bounds for the limit of the original tower. But from Section 2.2, one can also see that using infinite Galois theory, we can associate a finite $\pi$-set to any field extension. Hence given any tower, it is always possible to associate to it a ’tower’ of $\pi$-sets, and if we can generalize the concepts of the decomposition group, the inertia group and the higher ramification groups to the corresponding subsets of those $\pi$-sets, we may find some better way to analyze the asymptotic properties of towers in general case.
References


