The Class Group of Function Fields of Transcendence Degree One

Fragkiskos Gounelas

Final Third Year Undergraduate Individual Project
BSc Joint Mathematics and Computer Science
Imperial College London

Supervisor: Dr. Ambrus Pál

June 11, 2007

Abstract
In this report I aim to cover topics from the theory of algebraic curves, maintaining a strictly algebraic approach, despite the geometric nature of the objects studied. Quite vaguely I will show how the Riemann-Roch theorem aids in the study of function fields, which are defined by algebraic curves. I will also cover how a number theoretic object, namely the zeta function $\zeta_F(s)$, arises in this context and how one can use this to calculate an important invariant of an algebraic curve over a finite constant field, namely its class number.
Contents

1 Function Fields
   1.1 Valuation Rings, Discrete Valuations and Places ............... 1
   1.2 Divisors ......................................................... 14
   1.3 Field Extensions and the Ramification Formula ................. 18
   1.4 The Class Group and the Class Number ........................ 20

2 The Riemann-Roch Theorem ........................................... 21
   2.1 Background and Statement of the Theorem ..................... 21
   2.2 Corollaries and Uses of the Theorem ......................... 25
   2.3 Rational Function Fields and Elliptic Curves ................. 26

3 Finite Constant Field and the Zeta Function ....................... 28
   3.1 The Finiteness of the Class Number .......................... 28
   3.2 The Zeta Function in Function Fields ....................... 29
   3.3 A Functional Equation for $\zeta_F$ .......................... 33

4 The Class Number Formula ............................................ 35
   4.1 Background and Final Preparation ............................. 35
   4.2 The Class Number Formula In Function Fields ............... 35
   4.3 Finding the $L$-Polynomial ................................. 37

5 On Particular Function Fields ........................................ 41
   5.1 Quadratic Extensions of the Rational Function Field ....... 41
   5.2 A Worked Example .............................................. 45

6 Appendix .................................................................... 48
   6.1 Background Material ............................................. 48
   6.2 Worked Example in MAGMA ...................................... 49
Introduction

The theory of algebraic curves is relative new, blossoming primarily in the 19th and 20th century. The fully algebraic approach I present is as new as 70 years old, introduced in books such as [1]. Even though the main object of our study was aimed to be the class number formula induced by the zeta function on finite constant field function fields of transcendence degree 1, much theory was necessary for this to be covered thoroughly. Once someone has presented the appropriate tools though, the main calculation performed involve calculating the genus, the class number, and hence the zeta function of a function field. In papers such as [17], one can see that the theory has progressed enough so as to fully classify all function fields for a given genus, or a given class number.

What we present for congruence function fields though, is a part of results which are known as the Weil conjectures. André Weil went as far as to prove the equivalent of the Riemann hypothesis for the function field case. This states that the zeros of the zeta function $\zeta_F(s)$ where $s \in \mathbb{C}$ all lie on the line where $\text{Re}(s) = \frac{1}{2}$. Most of Weil’s conjectures however were standardised and made into theorems by the work of Pierre Deligne, specifically in [4] and [5].

In the first chapter I will cover function fields which are defined by an algebraic curve. The points on a curve, defined algebraically as places, will lead to the definition of divisors and finally to the divisor class group.

This foundational theory will allow me, in chapter 2, to present ways of calculating an invariant of the function field, namely the genus. I will see how the genus is linked to a specific class in the divisor class group, via the Riemann-Roch theorem, whose set of corollaries are of great importance.

Our work will become interesting however when working over finite fields in chapter 3, where we will prove that the class number, an invariant linked to the divisor class group, is in fact finite. In this case, we will see how the zeta function can be defined and what some of its properties are.

In chapter 4, the class number formula given by the zeta function for finite constant field function fields is introduced and I will show how it can be used to compute the class number.

In the 6-th chapter, I will discuss a special class of function fields, namely quadratic extensions of the rational function field, and also present Kummer’s theorem,
which is an invaluable tool when performing calculations related to function fields. This, and most of the theory covered in this report, is put to use on the function field $\mathbb{F}_5(x, y)$, where $y^2 = x^3 + 2x$.

A brief outline of the main concepts introduced in this report and the order they appear in is summarised in Figure 1.

![Diagram](image)

Figure 1: Main concepts and what chapters they lie in

Last but not least, I fully acknowledge the support of my supervisor Dr. Ambrus Pál, who not only proposed this incredibly fulfilling project to me, but without whose advice and support, the quality of this report would have left a lot to be desired!
1 Function Fields

This chapter is based on work in the books by Stichtenoth [15], which covers the material in elegant detail, but also that of Salvador [14] and Chevalley [1].

In classical number theory, one begins with the ring of integers \( \mathbb{Z} \) and then considers its field of fractions \( \mathbb{Q} \). In a similar manner, in the study of algebraic function fields, we begin with the polynomial ring \( K[x] \) over some field \( K \) and then consider its field of fractions defined as follows.

**Definition 1.1.**
The rational function field \( K(x) \) of one variable \( x \) is the field of all rational functions \( p(x)/q(x) \), where \( p, q \in K[x] \) such that \( q(x) \neq 0 \)

The next step, and in equivalence to number fields, is to consider finite extensions of this field of fractions.

**Definition 1.2.**
An algebraic function field \( F \) of one variable over a field \( K \) is a finite extension of \( K(x) \) for some element \( x \in F \) such that \( x \) is transcendental over \( K \).

To explain the above definitions, one can use the following example. Take \( \mathbb{F}_3 \), the finite field with 3 elements. Define the rational function field with this base field as \( \mathbb{F}_3(t) \). Elements in this field have the form \( \frac{h_2(t)}{h_1(t)} \) with \( h_1, h_2 \in \mathbb{F}_3[t] \). By constructing a finite algebraic extension of this field, say by adjoining \( \alpha \) whose minimal polynomial is \( p(y) = y^2 - t \), we see that this field takes the form \( \mathbb{F}_3(t)[y]/(p(y)) \). Elements in this field are of the form

\[
f(t) = q_1(t) + q_2(t)\sqrt{t}, \text{ with } q_1, q_2 \in \mathbb{F}_3(t)
\]

1.1 Valuation Rings, Discrete Valuations and Places

The title of this report implies that I will be working with function fields over one variable, or of transcendence degree one, such as the one in the above example. Note that it may as well be the case that we have a function field over 2 or more variables, but there will always be a functional equation between them, again, as in the above example.

**Definition 1.3.**
Given a field \( F \) and a sub-field \( K \), a valuation ring \( \mathcal{O} \), over \( K \), is a proper subring of \( F \) such that it contains \( K \), and for \( z \in F \), either \( z \in \mathcal{O} \) or \( z^{-1} \in \mathcal{O} \).
Given a function field, we will later prove, in theorem (1.23), that there are infinitely many valuation rings for a given function field. As an example, consider the case of the rational function field $K(x)$. Given an irreducible polynomial $p(x) \in K[x]$, we have

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), p(x) \in K[x], p(x) \nmid g(x) \right\}$$  \hspace{1cm} (1.1.1)

which is a valuation ring of $K(x)$ for any irreducible polynomial $p(x)$. Since we know that there are infinitely many irreducible polynomials in any polynomial ring, and that (as a consequence) the above valuation rings are all distinct, we are lead to the conclusion that there are infinitely many valuation rings of a rational function field.

Now, returning to the general case of a function field, consider the set $\mathfrak{P} = O \setminus O^*$, where $O^*$ is the multiplicative group of units (i.e. elements that have an inverse) of a valuation ring $O$. The elements of this set in fact form an ideal of $O$. This is obvious if one considers an $x \in \mathfrak{P}$ and a $z \in O$. For these, we have that $xz \in \mathfrak{P}$, since if $xz$ had an inverse $y \in O$, then $zy$ would be in $O$, and also would be an inverse to $x$, a contradiction. Hence, $\mathfrak{P}$ is an ideal of $O$ and we will later prove that it is more than just any ideal.

I will now show a different approach to the concept of a valuation ring and to the ideal $\mathfrak{P} = O \setminus O^*$. The following draws from ideas proposed by Dr. Ambrus Pál but also from the book by Salvador [14].

**Definition 1.4.**

A **discrete valuation** of $F/K$ is a map $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

1. $v(x) = \infty$ if and only if $x = 0$
2. $v(xy) = v(x) + v(y)$ for any $x, y \in F$
3. $v(x + y) \geq \min\{v(x), v(y)\}$ for any $x, y \in F$
4. There exists an element $z \in F$ with $v(z) = 1$
5. $v(a) = 0 \ \forall a \in K, a \neq 0$

An example of a valuation is the $\deg(\cdot)$ function, for instance acting on a polynomial.
Take a discrete valuation \( v \) and consider the set
\[
\mathcal{O}_v = \{ x \in F : v(x) \geq 0 \}
\]

**Proposition 1.5.**
For any discrete valuation \( v \), \( \mathcal{O}_v \) is a valuation ring.

**Proof**
First of all, note that \( K \) is contained in \( \mathcal{O}_v \) by the fifth condition of a discrete valuation. From the second and third condition we conclude that it is also closed under addition and multiplication. Also, we have the same zero and identity element as in \( F \) since \( x = 0 \in \mathcal{O}_v \) since \( v(0) = \infty > 0 \), and also \( 1 \in \mathcal{O}_v \) since \( 1 \in K \). Hence \( \mathcal{O}_v \) is a subring of \( F \).

Now, if \( x \in F \) we have that \( v(xx^{-1}) = v(x) + v(x^{-1}) \) from which \( 0 = v(1) = v(x) + v(x^{-1}) \) and hence \( v(x^{-1}) = -v(x) \). So by considering an \( x \) such that \( x \notin \mathcal{O}_v \) it must be that \( v(x) < 0 \) from which \( v(x^{-1}) > 0 \) and so we have proven that \( x \notin \mathcal{O}_v \Rightarrow x^{-1} \in \mathcal{O}_v \), which concludes our proof. \( \square \)

Now, our next aim is to prove that
\[
m_v = \{ x \in F : v(x) > 0 \}
\]
is an ideal of \( \mathcal{O}_v \). It is clear that \( m_v \) is an additive subgroup of \( (\mathcal{O}_v, +) \). Also, consider an element \( x \in m_v \) and a \( y \in \mathcal{O}_v \). We have that \( v(xy) = v(x) + v(y) > 0 \) and so \( xy \in m_v \), which implies that \( m_v \) is indeed an ideal in \( \mathcal{O}_v \).

It is now beginning to become obvious that there exists a correspondence between the two representations of valuation rings \( (\mathcal{O}, +) \) and \( \mathcal{O}_v \) and our aim is to show that \( m_v \) is equivalent to \( \mathcal{P} = \mathcal{O} \setminus \mathcal{O}^* \) that we defined earlier. These will in fact turn out to be maximal ideals, and with the help of proposition (1.9) we will pinpoint the exact equivalence between these two ideals.

We showed that \( \mathcal{P} \) is an ideal of \( \mathcal{O} \) and it is clear that this is a unique maximal ideal as it encloses all elements of the valuation ring that are not units. We have that there is no proper ideal of \( \mathcal{O} \) that contains a unit, as in this case we would have that for \( x, x^{-1} \in \mathcal{O} \), if \( I \) is an ideal of \( \mathcal{O} \) and \( x \in I \) then \( xx^{-1} = 1 \in I \) which implies that \( I = \mathcal{O} \). Hence the following definition.

**Definition 1.6.**
The unique maximal ideal \( \mathcal{P} = \mathcal{O} \setminus \mathcal{O}^* \) is called a place of \( F/K \). Finally, we define \( |F| \) as the set of all places of the function field \( F \).
For example a place of the above $\mathcal{O}_p(x)$ in (1.1.1) is

$$\mathfrak{P}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x)|f(x), p(x) \nmid g(x) \right\}$$  \hspace{1cm} (1.1.2)

It is now clear that every valuation ring is in fact a local ring (see 6.5). Since every valuation ring has a unique ideal $\mathfrak{P}$, it follows that one term essentially determines the other. Because of this, we will from now on refer to the valuation ring $\mathcal{O}_\mathfrak{P}$ of the place $\mathfrak{P}$. We have shown that both $\mathcal{O}_\mathfrak{P}$ and $\mathcal{O}_v$ are both representations of valuation rings, and our aim now is to show that $m_v$ is a place of $\mathcal{O}_v$. This is clear though, by considering the following. If $x \in \mathcal{O}_v$, we have that $v(x) \geq 0$. If $v(x) = 0$ then $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$ and so $x^{-1} \in \mathcal{O}_v$. If $v(x) > 0$ then in a similar manner of thought, $v(x^{-1}) \notin \mathcal{O}_v$ and hence $x \in \mathcal{O}_v \setminus \mathcal{O}_v^*$, which shows that $m_v = \{x \in F : v(x) > 0\} = \mathcal{O}_v \setminus \mathcal{O}_v^*$. It readily follows that $m_v$ is the unique maximal proper ideal of $\mathcal{O}_v$ and hence a place. We will now use the $\mathfrak{P}, \mathcal{O}_\mathfrak{P}$ notation to prove a few facts, before we show how this notation is linked to the $m_v, \mathcal{O}_v$ one, with and after proposition (1.9).

The constant field of the function field $F$ is defined as the algebraic closure $\bar{K}$ of $K$ in $F$, that is to say $\bar{K} = \{y \in F : y$ algebraic over $K\}$. This is a sub-field of $F$.

The following two lemmas will allow us to prove proposition (1.9).

**Lemma 1.7.**

For a valuation ring $\mathcal{O}_\mathfrak{P}$ and constant field $\bar{K}$ we have that $\bar{K} \subseteq \mathcal{O}_\mathfrak{P}$ and $\bar{K} \cap \mathfrak{P} = \{0\}$

**Proof**

Assume $z \in \bar{K}$ and suppose that $z \notin \mathcal{O}_\mathfrak{P}$. Then it must be that $z^{-1} \in \mathcal{O}_\mathfrak{P}$. Since $z \in \bar{K}$ we have that $z^{-1}$ is algebraic over $K$ and so there exist $a_1, \ldots, a_r \in K$ such that

$$a_r(z^{-1})^r + \ldots + a_1z^{-1} + 1 = 0$$

and so

$$z^{-1}(a_r(z^{-1})^{r-1} + \ldots + a_1) = -1$$

Therefore $z = -(a_r(z^{-1})^{r-1} + \ldots + a_1) \in K[z^{-1}] \subseteq \mathcal{O}_\mathfrak{P}$, and so $z \in \mathcal{O}_\mathfrak{P}$, which shows that $\bar{K} \subseteq \mathcal{O}_\mathfrak{P}$. We showed that if $z \in \bar{K}$, then $z^{-1} \in \bar{K}$ and so since $\mathfrak{P}$ does not contain any units of $\mathcal{O}_\mathfrak{P}$ we conclude that $\bar{K} \cap \mathfrak{P} = \{0\}$. \qed
Lemma 1.8.
Given a valuation ring $\mathcal{O}_P$ and its corresponding unique maximal ideal $\mathfrak{p}$, of a function field $F/K$, then by taking a non zero $x \in \mathfrak{p}$ and $x_1, \ldots, x_n \in \mathfrak{p}$ such that $x = x_1$ and $x_i \in x_{i+1} \mathfrak{p}$ for $i = 1, \ldots, n - 1$, we have that $n \leq [F : K(x)] < \infty$.

Proof
Firstly, since $F$ is a finite extension of the rational function field $K(x)$ of one variable, we must have that $[F : K(x)] < \infty$. Suppose now $x_1, x_2, \ldots, x_n$ are not linearly independent over $K$. Then there exist $p_1(x), p_2(x), \ldots, p_n(x) \in K(x)$ such that $\sum_{i=1}^n p_i(x) x_i = 0$. We can assume $x$ does not divide all of the $p_i$. By putting $a_i = p_i(0)$ we can define $j \in \{1, \ldots, n\}$ for which $a_j \neq 0$ and $a_i = 0$ for all $i > j$, we see that

$$-p_j(x) = \sum_{i \neq j} p_i(x) x_i$$

with $p_i(x) \in \mathcal{O}_P \supseteq K(x)$ for $i = 1, \ldots, n$. Now, because of the above and the fact that $x = x_1 \in \mathfrak{p}$, we have that $x_i \in x_j \mathfrak{p}$ for $i < j$ and $p_i(x) = xg_i(x)$ when $i > j$ for some polynomial $g_i(x)$. From (1.1.3), by dividing by $x_j$ we see that

$$-p_j(x) = \sum_{i < j} p_i(x) \frac{x_i}{x_j} + \sum_{i > j} \frac{x}{x_j} g_i(x) x_i$$

from which we can conclude that $p_j(x) \in \mathfrak{p}$ as $\frac{x}{x_j}$ and $\frac{x}{x_j}$ are in $\mathfrak{p}$. We have that $p_j(x) = a_j + xg_j(x)$ and so both $xg_j(x)$ and $p_j(x)$ are in $\mathfrak{p}$ and $a_j$ is in $K$, so $a_j = p_j(x) - xg_j(x) \neq 0$ is in $\mathfrak{p} \cap K$ which is a contradiction to the previous lemma. Hence, $x_1, x_2, \ldots, x_n$ are linearly independent. \qed

Proposition 1.9.
For a valuation $\mathcal{O}_P$ of a function field $F/K$ we have that

1. $\mathfrak{p}$ is a principal ideal
2. If $\mathfrak{p} = (t)$ then any $z \in F$ has a unique representation of the form $z = t^n u$ for $n \in \mathbb{Z}$ and $u \in \mathcal{O}_P$.
3. $\mathcal{O}_P$ is a principal ideal domain, more precisely, if $\mathfrak{p} = (t)$ then any other ideal $I$ of $\mathcal{O}_P$ will be such that $I = (t^n)$ for some $n \in \mathbb{N}$.

Proof
1) Assume $\mathfrak{p}$ is not a principal ideal. Choose a non-zero $x_1 \in \mathfrak{p}$. Since $\mathfrak{p}$ is not principal, there exists an $x_2 \in \mathfrak{p} \setminus x_1 \mathfrak{p}$. Then $x_2 x_1^{-1} \notin \mathcal{O}_P$ and so $x_2^{-1} x_1 \in \mathfrak{p}$. 5
Hence \( x_1 \in x_2 \mathcal{P} \). Following this procedure we can generate an infinite set \( x_1, x_2, \ldots \) such that \( x_i \in x_{i+1} \mathcal{P} \) which contradicts the above lemma.

2) As \( z \) or \( z^{-1} \) is in \( \mathcal{O}_\mathcal{P} \) one can assume without loss of generality that \( z \in \mathcal{O}_\mathcal{P} \). If \( z^{-1} \in \mathcal{O}_\mathcal{P} \) then \( z \in \mathcal{O}_\mathcal{P}^* \) and so \( z = t^0z \). If on the other hand \( z \in \mathcal{P} \), then the sequence \( x_1 = z, x_2 = t^{m-1}, x_3 = t^{m-2}, \ldots, x_m = t \) is bounded by the above lemma and so we can choose a maximal \( m \) such that \( z \in t^m \mathcal{P} \). Hence write \( z = t^m u \) with \( u \in \mathcal{O}_\mathcal{P} \). It must be that \( u \) is a unit of our valuation ring since otherwise \( u \in \mathcal{P} = t \mathcal{O}_\mathcal{P} \) and so \( u = tw \) for some \( w \) in the valuation ring and then \( z = t^{m+1}w \in t^{m+1} \mathcal{O}_{\mathcal{P}} \) which contradicts the maximallity of \( m \).

3) Let \( I \) be a non-zero ideal of the valuation ring \( \mathcal{O}_{\mathcal{P}} \). If \( x \in I \) a non-zero element, then there exists an \( r \in \mathbb{N}^* \) and a \( u \in \mathcal{O}_{\mathcal{P}}^* \) such that \( x = t^r u \) and so \( t^r = xu^{-1} \in I \). Hence, the set \( X = \{ r \in \mathbb{N} : t^r I \} \) is non empty. Now, choose \( n = \min(X) \) the minimum element of the set \( X \). If \( y \in I, y \neq 0 \), we know that \( y = t^m w \) for some \( w \in \mathcal{O}_{\mathcal{P}}^*, m \in \mathbb{N}^* \) from the above. Since \( m \geq n \), we have that \( y = t^m t^{m-n} w \in t^n \mathcal{O}_{\mathcal{P}} \) and so \( I \subseteq t^n \mathcal{O}_{\mathcal{P}} \). It is also obvious that \( t^n \mathcal{O}_{\mathcal{P}} \subseteq I \) and so we get what we started off to prove.

The proofs of the above come from \([15]\).

After fixing a place \( \mathcal{P} \), an element \( z \in F \), we showed in the above proposition, has a representation of the form \( t^n u \) where \( u \in \mathcal{O}_{\mathcal{P}}^* \) and \( t \in \mathcal{P} \). Hence, one can define a discrete valuation as in the following.

**Lemma 1.10.**

For any place \( \mathcal{P} = (t) \) of a valuation ring \( \mathcal{O}_\mathcal{P} \), given any \( z \in F \) and \( z = t^n u \) where \( u \in \mathcal{O}_{\mathcal{P}}^* \), we have that \( v_{\mathcal{P}}(z) = v_{\mathcal{P}}(t^n u) = n \) is a discrete valuation.

**Proof**

All the conditions necessary for a discrete valuation are trivially met apart from the third one, the triangle inequality. Again though, this is clear from what follows. Consider \( x, y \in F \) with \( v_{\mathcal{P}}(x) = n_1 \) and \( v_{\mathcal{P}}(y) = n_2 \). Assume that \( n_1 < \infty \) and also, without loss of generality, that \( n_2 \leq n_1 \). Then \( x = t^{n_1} u_1 \) and \( y = t^{n_2} u_2 \), \( u_1, u_2 \) being units of the valuation ring \( \mathcal{O}_\mathcal{P} \). Then \( x + y = t^{n_2}(t^{n_1-n_2}u_1 + u_2) = t^{n_2} z \) with \( z \in \mathcal{O}_\mathcal{P} \). If \( z = 0 \) then \( v_{\mathcal{P}}(x + y) = \infty > \min(n_1, n_2) \), otherwise \( z = t^n u \) for some unit \( u \). Therefore \( v_{\mathcal{P}}(x + y) = v_{\mathcal{P}}(t^{n_2+n} u) = n_2 + n \geq n_2 \) and \( n \geq n_2 = \min(n_1, n_2) \). Hence write \( x = t^n u \) for some \( u \). Therefore \( v_{\mathcal{P}}(x + y) = v_{\mathcal{P}}(t^{n_2+n} u) = n_2 + n \geq n_2 \) and so we are done.

Trivially now, one can see that the two notations \( \mathcal{O}_v \) and \( \mathcal{O}_{\mathcal{P}} \) are in fact equivalent.
Lemma 1.11.
\( \mathcal{O}_\mathfrak{P} \) is a maximal proper sub-ring of \( F \).

Proof
Let \( z \in F \setminus \mathcal{O}_\mathfrak{P} \). Consider a \( y \in F \), such that \( v_\mathfrak{P}(yz^{-k}) \geq 0 \) for some \( k \in \mathbb{N} \setminus \{0\} \).
Hence, \( w = yz^{-k} \in \mathcal{O}_\mathfrak{P} \) and so \( y = wz^k \) which shows that \( F = \mathcal{O}_\mathfrak{P}[z] \) and so any valuation ring is maximal.

Definition 1.12.
Let \( z \in F \) and \( \mathfrak{P} \in |F| \).
- We say that \( \mathfrak{P} \) is a zero of \( z \) if and only if \( v_\mathfrak{P}(z) > 0 \)
- We say that \( \mathfrak{P} \) is a pole of \( z \) if and only if \( v_\mathfrak{P}(z) < 0 \)

If \( v_\mathfrak{P}(z) = m > 0 \) (or \( v_\mathfrak{P}(z) = -m < 0 \)) we say that \( \mathfrak{P} \) is a zero (pole) of order \( m \).

Definition 1.13.
The residue class ring is defined as \( F_\mathfrak{P} = \mathcal{O}_\mathfrak{P}/\mathfrak{P} \). The map \( F \to F_\mathfrak{P} \cup \{\infty\} \) such that \( z \mapsto (z + \mathfrak{P}) \) (or \( z \mapsto z(\mathfrak{P}) \)) is called the residue class map.

Since \( \mathfrak{P} \) is a maximal ideal, \( F_\mathfrak{P} \) is a field.

Considering lemma (1.7) we know that \( K \cap \mathfrak{P} = \{0\} \). We also know that \( K \subseteq \mathcal{O}_\mathfrak{P} \) for any valuation ring \( \mathcal{O}_\mathfrak{P} \). Hence, this gives that \( K \) injects into \( \mathcal{O}_\mathfrak{P} \) and also that \( \mathcal{O}_\mathfrak{P} \) surjects onto \( \mathcal{O}_\mathfrak{P}/\mathfrak{P} = \{x + \mathfrak{P} : x \in \mathcal{O}_\mathfrak{P}\} \). We can readily see now that every element of \( K \) will lie in a different class of \( \mathcal{O}_\mathfrak{P}/\mathfrak{P} \), since, if otherwise, we could consider \( x, y \in K \) such that \( x + \mathfrak{P} = y + \mathfrak{P} \). We would then have \( x - y \in \mathfrak{P} \) which is a contradiction since \( K \cap \mathfrak{P} = \{0\} \). Hence, \( F_\mathfrak{P} = \mathcal{O}_\mathfrak{P}/\mathfrak{P} \) is an extension of \( K \), in fact, we will show with proposition (1.15) that this extension is finite. We can define the following

Definition 1.14.
The degree of a place \( \mathfrak{P} \) is defined as \( \deg(\mathfrak{P}) = [F_\mathfrak{P} : K] \)

Proposition 1.15.
Given a place \( \mathfrak{P} \) of a function field \( F/K \) and a non-zero \( x \in \mathfrak{P} \), we have that \( \deg(\mathfrak{P}) \leq [F : K(x)] < \infty \).

Proof
That \( [F : K(x)] < \infty \) is trivial, since this is how a function field is defined. Hence, we need to show that \( \{z_i\}_{i=1}^n \in \mathcal{O}_\mathfrak{P} \) are linearly independent over \( K(x) \) if
their residue classes \( \{ z_i + \mathfrak{P} \}_{i=1}^n \in F_\mathfrak{P} \) are linearly independent over \( K \). Assume there exists a non-trivial relation \( \sum_{i=1}^n p_i(x)z_i = 0 \) where \( p_i(x) \in K(x) \). We can assume that not all \( p_i(x) \) are divisible by \( x \). Say \( p_i(x) = a_i + xg_i(x) \), \( a_i \in K \) not all zero. Now, we have that the residue class map sends the \( p_i(x) \) to the class containing \( a_i \) because \( x \in \mathfrak{P} \) and so in \( \mathcal{O}_\mathfrak{P}/\mathfrak{P} \) we have \( (xg_i(x) + \mathfrak{P}) = 0 \). Hence, by applying the residue class map to the above relation we get \( 0 = 0(\mathfrak{P}) = \sum_{i=1}^n p_i(x)(\mathfrak{P})z_i(\mathfrak{P}) = \sum_{i=1}^n a_i\mathfrak{P}z_i(\mathfrak{P}) \) which contradicts the linear independence of the \( \{ z_i(\mathfrak{P}) \}_{i=1}^n = \{ z_i + \mathfrak{P} \}_{i=1}^n \) over \( K \).

Lemma 1.16.

In a function field \( F/K \), if \( K \) is algebraically closed (\( K = \bar{K} \)), we have that \( \deg(\mathfrak{P}) = 1 \) for any place \( \mathfrak{P} \in |F| \).

Proof

Since \( \deg(\mathfrak{P}) = [\mathcal{O}_\mathfrak{P}/\mathfrak{P} : K] < \infty \), but also that any finite extension of \( K \) must be algebraic, we can readily see that \( [\mathcal{O}_\mathfrak{P}/\mathfrak{P} : K] = 1 \) since \( K = \bar{K} \) gives us \( \mathcal{O}_\mathfrak{P}/\mathfrak{P} = K \).

Theorem 1.17. (Going Up Theorem)

For a function field \( F/K \) and a sub-ring \( R \) such that \( K \subseteq R \subseteq F \), consider a proper ideal \( I \) of \( R \). There exists a place \( \mathfrak{P} \) of \( F \) such that \( I \subseteq \mathfrak{P} \) and \( R \subseteq \mathcal{O}_\mathfrak{P} \).

Proof

Following methods from [1] and [15], let

\[ \mathcal{F} = \{ S : S \text{ a sub-ring of } F \text{ with } R \subseteq S \text{ and } IS \neq S \} \]

It is clear that \( R \in \mathcal{F} \) and so \( \mathcal{F} \neq \{0\} \). We would like to work on proving the conditions necessary, for Zorn’s lemma to work on this set. That is that \( \mathcal{F} \) is a partially ordered set in which every chain has an upper bound. Zorn’s lemma will then provide us with a maximal element in \( \mathcal{F} \) which we will show is a valuation ring.

If \( \mathcal{F}' \subseteq \mathcal{F} \) is a totally ordered subset of \( \mathcal{F} \), then \( T = \bigcup \{ S : S \in \mathcal{F}' \} \) is a sub-ring of \( F \) such that \( R \subseteq T \subseteq F \). One needs to verify that \( IT \neq T \), which is made clear by the following. Assume not, then \( 1 \in IT \) so \( 1 = \sum_{k=1}^n a ks_k \) (definition of elements of \( IT \)) where \( a_k \in I \) and \( s_k \in T \). Since \( \mathcal{F}' \) is totally ordered, there exists an \( S_0 \in \mathcal{F}' \) with \( \{ s_i \}_{i=1}^n \subseteq S_0 \), which implies that \( 1 \in IS_0 \), a contradiction.

Now, by Zorn’s lemma there exists a ring \( \mathcal{O} \subseteq F \) which is maximal with respect
to the properties that $R \subseteq \mathcal{O} \subseteq F$ and $IO \neq \mathcal{O}$. As $I \neq \{0\}$ and $IO \neq \mathcal{O}$ we have that $\mathcal{O} \subseteq F$ and also that $I \subseteq \mathcal{O} \setminus \mathcal{O}^*$. Now, choose an element $z \in F \setminus \mathcal{O}$ such that neither $z$ nor $z^{-1}$ are in $\mathcal{O}$ (assume that one such exists). We have that $\mathcal{O} \subseteq \mathcal{O}[z]$ and so from the maximallity of $\mathcal{O}$, we conclude that $\mathcal{O}[z] \notin F$ and hence that $IO[z] = \mathcal{O}[z]$ and $IO[z^{-1}] = \mathcal{O}[z^{-1}]$. We can now choose elements $\{a_i\}_{i=0}^n$ and $\{b_j\}_{j=0}^m$ such that

$$1 = a_0 + a_1 z + \ldots + a_n z^n$$

$$1 = b_0 + b_1 z^{-1} + \ldots + b_m z^{-m}$$

and $n,m$ are minimal. By multiplying the first with $1 - b_0$ and the second with $a_n z^n$ and finally adding the results of both operations together, one gets $1 = c_0 + c_1 z + \ldots + c_n z^n$ where $c_0, \ldots, c_n \in IO$. This however contradicts the fact that $n$ is minimal and so either $z$ or $z^{-1}$ must be in $\mathcal{O}$, for any $z \in F$. Hence, we have proven that $\mathcal{O}$ is a valuation ring of $F/K$.

**Corollary 1.18.**

For every $z$ in a function field $F/K$ which is transcendental over $K$, we have that $z$ has at least one zero and one pole. More specifically, the set of places of $F$ is non empty.

**Proof**

From the definition of $z$, and following notation used in the previous theorem, we have that $K \subset K[z] = R$. Now, assume $I = zR$, an ideal of $R$. The previous theorem proves that there exists a valuation ring $\mathcal{O}_\mathfrak{p}$, and hence a place $\mathfrak{p}$, such that $z \in \mathfrak{p}$. This shows that $\mathfrak{p}$ is a zero of $z$. In a similar manner one shows that $z^{-1}$ has a zero $\mathfrak{p}'$, which is a pole for $z$, by the definition of discrete valuations

$(0 = v_\mathfrak{p}(zz^{-1}) = v_\mathfrak{p}(z) + v_\mathfrak{p}(z^{-1}) \Rightarrow v_\mathfrak{p}(z) = -v_\mathfrak{p}(z^{-1}))$.

To prove that a function field has infinitely many places one can use the following, which is know as the weak approximation theorem, which states that all the elements of a subset of a function field can be approximated (with discrete valuations used as a measure), to whatever accuracy is necessary, by a single element $x$.

**Theorem 1.19. (Weak Approximation Theorem)**

Given a function field $F/K$, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ pair wise distinct places of $F/K$, $x_1, \ldots, x_n \in F$ and $r_1, \ldots, r_n \in \mathbb{Z}$, there exists some $x \in F$ such that

$$v_{\mathfrak{p}_i}(x - x_i) = r_i \text{ for } i = 1, \ldots, n$$
**Proof**
As in the originating text of this proof [15], it is a good approach to attack this rather technical theorem by splitting the proof into sections/lemmas.

**Lemma 1.20.**
There exists $u \in F$ such that $v_1(u) > 0$ and $v_i(u) < 0$ for $i = 2, \ldots, n$.

**Proof**
We will prove this step by induction on $n$. Since valuation rings are maximal proper sub-rings of $F$ (See 1.11), we have that neither of the $\mathcal{O}_{q_i}$ for $i = 1, 2$ includes the other. We can therefore pick $y_1 \in \mathcal{O}_{q_1} \setminus \mathcal{O}_{q_2}$ and $y_2 \in \mathcal{O}_{q_2} \setminus \mathcal{O}_{q_1}$. Then we have that $v_1(y_1) \geq 0$ and $v_2(y_2) \geq 0$, but also that $v_1(y_2) < 0$ and $v_2(y_1) < 0$. By choosing $u = y_1/y_2$ we conclude the base case $n = 2$ since $u$ is such that $v_1(u) > 0$ and $v_2(u) < 0$. Now, for $n > 2$, assume that there exists a $y$ which satisfies the $n-1$ case. If $v_n(y) < 0$ we are finished. Otherwise, if $v_n(y) \geq 0$ we can choose $z$ with $v_1(z) > 0$ and $v_n(z) < 0$ and let $u = y + z^r$ for some $r \in \mathbb{N}^*$ which has $rv_i(z) \neq v_i(y) \forall i \in \{1, \ldots, n-1\}$. Hence, from the hypothesis we have that $v_1(u) \geq \min(v_1(y), rv_1(z)) > 0$ and $v_i(u) = \min(v_i(y), rv_i(z)) < 0 \forall i \in \{2, \ldots, n\}$. 

**Lemma 1.21.**
There exists $w \in F$ such that $v_1(w - 1) > r_1$ and $v_i(w) > r_i$ for $i = 2, \ldots, n$.

**Proof**
Choosing $u = y+z^r$ exactly as in the previous lemma, we can define $w = (1+u^s)^{-1}$. For this, there exists an $s \in \mathbb{N}$ such that $v_1(w - 1) = v_1(-u^s(1+u^s)^{-1}) = sv_1(u) > r_1$ and also that $v_i(w) = -v_i(1+u^s) = -sv_i(u) > r_i \forall i \in \{2, \ldots, n\}$ which concludes the proof of this lemma.

**Lemma 1.22.**
Given $y_1, \ldots, y_n \in F$, there exists $z \in F$ with $v_i(z - y_i) > r_i$ for $i = 1, \ldots, n$.

**Proof**
By choosing an $s \in \mathbb{Z}$ such that $v_i(y_j) \geq s$ for all $i, j \in \{1, \ldots, n\}$ we can use the second lemma to show that there exist $w_1, \ldots, w_n$ such that $v_i(w_i - 1) > r_i - s$ and $v_i(w_j) > r_i - s$ for $i \neq j$. Then a suitable choice of $z = \sum_{j=1}^n y_j w_j$ concludes the proof of the third lemma.

With these in mind, one can finally conclude the proof of the weak approximation
theorem as follows. In the third lemma, we showed the existence of a particular \( z \) which satisfies \( v_i(z - x_i) > r_i \) when \( i = 1, \ldots, n \). We can next choose \( z_i \in F \) such that \( v_i(z_i) = r_i \). Using the third lemma again, but on the set \( \{ z_i \} \), we derive that there exists a \( z' \) such that \( v_i(z' - z_i) > r_i \) for \( i = 1, \ldots, n \). It now follows that

\[
v_i(z') = v_i((z' - z_i) + z_i) = \min(v_i(z' - z_i), v_i(z_i)) = r_i
\]

And now by letting \( x = z + z' \) we have that

\[
v_i(x - x_i) = v_i((z - x_i) + z') = \min(v_i(z - x_i), v_i(z')) = r_i
\]

Which finishes our proof. \( \square \)

**Theorem 1.23.**

A function field has infinitely many places.

**Proof**

Assume there is a finite number of places \( \mathfrak{P}_1, \ldots, \mathfrak{P}_n \). From the weak approximation theorem above, we deduce that there exists a non-zero \( x \in F \) such that \( v_{\mathfrak{P}_i}(x) > 0 \) when \( i = 1, \ldots, n \). Which is a contradiction since in this case, \( x \) would have no poles, thus contradicting proposition (1.18). \( \square \)

**Proposition 1.24.**

Let \( F/K \) be a function field and \( \mathfrak{P}_1, \ldots, \mathfrak{P}_r \) be zeros of the element \( x \in F \). Then

\[
\sum_{i=1}^{r} v_{\mathfrak{P}_i}(x) \deg(\mathfrak{P}_i) \leq [F : K(x)]
\]

**Proof**

Let \( v_i = v_{\mathfrak{P}_i}, f_i = \deg(\mathfrak{P}_i) \) and \( e_i = v_i(x) \). For any \( i \), there is an element \( t_i \) such that \( v_i(t_i) = 1 \) and \( v_k(t_i) = 0 \) for all \( k \neq i \) (choose \( \mathfrak{P}_i = (t_i) \) for example). Since \( K \subseteq F_{\mathfrak{P}_i} \), we can choose a basis of \( F_{\mathfrak{P}_i} \) as a \( K \)-vector space, let this be \( s_{ij}(\mathfrak{P}_i), \ldots, s_{ijf_i}(\mathfrak{P}_i) \in F_{\mathfrak{P}_i} \), where \( s_{ij} \in \mathcal{O}_{\mathfrak{P}_i} \). By the weak approximation theorem (1.19), there exists \( z_{ij} \in F \) such that, for all \( i, j \), we have \( v_i(s_{ij} - z_{ij}) > 0 \) and \( v_k(z_{ij}) \geq e_k \) for \( k \neq i \). We aim now to prove that the elements \( t_i^a z_{ij} \), with \( 1 \leq i \leq r, 1 \leq j \leq f_i \) and \( 0 \leq a < e_i \), are linearly independent over \( K(x) \), as this will show that this basis has dimension \( \sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} v_{\mathfrak{P}_i}(x) \deg(\mathfrak{P}_i) \), which will conclude the proposition.
Assume the contrary. Then there exists a non trivial relation over \( K(x) \)

\[
\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \phi_{ija} t_i^a z_{ij} = 0 \quad (1.1.4)
\]

All the \( \phi_{ija} \in K[x] \) and without loss of generality we can assume that not all of them are divisible by \( x \). We then split the \( \phi_{ija} \) into the following two sets, depending on whether they are divisible by \( x \) or not. So, let \( k \in \{1, \ldots, r\} \) and \( c \in \{0, \ldots, e_k - 1\} \) such that \( x \) divides \( \phi_{kj}a \) when \( a < c \) for \( j \in \{1, \ldots, f_k\} \), and \( x \) does not divide \( \phi_{kjc} \) for \( j \in \{1, \ldots, f_k\} \). Now, multiplying (1.1.4) by \( t_k^c \) one obtains

\[
\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \phi_{ija} t_i^a t_k^c z_{ij} = 0 \quad (1.1.5)
\]

We have that all the summands in (1.1.5) are in \( \mathfrak{P}_k \) because of the following. When \( i = k \) and \( a < c \), and noting that \( v_k(\phi_{kj}a) \geq e_k \) since \( x \) divides \( \phi_{kj}a \), we have that \( v_k(\phi_{kj}a t_k^{a-c} z_{kj}) \geq e_k + a - c \geq e_k - c > 0 \). Now, when \( i = k \) and \( a > c \), one similarly gets \( v_k(\phi_{kj}a t_k^{a-c} z_{kj}) \geq a - c > 0 \). Whereas when \( i \neq k \) we have \( v_k(\phi_{ija} t_i^a t_k^c z_{ij}) = v_k(\phi_{ija}) + av_k(t_i) - cv_k(t_k) + v_k(z_{ij}) \geq 0 + 0 - c + e_k > 0 \). Hence, in all cases we have \( \sum_{j=1}^{f_k} \phi_{kjc} z_{kj} \in \mathfrak{P}_k \).

From the way they were defined, \( \phi_{kjc}(\mathfrak{P}_k) \in K \) and not all \( \phi_{kjc}(\mathfrak{P}_k) = 0 \) since we assumed \( x \) does not divide these for \( j \in \{1, \ldots, f_k\} \). Finally, we see that we now have a non trivial relation such that

\[
\sum_{j=1}^{f_k} \phi_{kjc}(\mathfrak{P}_k) z_{kj}(\mathfrak{P}_k) = 0
\]

over \( K \), which is a contradiction, since we assumed that \( \{z_{kj}(\mathfrak{P}_k)\}_{j=1}^{f_k} \) is a basis of \( F_{\mathfrak{P}_k}/K \).

\textbf{Remark 1.25.} 
This proposition shows the important fact that any element of a function field has a finite number of zeros and poles, since, a zero of \( x \) is a place \( \mathfrak{P} \) such that \( v_\mathfrak{P}(x) > 0 \). If otherwise, the left hand side of the inequality of the above proposition would sum to infinity! Likewise a zero of \( x^{-1} \) is a pole of \( x \), so any element has a finite number of poles as well.
To end the section on places, it is necessary to consider some facts about the rational function field \( K(x)/K \). Recalling our definition of (1.1.2), we see that the degree of any place of the rational function field is simply the degree of the monic irreducible to which it corresponds (in (1.1.2) this is called \( p(x) \)). I will prove that there exists one more place of the rational function field, the place at infinity \( \mathfrak{P}_\infty \), defined in (1.1.7), in which case, the degree is 1. The ideal \( \mathfrak{P}_\infty \) here is generated by \( \frac{1}{x} \).

**Proposition 1.26.**

There are no places of the rational function field \( K(x)/K \) other than the following

\[
\mathfrak{P}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \parallel f(x), p(x) \nmid g(x) \right\} \tag{1.1.6} \\
\mathfrak{P}_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \deg(f(x)) < \deg(g(x)) \right\} \tag{1.1.7}
\]

where \( p(x) \) is an arbitrary monic irreducible polynomial in \( K[x] \)

**Proof**

One can, in a straightforward manner, verify that the two above cases, do in fact represent places of the rational function field. What requires work though, is to show that any place of \( K(x)/K \) is of that form. Let \( \mathfrak{P} \) be any place in \( K(x) \) and let \( \mathcal{O}_\mathfrak{P} \) be its ring. We distinguish two cases

**Case 1**) Assume an \( x \in \mathcal{O}_\mathfrak{P} \). Since \( \mathcal{O}_\mathfrak{P} \) is a ring which contains \( K \), but also transcendental elements of the function field \( F \), it follows that it must contain \( K[x] \) as well. We proved that any place is a prime ideal in its valuation ring, so it must be that \( \mathfrak{P}' = \mathfrak{P} \cap K[x] \) is also a prime ideal, but in \( K[x] \). We here distinguish two cases though, either that \( \mathfrak{P}' \) will be the trivial ideal, or it will be generated by some irreducible polynomial \( f \in K[x] \). The first case represents an impossibility though, since then \( \mathfrak{P} \cap K[x] = \{0\} \) which implies that all \( \alpha \in K[x] \) are a unit in \( \mathcal{O}_\mathfrak{P} \), which in turn implies that \( K(x) \subseteq \mathcal{O}_\mathfrak{P} \), a contradiction. Hence, \( \mathfrak{P}' \) is generated by a polynomial \( f \). Now, assume \( g, h \in K[x] \), such that \( h \) is not divisible by \( f \). It is clear that \( h \notin \mathfrak{P} \) and so is a unit in \( \mathcal{O}_\mathfrak{P} \), from which, \( gh^{-1} \in \mathcal{O}_\mathfrak{P} \) and so \( \mathcal{O}_\mathfrak{P} \subseteq \mathcal{O}_{\mathfrak{P}} \). Choose a \( u \in K(x) \setminus \mathcal{O}_\mathfrak{P} \). Then one can write \( u = g/h \) where \( g, h \in K[x] \) are such that are coprime to each other, and \( h \) is divisible by \( f \). If \( u \) were in \( \mathcal{O}_\mathfrak{P} \), we would have \( h^{-1} = g^{-1}/u \), but this is impossible since \( h \notin \mathfrak{P} \Rightarrow h \) not a unit in \( \mathcal{O}_\mathfrak{P} \). Hence, when \( x \in \mathcal{O}_\mathfrak{P} \), \( \mathfrak{P} \) is of the form in (1.1.6).

**Case 2**) Assume now that \( x \notin \mathcal{O}_\mathfrak{P} \), we conclude that \( x^{-1} \in \mathcal{O}_\mathfrak{P} \) and so all
\[ \alpha \in \mathfrak{P}' = \mathfrak{P} \cap K[x^{-1}] \] are divisible by an irreducible \( f' \in K[x^{-1}] \). Now, since \( x^{-1} \) is not a unit in \( \mathcal{O}_\mathfrak{p} \), it must be in \( \mathfrak{P}' \) and is therefore divisible by \( f' \), from which we conclude that \( f' = x^{-1} \) and so \( \mathfrak{P} = \mathfrak{P}_\infty \), which concludes the proof. \( \square \)

### 1.2 Divisors

**Definition 1.27.**

Let \( D_F \) be the additive free abelian group generated by the places of \( F/K \). This is the divisor group of the function field \( F/K \). Every element of \( D_F \) is called a divisor of \( F/K \).

In more explanatory terms

\[
D \in D_F \text{ we have } D = \sum_{\mathfrak{P} \in |F|} n_{\mathfrak{P}} \mathfrak{P}
\]

which is a formal finite sum. A list of further consequences and definitions in relation to divisors is summed in the following.

For \( \Omega \in |F| \) and \( D = \sum n_{\mathfrak{P}} \mathfrak{P} \) we will frequently use the notation \( v_{\mathfrak{P}}(D) = n_{\mathfrak{P}} \). A prime divisor is of the form \( D = \mathfrak{P} \) where \( \mathfrak{P} \) is a place. For \( D = \sum n_{\mathfrak{P}} \mathfrak{P} \) and \( D' = \sum n'_{\mathfrak{P}} \mathfrak{P} \) we have

\[
D + D' = \sum (n_{\mathfrak{P}} + n'_{\mathfrak{P}}) \mathfrak{P}
\]

a direct consequence of the additive group structure of \( D_F \). The zero element of \( D_F \) is \( 0 = \sum r_{\mathfrak{P}} \mathfrak{P} \) where all \( r_{\mathfrak{P}} \) are 0. Also

\[
supp(D) = \{ \mathfrak{P} \in |F| : v_{\mathfrak{P}}(D) \neq 0 \}
\]

and it is clear now that \( D = \sum_{\mathfrak{P} \in supp(D)} v_{\mathfrak{P}}(D) \mathfrak{P} \). Also, \( D_1 \leq D_2 \) if and only if \( v_{\mathfrak{P}}(D_1) \leq v_{\mathfrak{P}}(D_2) \) for all \( \mathfrak{P} \in |F| \). Finally, we say that a divisor \( D \) is integral if \( D \geq 0 \), that is \( v_{\mathfrak{P}}(D) \geq 0 \) for all places \( \mathfrak{P} \).

We can naturally extend the notion of the degree of a place \( \mathfrak{P} \) to that of the degree of a divisor \( D \) by considering the same homomorphism as in the case involving places, but this time as \( \deg : D_F \to \mathbb{Z} \) such that

\[
\deg(D) = \sum_{\mathfrak{P} \in |F|} v_{\mathfrak{P}}(D) \deg(\mathfrak{P})
\]

In light of the above definition and lemma (1.16), when \( K \) is algebraically closed, the \( \deg(\cdot) \) map acting on a divisor is surjective onto \( \mathbb{Z} \). We will later show in
(3.4(iii)) that it’s also surjective when $K$ is finite, but this requires the Riemann-Roch theorem.

The expression $(x) = \sum_{\mathfrak{p} \in |F|} v_{\mathfrak{p}}(x)\mathfrak{p}$ is of great importance in our study of the class group of function fields. This in fact is an element of $\mathcal{D}_F$ because of remark (1.25), regarding the fact that any element of $F/K$ has a finite number of poles and zeros, which in turn makes $(x)$ satisfy the necessary condition that divisors must satisfy, that is that they are a sum of multiples of a finite number of places.

**Remark 1.28.**

In some of the bibliography, namely [14], the author decides to write divisors multiplicatively to more so fit the intuitive representation of writing things as a product of primes (places). In this case one would look at an element $\mathfrak{D} \in \mathcal{D}_F$ in the form of $\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{D})}$ where again, not all $v_{\mathfrak{p}}(\mathfrak{D})$ would be non zero. It is however customary, in books such as [1] which is one of the first to treat this topic in such a way, to use the additive notation and it is this that I chose to follow.

**Definition 1.29.**

The **principal divisor** of $x \in F/K$ is defined as

$$(x) = \sum_{\mathfrak{p} \in |F|} v_{\mathfrak{p}}(x)\mathfrak{p}$$

Also, denote by $Z$ the set of zeroes, and by $N$ the set of poles of $x$ in $|F|$. We define

$$(x)_0 = \sum_{\mathfrak{p} \in Z} v_{\mathfrak{p}}(x)\mathfrak{p}, \text{ the zero divisor of } x$$

$$(x)_\infty = \sum_{\mathfrak{p} \in N} -v_{\mathfrak{p}}(x)\mathfrak{p}, \text{ the pole divisor of } x$$

From this definition we can see that $(x) = 0$ if and only if $x \in K$. This follows directly from the definition of a principal divisor, but also from the definition of a discrete valuation, which is such that $v(k) = 0$ for all $k \in K$. Now, the principal divisors form a subset of $\mathcal{D}_F$, which can trivially be shown to be a subgroup.

**Definition 1.30.**

The **group of principal divisors** of $F/K$ is defined as the following subgroup of $\mathcal{D}_F$

$$\mathcal{P}_F = \{(x) \mid 0 \neq x \in F\}$$
From this definition, it is clear that the map $F^* \to \mathcal{P}_F$ is a homomorphism, which in fact has kernel the group $K^*$. In light of theorem (1.36), we will also be able to conclude the following short exact sequence

$$
\{0\} \to K^* \to F^* \to \mathcal{P}_F \to \{0\}
$$

(1.2.1)

**Definition 1.31.**
For a divisor $A$ let

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

In this definition, if $A = \sum n_i \mathfrak{P}_i - \sum m_j \mathfrak{Q}_j$, $\mathfrak{P}_i$ and $\mathfrak{Q}_j$ being places of $F$, one sees that $\mathcal{L}(A)$ is the set of elements of $F$ that have zeros of order greater than $n_i$, and poles of order less than $m_j$. Or, alternatively, $x \in \mathcal{L}(A)$ if and only if $v_{\mathfrak{P}}(x) \geq -v_{\mathfrak{P}}(A)$, $\forall \mathfrak{P} \in |F|$. In fact, we will show the following

**Lemma 1.32.**
For $A \in D_F$, we have that $\mathcal{L}(A)$ is a $K$-vector space.

**Proof**
If $a, b \in \mathcal{L}(A)$ and $x \in K$. For any place $\mathfrak{P}$, we have that $v_{\mathfrak{P}}(a+b) \geq \min(v_{\mathfrak{P}}(a), v_{\mathfrak{P}}(b)) \geq -v_{\mathfrak{P}}(A)$ from the definition of $\mathcal{L}(A)$. Also, $v_{\mathfrak{P}}(xa) = v_{\mathfrak{P}}(x) + v_{\mathfrak{P}}(a) \geq -v_{\mathfrak{P}}(A)$. Hence $a+b$ and $xa$ are in $\mathcal{L}(A)$ and so it is a $K$-vector space.

So now, one can define $\dim_K(\mathcal{L}(A))$ as the dimension of this vector space. This is called the **dimension of a divisor** $\dim(A)$, denoted for simplicity as $l(A)$.

We will now progressively prove information in relation to this vector space $\mathcal{L}(A)$, in aim of setting the background necessary for the later chapter on the theorem of Riemann-Roch, but also to prove theorem (1.36), which is fundamental in showing properties of the class group, which will be discussed later on.

**Lemma 1.33.**
For a function field $F/K$

i) $\mathcal{L}(0) = K$

ii) If $A \in D_F$ such that $A < 0$, then $\mathcal{L}(A) = \{0\}$

**Proof**
1) The fact that $K \subseteq \mathcal{L}(0)$ is trivial since $(x) = 0$ for all non-zero $x \in K$. Now, if $0 \neq x \in \mathcal{L}(0)$, then we have that $(x) \geq 0$ which is a contradiction, since this would imply that $x$ has no pole, going against what we proved in corollary (1.18), which in turn implies that $x \in K$. 

16
2) We come to the same contradiction in this case as well, since if a non-zero $x \in \mathcal{L}(\mathfrak{A})$ then $(x) \geq -\mathfrak{A} > 0$, implying $x$ has no poles. 

Lemma 1.34.
If $\mathfrak{A}, \mathfrak{B} \in D_F$ such that $\mathfrak{A} \leq \mathfrak{B}$, we have that

- $\mathcal{L}(\mathfrak{A}) \subseteq \mathcal{L}(\mathfrak{B})$ and also that
- $\dim(\mathcal{L}(\mathfrak{B})/\mathcal{L}(\mathfrak{A})) \leq \deg(\mathfrak{B}) - \deg(\mathfrak{A})$

Proof
The first is trivial since if $\mathfrak{A} \leq \mathfrak{B}$, it is clear how $\{x \in F : (x) \geq -\mathfrak{A}\} \subseteq \{x \in F : (x) \geq -\mathfrak{B}\}$ and so $\mathcal{L}(\mathfrak{A}) \subseteq \mathcal{L}(\mathfrak{B})$. For the second, we work by induction, relying on the fact that a divisor is a sum of only finitely many places. Assume, as a base case, that $\mathfrak{B} = \mathfrak{A} + P$ for some place $P$ of the function field $F/K$. We can choose an element $t \in F$ such that $v_P(t) = v_P(\mathfrak{B}) = v_P(\mathfrak{A}) + 1$. For any $x \in \mathcal{L}(\mathfrak{B})$ we have $v_P(x) \geq -v_P(\mathfrak{B}) = -v_P(t) \Rightarrow v_P(x) + v_P(t) \geq 0 \Rightarrow v_P(xt) \geq 0$ and so $xt \in \mathcal{O}_P$. So, we showed that there exists a map $\Psi : \mathcal{L}(\mathfrak{B}) \to F_P$ which maps $x \mapsto (xt)(P)$. Now, $x \in \ker(\Psi)$ if and only if $v_P(xt) > 0$, or in other words, if and only if $v_P(x) \geq -v_P(\mathfrak{A})$. Hence $\ker(\Psi) = \mathcal{L}(\mathfrak{A})$ and $\Psi$ induces a $K$-linear injective map $\mathcal{L}(\mathfrak{A})/\mathcal{L}(\mathfrak{B}) \to F_P$. Hence

$$\dim(\mathcal{L}(\mathfrak{A})/\mathcal{L}(\mathfrak{B})) \leq \dim(F_P) = \deg(\mathfrak{B}) - \deg(\mathfrak{A})$$

which concludes our proof.

Proposition 1.35.
For any $\mathfrak{A} \in D_F$, $\mathcal{L}(\mathfrak{A})$ is a finite dimensional $K$-vector space. In fact, If $\mathfrak{A} = \mathfrak{A}_+ - \mathfrak{A}_-$, with both $\mathfrak{A}_+ > 0$ and $\mathfrak{A}_- > 0$, we have that $\dim(\mathcal{L}(\mathfrak{A})) \leq \deg(\mathfrak{A}_+) + 1$.

Proof
Since $\mathcal{L}(\mathfrak{A}) \subseteq \mathcal{L}(\mathfrak{A}_+)$, it is sufficient to show that $\dim(\mathcal{L}(\mathfrak{A}_+)) \leq \deg(\mathfrak{A}_+) + 1$. Now, we know that $\mathfrak{A}_+ \geq 0$ so from the previous lemma, $\dim(\mathcal{L}(\mathfrak{A}_+)/\mathcal{L}(0)) \leq \deg(\mathfrak{A}_+)$. We also know that $\mathcal{L}(0) = K$ though, from (1.33), and so $\dim(\mathcal{L}(\mathfrak{A}_+)/\mathcal{L}(0)) = \dim(\mathcal{L}(\mathfrak{A}_+)/K) = \dim(\mathcal{L}(\mathfrak{A}_+)) - 1$, which completes our proof.

Theorem 1.36.
For a function field $F/K$, we have $\mathcal{P}_F \subseteq \ker(\deg(D_F))$, or in explanatory terms, principal divisors have degree zero. More specifically, one has, for $x \in F \setminus K$, that 

$$\deg((x)_0) = \deg((x)_\infty) = [F : K(x)]$$

17
Proof
We know that \((x)_{\infty} = \sum_{i=1}^{r} -v_{\mathfrak{P}_i}(x)\mathfrak{P}_i\), the \(\mathfrak{P}_i\) being places of the function field \(F/K\), which are in fact the poles of \(x\). We then have that \(\deg((x)_{\infty}) \leq [F : K(x)] = n\) from (1.24). Hence it remains to show that \(n \leq \deg((x)_{\infty})\) as well, to conclude the proof.

Choose a basis \(u_1, \ldots, u_n\) of \(F/K(x)\) and a \(C \in \mathcal{D}\) for which \((u)_{i} \geq -C\) for all \(i = 1, \ldots, n\). Then, \(l(k(x)_{\infty} + C) \geq n(k+1)\) for all \(0 \leq k \in \mathbb{N}\) since \(x^iu_j \in \mathcal{L}(k(x)_{\infty} + C)\) for \(0 \leq i \leq k\), and \(0 \leq j \leq n\) \((x^iu_j\) are linearly independent over \(K\) since the \(u_j\) are linearly independent over \(K(x)\)). Now, we can set \(c = \deg(C)\) and use the previous proposition to show that \(n(k+1) \leq l(k(x)_{\infty} + C) \leq k \deg((x)_{\infty}) + c + 1\).

Whence, for all \(k\)
\[
k \deg((x)_{\infty}) - n \geq n - c - 1
\]
This inequality is only possible when \(\deg((x)_{\infty}) \geq n\) which concludes that \(\deg((x)_{\infty}) = n\).

Now, since \((x)_{0} = (x^{-1})_{\infty}\) we have that
\[
\deg((x)_{0}) = \deg((x^{-1})_{\infty}) = [F : K(x^{-1})] = [F : K(x)]
\]
\[\square\]

1.3 Field Extensions and the Ramification Formula
In this section I will briefly mention some facts that will aid in finding places of algebraic extensions of a function field. An algebraic extension of a function field \(F/K\), is \(F'/K'\) such that \(F \subseteq F'\) is algebraic and \(K \subseteq K'\). An easy result which follows from this definition is that \(K'/K\) is in fact an algebraic extension as well. Material here draws primarily from chapter III in [15].

Definition 1.37.
A place \(\mathfrak{P}' \in |F'|\) is said to lie over \(\mathfrak{P} \in |F|\) if \(\mathfrak{P} \subseteq \mathfrak{P}'\). In this case, we write \(\mathfrak{P}'|\mathfrak{P}\).

One can now continue and prove that if \(\mathfrak{P}'|\mathfrak{P}\), we have that \(O_{\mathfrak{P}} \subseteq O_{\mathfrak{P}'}\) and also that there exists an integer \(e \geq 1\) such that for all \(x \in F\) we have \(v_{\mathfrak{P}'}(x) = ev_{\mathfrak{P}}(x)\). We denote this integer \(e(\mathfrak{P}'|\mathfrak{P}) = e\) as the ramification index of \(\mathfrak{P}'|\mathfrak{P}\) and
as with the ring of integers of a number field, we say that \( P' \mid P \) is ramified if \( e(P' \mid P) > 1 \). Finally, let \( f(P' \mid P) = [F'_P : F_P] \) be the relative degree of \( P' \) over \( P \).

In classic algebraic number theory, we aim to find which fractional ideals ramify or split completely into prime ideals. Working on quadratic number fields though, we have the advantage of only having to consider one or two prime ideals, say \( P_1, P_2 \), which multiplied together in the possible combinations of \( P_1, P_1 P_2, P_2 \) to subsequently match the inert, splits completely and ramified cases, give us our fractional ideal. This is due to the ramification formula, an equivalent for which, in the function field case, is given below

**Theorem 1.38. (Ramification Formula)**

Given a finite extension \( F'/K' \) of a function field \( F/K \), consider \( P \) a place of \( F/K \) and \( P_1, \ldots, P_m \) the places of \( F'/K' \) which lie over \( P \). If \( e_i = e(P_i \mid P) \) and \( f_i = f(P_i \mid P) \), we have that

\[
\sum_{i=1}^{m} e_i f_i = [F' : F]
\]

The proof of the above is not complicated, it involves writing \( [F' : K(x)] \) in two ways and finally, by equating the two results, the formula follows. The following theorem is not so much useful in its purpose of showing that a polynomial is irreducible, but more so in showing that for some specific places of a function field, there is a unique place which lies over each one of them, and this place ramifies to the degree of the polynomial which we are considering.

**Theorem 1.39. (Eisenstein’s Criterion)**

For a function field \( F/K \) and a polynomial

\[
\phi(T) = a_n T^n + \ldots a_1 T + a_0 \in F[T]
\]

assume that there is a place \( P \in |F| \) such that one of the following two hold

1. We have \( v_P(a_n) = 0 \) and \( v_P(a_i) \geq v_P(a_0) > 0 \) for \( i \in \{1, \ldots, n-1\} \) and \( \gcd(n, v_P(a_0)) = 1 \)
2. We have \( v_P(a_n) = 0 \) and \( v_P(a_i) \geq 0 \) for \( i \in \{1, \ldots, n-1\} \) and \( v_P(a_0) < 0 \) \( \gcd(n, v_P(a_0)) = 1 \)

We then have that \( \phi(T) \) is irreducible. Now, if \( F'/K' \) is an algebraic extension of \( F/K \) such that \( F' = F(y) \) where \( y \) is a root of \( \phi(T) \), we have that \( P \) has a unique extension \( P' \in |F'| \) such that \( e(P' \mid P) = n \) and \( f(P' \mid P) = 1 \).

These theorems will be put to use in the worked example at the end of this report.
1.4 The Class Group and the Class Number

The main interest of this report and the purpose of stating all the above have been to define the class group of a function field. This is a factor group, whose properties we will be studying extensively. We will however only be defining what the class group is here, it’s properties, including our main interest, the class number, will be discussed in later chapters.

**Definition 1.40.**
The divisor class group is a quotient group and is defined as

\[ \text{Cl}_F = \mathcal{D}_F / \mathcal{P}_F \]

In this case, since \( \mathcal{D}_F \) is a group under addition, we see that \( \text{Cl}_F = \mathcal{D}_F / \mathcal{P}_F = \{ (x) + \mathcal{O} : \mathcal{O} \in \mathcal{D}_F, (x) \in \mathcal{P}_F \} \). Using the degree function on a divisor of \( F/K \), one maps elements of \( \text{Cl}_F \) onto \( \mathbb{Z} \). In fact this map is a homomorphism. We define the kernel of this map as \( \text{Cl}_F^0 \) and we are lead to the following short exact sequence of homomorphisms

\[ \{0\} \rightarrow \text{Cl}_F^0 \rightarrow \text{Cl}_F \rightarrow \mathbb{Z} \rightarrow \{0\} \]

This sequence also tells us that the order of the class group is not finite and one can also prove that \( \text{Cl}_F \cong \text{Cl}_F^0 \oplus \mathbb{Z} \), a discussion for which lies in [14], pages 64, 65.

The image of the degree map acting on divisors is a normal subgroup of \( \mathbb{Z} \) and so it is of the form \( \rho \mathbb{Z} \). We will see more about this \( \rho \) in finite fields, namely in (3.4) and then in (4.4).

Now, if we restrict ourselves to the group \( \text{Cl}_F^0 \) and consider its order, which is called the class number and is denoted as \( h_F \) for a function field \( F/K \), we will see in later chapters that many properties arise around this number, especially in the case where our field of constants is a finite field.

The above exact sequence tells us that there are exactly \( h_F \) divisor classes \( (\in \text{Cl}_F) \) of degree \( n \), for any integer \( n \). I will be looking at methods for calculating \( h_F \) in chapter 4, as well as a proof that the class number is a finite number when the field of constants \( K \) is finite. This proof however requires the Riemann-Roch theorem, covered in a later chapter.

Considering the above exact sequence but also that in (1.2.1) we can generalise to the following

\[ \{0\} \rightarrow K^* \rightarrow F^* \rightarrow \mathcal{D}_F \rightarrow \text{Cl}_F \rightarrow \{0\} \]
A brief discussion follows on the importance of calculating the class number. In number fields, one considers a finite algebraic extension of $\mathbb{Q}$ and considers fractional ideals and principal fractional ideals, concepts which are equivalent to divisors and principal divisors respectively. Naturally the class group of a number field is defined as the quotient group of fractional ideals over the principal fractional ideals, and any algebraic number theory book will prove that in quadratic number fields, that is where the degree of the extension is 2, we have that the class number is finite. Even more so there is an important theorem which states that the ring of integers of a quadratic number field, that is elements of $\mathbb{Q}(\sqrt{d})$, where $d$ is a square free integer, which satisfy a polynomial in $\mathbb{Z}$, is a unique factorisation domain if and only if the class number is 1.

However, even though nothing equivalent exists in the function field case, we will see that the class number is linked to the zeta function of a function field which in turn provides us invaluable properties of the field and so of the algebraic curve which the field is defined by.

Finally, a table summarising advanced equivalences between number and function fields is included at the end of [3], the very basic ones though being the following.

<table>
<thead>
<tr>
<th>Number Fields</th>
<th>Function Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fractional ideal</td>
<td>Divisor</td>
</tr>
<tr>
<td>Principal fractional ideal</td>
<td>Principal divisor</td>
</tr>
<tr>
<td>Ideal class group</td>
<td>Divisor class group</td>
</tr>
</tbody>
</table>

2 The Riemann-Roch Theorem

2.1 Background and Statement of the Theorem

From the definition of $\mathcal{L}(\mathfrak{A})$ and that two divisors $\mathfrak{B}, \mathfrak{C} \in \mathcal{D}_F$ lie in the same divisor class of $\mathcal{C}l_F$ if and only if there exists an $x \in F$ such that $\mathfrak{A} = \mathfrak{B} + (x)$, we must note the following fact.

**Lemma 2.1.**

$\mathcal{L}(\mathfrak{A}) \neq \{0\}$ if and only if there is a divisor $\mathfrak{B}$ lying in the same class of the divisor class group as $\mathfrak{A}$, with $\mathfrak{B} \geq 0$.

Continuing from (1.34), we prove the following results
Lemma 2.2.
If $\mathfrak{A}, \mathfrak{A}' \in \mathcal{D}_F$ lie in the same class of $\mathcal{C}l_F$ then $\mathcal{L}(\mathfrak{A})$ and $\mathcal{L}(\mathfrak{A}')$ are isomorphic as $K$-vector spaces.

Proof
By assuming they lie in the same class of the divisor class group we can deduce that $\mathfrak{A} = \mathfrak{A}' + (z)$ for some non-zero $z \in F$. Now, consider the map $\phi : \mathcal{L}(\mathfrak{A}) \to F$ such that $\phi(x) = xz$. This $K$-linear map is such that $\text{Im}(\phi) \subseteq \mathcal{L}(\mathfrak{A}')$. We can define a map $\psi : \mathcal{L}(\mathfrak{A}') \to F$ such that $\psi(x) = xz^{-1}$. Then $\phi$ and $\psi$ are inverses and so $\phi$ is an isomorphism between $\mathcal{L}(\mathfrak{A})$ and $\mathcal{L}(\mathfrak{A}')$.

Lemma 2.3.
For a divisor $\mathfrak{A} \in \mathcal{D}_F$ such that $\deg(\mathfrak{A}) = 0$ the following two are equivalent

i) $\mathfrak{A}$ is principal

ii) $l(\mathfrak{A}) = 1$

Proof
(1) $\Rightarrow$ (2) If $\mathfrak{A} = (x)$ then we have that $x^{-1} \in \mathcal{L}(\mathfrak{A})$ which implies that $l(\mathfrak{A}) \geq 1$. From (2.1) we have that there exists a divisor $\mathfrak{B}$ in the same class as $\mathfrak{A}$ such that $\mathfrak{B} \geq 0$. Elements in the same class have the same dimension (see (2.2)) and degree, so since $\mathfrak{B} \geq 0$ and $\deg(\mathfrak{B}) = 0$ we have $\mathfrak{B} = 0$ and hence $l(\mathfrak{A}) = l(\mathfrak{B}) = l(0) = 1$.

(2) $\Rightarrow$ (1) Choose a non zero $z \in \mathcal{L}(\mathfrak{A})$. We have $(z) + \mathfrak{A} \geq 0$ and $\deg((z) + \mathfrak{A}) = 0$ and so like before, $\mathfrak{A} = -(z) = (z^{-1})$ which is principal.

Lemma 2.4.
For a divisor $\mathfrak{A}$ we have that if $\deg(\mathfrak{A}) \leq 0$ then $l(\mathfrak{A}) = 0$ except when $\mathfrak{A}$ and 0 lie in the same class of the divisor class group, in which case we have $l(\mathfrak{A}) = 1$.

Proof
For $\deg(\mathfrak{A}) < 0$ take an $x \in \mathcal{L}(\mathfrak{A})$, we then have that $\deg((x) + \mathfrak{A}) < 0$ since $\deg((x)) = 0$ from (1.36), but also that $\deg((x) + \mathfrak{A}) \geq 0$ from the definition of $\mathcal{L}(\mathfrak{A})$. Hence, in this case, $l(\mathfrak{A}) = 0$. If $\deg(\mathfrak{A}) = 0$ then for an $x \in \mathcal{L}(\mathfrak{A})$ we have $(x) + \mathfrak{A} \geq 0$ having degree 0 and thus that $(x) + \mathfrak{A} = 0$, so it must be that $\mathfrak{A}$ lies in the zero class of the divisor class group. Now, we have that $\mathcal{L}(0) = K$ since $x \in \mathcal{L}(0)$ means that $x$ has no poles and so $x \in K$, which finally implies that $l(\mathfrak{A}) = 1$.  

22
Lemma 2.5.
There is a $\gamma \in \mathbb{Z}$, such that for every divisor $A$ of a function field $F/K$, the following holds

$$\deg(A) - l(A) \leq \gamma$$

Proof
From (1.34) we conclude that if $A_1, A_2 \in D_F$ such that $A_1 \leq A_2$, then $\deg(A_1) - l(A_1) \leq \deg(A_2) - l(A_2)$. Fix an $x \in F \setminus K$. For $B = (x)_\infty$, there is a $C \geq 0 \in D_F$ such that $l(kB + C) \geq (k + 1)\deg(B)$ for all $k \geq 0$, just like in the proof of (1.36).

Now, using (1.34) again, we conclude that $l(kB + C) \leq l(kB) + \deg(C)$. And now we can combine the two results to get, for all $k > 0$

$$l(kB) \geq (k + 1)\deg(B) - \deg(C)$$
$$= \deg(kB) + ([F : K(x)] - \deg(C))$$
$$= \deg(kB) + \gamma$$

Our aim now it to show that this works when we have $A \in D_F$ rather than $kB$. To do this we will prove that given a divisor $A$, there exist $A_1, D \in D_F$ and $k \in \mathbb{Z}$ such that $A_1, D$ lie in the same class of the divisor class group $Cl_F$, and also $A \leq A_1$ and $D \leq kB$. This is clear though by considering the following. Choose $A_1 \geq A$ such that $A_1 \geq 0$. We then have $l(kB - A_1) \geq l(kB) - \deg(A_1) \geq \deg(kB) - \gamma - \deg(A_1) > 0$, which holds when $k$ is sufficiently large. Whence there is a non-zero $z \in \mathcal{L}(kB - A_1)$. We can now set $D = A_1 - (z)$ and we can easily verify that $A_1$ and $D$ lie in the same class of $Cl_F$ and also that $D \leq A_1 - (A_1 - kB) = kB$ which was the other requirement.

Hence we can now complete our proof by using the above claim and the following.

$$\deg(A) - l(A) \leq \deg(A_1) - l(A_1)$$
$$= \deg(D) - l(D)$$
$$\leq \deg(kB) - l(kB)$$
$$\leq \gamma$$

The first inequality follows from (1.34), the second equality from lemma (2.2). The third inequality follows from (1.34) again since $D \leq kB$. \qed
Definition 2.6.
The **genus of a function field** $F/K$ is defined as

$$g = \max \{ \deg(\mathfrak{A}) - l(\mathfrak{A}) + 1 : \mathfrak{A} \in \mathcal{D}_F \}$$

The genus is a non-negative integer which is constant for every function field $F/K$. It is a number of great importance in the study of fields of algebraic curves, not only from a number theoretical point of view, but also geometric and topological. This definition is not very helpful though, in a sense of providing a simple way for computing the genus for a given function field, or even understanding what it is. One can resort though, to a definition of the genus which originates from topology; this says that the genus is simply the number of holes a topological space has, the standard example being the doughnut, which has genus 1.

**Theorem 2.7. (Riemann's Theorem)**
For a function field $F/K$, we have that for any divisor $\mathfrak{A} \in \mathcal{D}_F$

$$l(\mathfrak{A}) \geq \deg(\mathfrak{A}) - g + 1$$

**Proof**
Follows directly from the definition of the genus $g$ and lemma (2.5).

**Corollary 2.8.**
There is an integer $c$, depending on the function field $F/K$, such that whenever $\deg(\mathfrak{A}) \geq c$, for $\mathfrak{A} \in \mathcal{D}_F$, we have

$$\dim(\mathfrak{A}) = \deg(\mathfrak{A}) + 1 - g$$

**Proof**
Choose a divisor $\mathfrak{B}$ such that $g = \deg(\mathfrak{B}) - \dim(\mathfrak{B}) + 1$, note that this exists by the definition of the genus. Now, set $c = \deg(\mathfrak{B}) + g$. If $\deg(\mathfrak{A}) \geq c$, we have

$$\dim(\mathfrak{A} - \mathfrak{B}) \geq \deg(\mathfrak{A} - \mathfrak{B}) + 1 - g \geq - \deg(\mathfrak{B}) + 1 - g \geq 1$$

Hence, we can choose an $0 \neq x \in \mathcal{L}(\mathfrak{A} - \mathfrak{B})$. Now, let $\mathfrak{W} = \mathfrak{A} + (x) \geq \mathfrak{B}$ and consider the following

\[
\begin{align*}
\deg(\mathfrak{A}) - \dim(\mathfrak{A}) &= \deg(\mathfrak{W}) - \dim(\mathfrak{W}) \quad (2.1.1) \\
&\geq \deg(\mathfrak{B}) - \dim(\mathfrak{B}) \quad (2.1.2) \\
&= g - 1
\end{align*}
\]
where (2.1.1) follows because \(A, W\) lie in the same class of the divisor class group, and (2.1.2) because of \(1.34\). Now the result follows as an application of Riemann’s theorem.

**Theorem 2.9. (Riemann-Roch theorem)**

For the genus \(g_F \in \mathbb{N}\) and a divisor class \([C] \in \text{Cl}_F\) of a function field \(F/K\), we have that for all \(C \in [C]\) and \(A \in D_F\)

\[
l(A) = \deg(A) - g_F + 1 + l(C - A)
\]

This divisor class \([C] \in \text{Cl}_F\) is called the **canonical class**, and it is formed by a special set of divisors which have properties in relation to Weil differentials, a construction which one would use to provide a simple proof of the Riemann-Roch theorem.

**2.2 Corollaries and Uses of the Theorem**

A significant to our study set of corollaries can be deduced from the Riemann-Roch theorem. Starting from (2.9), if we replace \(A = 0\), we get

**Corollary 2.10.**

For any \(C \in C\), \(l(C) = g\)

In a similar manner if we replace \(A = C \in C\), where \(C\) is the canonical class, we conclude that

**Corollary 2.11.**

For any \(C \in C\), \(\deg(C) = 2g - 2\)

From the two above, we can prove further results, which classify the elements of the canonical class.

**Corollary 2.12.**

A divisor \(A\) is in the canonical divisor class \(C\) if and only if \(\deg(A) = 2g - 2\) and \(l(A) \geq g\)

**Proof**

We have proven the if part of this statement in (2.11). For the only if, we have that for a chosen \(W \in C\), \(g \leq l(A) = \deg(A) + 1 - g + l(W - A) = g - 1 + l(W - A)\) which in turn implies \(l(W - A) \geq 1\). Now, since \(\deg(W - A) = 0\) we have from (2.3) that \(W - A = (x)\) for some \(x \in F\) and so they lie in the same divisor class. Hence, \(A\) has \(\deg(A) = 2g - 2\) and \(l(A) \geq g\). 

\[\square\]
Corollary 2.13.
For any $\mathfrak{A}$, such that $\deg(\mathfrak{A}) \geq 2g - 2$ we have that $l(\mathfrak{A}) = \deg(\mathfrak{A}) - g + 1$, except in the case that $\deg(\mathfrak{A}) = 2g - 2$ and $\mathfrak{A} \in \mathcal{C}$.

Proof
Since $\deg(\mathfrak{A}) \geq 2g - 2$ we have that for $\mathcal{C} \in \mathcal{C}$, $\deg(\mathcal{C} - \mathfrak{A}) \leq 0$ and the result follows from (2.4).

Many further interesting results come from the Riemann-Roch theorem, such as the Strong Approximation Theorem, but also the Weierstrass Gap Theorem to name a few. These are covered in [15].

2.3 Rational Function Fields and Elliptic Curves

For the case of the rational function field $K(x)/K$, we conclude that

Proposition 2.14.
For a function field $F/K$, the following two are equivalent

i) $F/K$ is a rational function field, i.e. $F = K(x)$.

ii) $F/K$ has genus $g_F = 0$ and there exists a divisor $\mathfrak{A}$ with $\deg(\mathfrak{A}) = 1$

Proof
(1) $\Rightarrow$ (2) Consider the place at infinity $\mathfrak{P}_\infty$, which is generated by $\frac{1}{x}$. For any integer $r \geq 0$, we have that $1, x, \ldots, x^r \in L(r\mathfrak{P}_\infty)$ (why?). Hence, by (2.8) and for a suitably large $r$ we have

$$r + 1 \leq \dim(r\mathfrak{P}_\infty) = \deg(r\mathfrak{P}_\infty) + 1 - g_F = r + 1 - g_F$$

Which implies that $g_F \leq 0$ and so that $g_F = 0$.

(2) $\Rightarrow$ (1) We have $\deg(\mathfrak{A}) \geq 2g_F - 1$ and so that $\dim(\mathfrak{A}) = \deg(\mathfrak{A}) + 1 - g_F = 2$ from (2.13). Now, (2.1) gives us that there exists a $\mathfrak{B} \geq 0$ such that $\mathfrak{A}, \mathfrak{B}$ lie in the same class of the divisor class group. This gives that $\dim(\mathfrak{B}) = 2$ and so that there exists an $x \in L(\mathfrak{B}) \setminus K$, so $(x) \neq 0$ and we have $(x) + \mathfrak{B} \geq 0$ $\Rightarrow (x)_0 - (x)_\infty + \mathfrak{B} \geq 0$. However, we have that $\deg(\mathfrak{B}) = 1$ and since $\mathfrak{B} \geq 0$ this is only possible if $\mathfrak{B} = (x)_\infty$ (why?). However, we have from (1.36) that $[F: K(x)] = \deg((x)_\infty) = \deg(\mathfrak{B}) = 1$ and so $F = K(x)$.

Lemma 2.15.
Every function field $F/K$ of genus $g = 0$ has class number $h_F = 1$. 


**Proof**

We want to show that every divisor $\mathfrak{A}$ with $\text{deg}(\mathfrak{A}) = 0$ is principal. To do this, we consider the fact that $2g - 2 = -2 < 0$ and hence from corollary (2.13) of the Riemann-Roch Theorem, we have that $l(\mathfrak{A}) = \text{deg}(\mathfrak{A}) + 1 - g$. Hence we get that $l(\mathfrak{A}) = 1$. Due to this result, we see that there exists an $x \in F$ such that $(x) \geq -\mathfrak{A}$, but by considering the fact that principal divisors have degree 0 and also the assumption that $\text{deg}(\mathfrak{A}) = 0$ we must have that $\mathfrak{A} = -(x) = (x^{-1})$ ($x^{-1}$ being the inverse of $(x)$ in the additive group of divisors) which concludes our efforts to show that $\mathfrak{A}$ is indeed principal. \qed

The above classify some of the genus 0 curves and our aim now is to do something similar for $g_F = 1$.

**Definition 2.16.**

An elliptic function field $F/K$ is such that the following two hold

i) $g_F = 1$

ii) There exists a divisor of degree 1

Condition two will become trivial in function fields of finite constant field by Schmidt’s theorem (4.4). An example of an elliptic function field is included as a worked example at the end of this report. However, we will need to prove some properties of genus 1 curves to be able to study the class numbers of elliptic function fields.

**Lemma 2.17.**

For a function field $F/K$ such that $g_F = 1$ we have that the canonical class in the divisor class group is the zero class.

**Proof**

The claim is yet another corollary of the Riemann-Roch theorem. It follows by (2.10) and (2.11) that $l(\mathcal{C}) = 1$ and $\text{deg}(\mathcal{C}) = 0$ and hence we can use (2.4) to get that $\mathcal{C} = [0]$. \qed

**Lemma 2.18.**

For a function field $F/K$ such that $g_F = 1$, every class in the divisor class group which consists of divisors of degree 1 contains a unique place of degree 1. In other words, the map

$$
\phi : |F| \rightarrow \mathcal{Cl}_F^1
$$

$$
\mathfrak{p} \mapsto [\mathfrak{p}]
$$

is a bijection.
Proof
The first part of the proof is to show that the map is surjective. For \( \mathfrak{A} \in \mathcal{D}_F \) such that \( \deg(\mathfrak{A}) = 1 \), we have, using (2.17) and the Riemann-Roch theorem, that

\[
I(\mathfrak{A}) - I(-\mathfrak{A}) = \deg(\mathfrak{A}) = 1
\]

However, \( I(-\mathfrak{A}) = 0 \) since \( \deg(-\mathfrak{A}) = -1 < 0 \) and we can use (2.4). Hence, we get \( I(\mathfrak{A}) = 1 \) and so there exists an \( x \in \mathcal{L}(\mathfrak{A}) \) such that \( \mathcal{D}_x = (x) + \mathfrak{A} \geq 0 \). But we also have that \( \deg(\mathcal{D}_x) = 1 \) and so it must be that \( \mathcal{D}_x = \mathfrak{P}_x \), a place of degree 1 (an effective divisor of degree 1 must be a place).

Now, to prove that it is injective, consider two places \( \mathfrak{P}_1, \mathfrak{P}_2 \in [\mathfrak{A}] \) such that

\[
\mathfrak{P}_1 + (x_1) = \mathfrak{A} \\
\mathfrak{P}_2 + (x_2) = \mathfrak{A}
\]

for \( x_1, x_2 \in \mathcal{L}(\mathfrak{A}) \). Hence we get \( \mathfrak{P}_1 = \mathfrak{P}_2 + (x_2 - x_1) \). However, we have that \( I(\mathfrak{A}) = 1 \) and so \( \mathcal{L}(\mathfrak{A}) = K \) which implies that \( x_2 - x_1 \in K \). Thus, \( \mathfrak{P}_1 = \mathfrak{P}_2 \). \( \square \)

3 Finite Constant Field and the Zeta Function
Throughout this chapter, we will work with function fields \( F/K \) such that the field of constants \( \overline{K} \) is finite.

Let \( A_n \) be the number of integral divisors \( \mathcal{D} \) of degree \( n \), that is

\[
A_n = |\{ \mathcal{D} \in \mathcal{D}_F : \mathcal{D} \geq 0, \deg(\mathcal{D}) = n \}|
\]

Also, let

\[
\rho = \min\{ n \in \mathbb{N} : \mathcal{D} \in \mathcal{D}_F, \deg(\mathcal{D}) = n \}
\]

One needs to recall here that \( \rho \mathbb{Z} \) generates the image of the degree map acting on divisors. In fact, we will later prove that \( \rho = 1 \).

3.1 The Finiteness of the Class Number
Lemma 3.1.
For any \( n \geq 0, n \in \mathbb{N} \), we have that \( A_n \) is finite.
Proof Since a positive divisor is a sum of places, we can restrict ourselves to proving the finiteness of the set \( \{ \mathfrak{P} \in |F| : \deg(\mathfrak{P}) \leq n \} \). Choose an \( x \in F \setminus \mathbb{F}_q \) and define \( S_0 = \{ \mathfrak{P}_0 \in |\mathbb{F}_q(x)| : \deg(\mathfrak{P}_0) \leq n \} \). We have that \( \mathfrak{P} \cap \mathbb{F}_q(x) \in S_0 \) for any place \( \mathfrak{P} \). Also, we have that any \( \mathfrak{P}_0 \in S_0 \) has only finitely many extensions in \( F \), since \( F/\mathbb{F}_q(x) \) is finite algebraic. It suffices to show that \( S_0 \) is finite. This is clear though since all, apart from one, of the places of \( \mathbb{F}_q(x) \) correspond to irreducible polynomials in \( \mathbb{F}_q[x] \) (see 1.26) of degree up to \( n \). And since there are finitely many of these (the coefficient field \( \mathbb{F}_q \) is finite!), the result follows.

Theorem 3.2. For a function field \( F \) of finite constant field \( \bar{K} = \mathbb{F}_q \), the class number \( h_F = |\mathcal{Cl}_F| = \{ [\mathcal{C}] \in \mathcal{Cl}_F : \deg([\mathcal{C}]) = 0 \} \) is a finite number.

Proof By choosing a divisor \( \mathcal{D} \in \mathcal{D}_F \) of degree \( n \geq g \) where \( g \) is the genus, we can consider the set of divisor classes \( C^n_F = \{ [\mathcal{C}] \in \mathcal{Cl}_F : \deg([\mathcal{C}]) = n \} \). Now, it is easy to see that the map

\[
\begin{cases}
\mathcal{Cl}_F^0 & \rightarrow C^n_F \\
[\mathfrak{A}] & \mapsto [\mathfrak{A} + \mathcal{C}]
\end{cases}
\]

is a bijection and hence we need to only work on proving that \( C^n_F \) is finite.

For a divisor class \( [\mathcal{C}] \in \mathcal{Cl}_F \), we have, from \( \deg([\mathcal{C}]) = n \geq g \) and the Riemann-Roch theorem, that \( l([\mathcal{C}]) \geq n + 1 - g \geq 1 \) and so \( \mathcal{L}([\mathcal{C}]) \neq \{0\} \) and so by (2.1), there exists a divisor in \([\mathcal{C}]\) of degree \( \geq 0 \). But, by the the previous lemma, there exist only finitely many divisors of degree \( n \).

3.2 The Zeta Function in Function Fields

For a prime divisor (a place) \( \mathfrak{P} \) of \( F/K \), define the cardinality of the residue class field \( \mathcal{O}_{\mathfrak{P}}/\mathfrak{P} \) as \( N(\mathfrak{P}) \). The notion of \( N(\cdot) \) can be extended to act on a divisor in a natural way as shown below in (3.2.1), assuming the fact that for distinct places \( \mathfrak{P}_1, \mathfrak{P}_2 \) we have \( N(\mathfrak{P}_1 + \mathfrak{P}_2) = N(\mathfrak{P}_1)N(\mathfrak{P}_2) \). This last assertion may seem counterintuitive, since one usually has \( N(ab) = N(a)N(b) \) for a norm \( N(\cdot) \) and nothing more can usually be said in generality. However this is justified from our decision to write divisors additively, explained in remark (1.28). Should we have chosen to write divisors in the form \( \mathcal{D} = \prod_{\mathfrak{P}} \mathfrak{P}^{v\mathfrak{P}(\mathcal{D})} \) then our norm would maintain its usual property.
Definition 3.3.

The zeta function on $F$ is defined as

$$
\zeta_F(s) = \sum_{D \geq 0} \frac{1}{(N(D))^s}
$$

Note now that since we have that $K$ is finite, then it is such that $K = \mathbb{F}_q$ where $q = p^r$ for some prime integer $p$. Hence, we have that $|K| = q$ and so, since $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ is a $K$-vector space, $N(\mathfrak{p}) = |\mathcal{O}_\mathfrak{p}/\mathfrak{p}| = q^{\deg(\mathfrak{p})}$. Now, for $\mathfrak{D} = \sum_{\mathfrak{p} \in |F|} v_{\mathfrak{p}}(\mathfrak{D}) \mathfrak{p}$, it holds that

$$
N(\mathfrak{D}) = N \left( \sum_{\mathfrak{p} \in |F|} v_{\mathfrak{p}}(\mathfrak{D}) \mathfrak{p} \right) = \prod_{\mathfrak{p} \in |F|} \left(q^{\deg(\mathfrak{p})}\right)^{v_{\mathfrak{p}}(\mathfrak{D})} \quad (3.2.1)
$$

and so the zeta function can be written as

$$
\zeta_F(s) = \sum_{D \geq 0} q^{-\deg(\mathfrak{D})s} \quad (3.2.2)
$$

Our next aim is to show that the zeta function converges when the real part of $s$ is greater than 1. This however requires a few lemmas, which in fact, will be used later on as well.

Lemma 3.4.

1. If $\rho \nmid n$ then $A_n = 0$

2. For a fixed class $[\mathfrak{C}]$ in the divisor class group $\text{Cl}_F$, we have that

$$
|\{\mathfrak{A} \in [\mathfrak{C}] : \mathfrak{A} \geq 0\}| = \frac{q^{l([\mathfrak{C}])} - 1}{q - 1}
$$

3. For $n > 2g - 2$ and $\rho | n$, where $g$ is the genus of $F/K$, and $h_F$ is the class number

$$
A_n = h_F \frac{q^{n+1} - 1}{q - 1}
$$
Proof

1) This is a consequence of the image of the degree map being a normal subgroup of \( \mathbb{Z} \) and thus being of the form \( \rho \mathbb{Z} \), as I discussed after definition (1.40).

2) From the conditions, we have that \( \mathfrak{A} = (x) + [\mathcal{C}] \) for some \( x \in F \) with \( (x) \geq -[\mathcal{C}] \), or in other words, \( x \in \mathfrak{L}([\mathcal{C}]) \setminus \{0\} \). Now, since \( \mathfrak{L}([\mathcal{C}]) \) is a \( K \)-vector space and \( K \) has \( q \) elements, we can deduce that there exist exactly \( q^{l([\mathcal{C}])} - 1 \) elements in \( \mathfrak{L}([\mathcal{C}]) \setminus \{0\} \). Also, two elements of this set give rise to the same divisor if and only if their difference is a constant \( 0 \neq \alpha \in K = \mathbb{F}_q \). The second statement gives rise to \( q - 1 \) possible such combinations, and hence the result follows.

3) From remarks we saw after the definition of the class number, there are \( h_F \) divisor classes of degree \( n \). By the previous part of this lemma and corollary (2.13) of the Riemann-Roch theorem, we get that if \( [\mathcal{C}_i] \), for \( i = 1, \ldots, h_F \), are the divisor classes, then

\[
|\{ \mathfrak{A} \in [\mathcal{C}_i] : \mathfrak{A} \geq 0 \}| = \frac{q^{l([\mathcal{C}_i])} - 1}{q - 1} = \frac{q^{n+1-g} - 1}{q - 1}
\]

The result is now clear, since for any divisor \( \mathfrak{D} \) of degree \( n \), we know that it must lie within one of the \( [\mathcal{C}_i] \) and hence

\[
A_n = \sum_{i=1}^{h_F} |\{ \mathfrak{A} \in [\mathcal{C}_i] : \mathfrak{A} \geq 0 \}| = h_F \frac{q^{n+1-g} - 1}{q - 1}
\]

Lemma 3.5.

The series \( \zeta_F(s) \) converges absolutely and uniformly in compact (closed and bounded) subsets of \( \{ s \in \mathbb{C} : \text{Re}(s) > 1 \} \).

Proof

Using the definitions from above

\[
\zeta_F(s) = \sum_{\mathfrak{D} \geq 0} \frac{1}{q^{\deg(\mathfrak{D})} s} = \sum_{n=0}^{\infty} A_{\rho n} q^{-n \rho s}
\]

\[
= \sum_{n=0}^{t} A_{\rho n} q^{-n \rho s} + \sum_{n=t+1}^{\infty} A_{\rho n} q^{-n \rho s}
\]

31
where \( t = \frac{2g-2}{\rho} \). Note that \( \rho \mid 2g-2 \) since \( \text{deg}(\mathcal{C}) = 2g-2 \), where \( \mathcal{C} \) is the canonical class, and this number lies in \( \rho \mathbb{Z} \), the image of the \( \text{deg}() \) map.

Now, applying lemma (3.4) part 2 on the second element of the above sum, we get

\[
\sum_{n=t+1}^{\infty} A_{\rho n} q^{-n \rho s} = \frac{h_F}{q-1} \sum_{n=t+1}^{\infty} (q^{n \rho - g+1} - 1) q^{-n \rho s}
\]

In our attempt to prove convergence of the infinite sum, the following finally gives us the result we need. Consider the standard complex norm, and that \( s = a + ib \), with \( a, b \in \mathbb{R} \)

\[
\sum_{n=t+1}^{\infty} \left| (q^{n \rho - g+1} - 1) q^{-n \rho s} \right| = \sum_{n=t+1}^{\infty} (q^{n \rho - g+1} - 1) q^{-n \rho} |q|^s = \sum_{n=t+1}^{\infty} (q^{n \rho - g+1} - 1) q^{-n \rho} e^{a \ln(q)} |e^{i(b \ln(q))} |
\]

\[
\sum_{n=t+1}^{\infty} (q^{n \rho - g+1} - 1) q^{-n \rho} e^{a \ln(q)} = \sum_{n=t+1}^{\infty} (q^{n \rho - g+1} - 1) q^{-n \rho} q^a = \sum_{n=t+1}^{\infty} (q^{n \rho - g+1} - 1) q^{-n \rho} Re(s) = \frac{1}{q^{\rho-1}} \sum_{n=t+1}^{\infty} (q^{1-\text{Re}(s)})^{n \rho} - \sum_{n=t+1}^{\infty} (q^{-\text{Re}(s)})^{n \rho}
\]

It is now clear that if \( \text{Re}(s) < 1 \), then the above series does not converge, which gives us our result. \( \square \)

Our aim is to prove that there exists a different formula for \( \zeta_F(s) \), namely the product based formula. Through this, we will show in the next chapter that \( \rho = 1 \) and thus that there exist divisors of degree 1.

**Proposition 3.6.**

*We have that for \( \text{Re}(s) > 1 \)*

\[
\zeta_F(s) = \prod_{\mathfrak{P} \in |F|} (1 - N(\mathfrak{P})^{-s})^{-1}
\]

*Proof*

Chose any place \( \mathfrak{P} \in |F| \) of our function field \( F/\mathbb{F}_q \) and set \( n = \text{deg}(\mathfrak{P}) \). Now, consider

\[
a_\mathfrak{P} = \frac{1}{1 - \frac{1}{N(\mathfrak{P})^s}} - 1 = \frac{1}{1 - q^{-ns}} - 1 = \frac{q^{-ns}}{1 - q^{-ns}} = \frac{1}{q^{ns} - 1}
\]
The triangle inequality gives $|q^{n_s} - 1| \geq |q^{n_s}| - 1 = q^{n\alpha}$ where $\alpha = \Re(s)$. Since $\Re(s) = \alpha > 1$ we have that when $n$ is large enough the following holds

$$|a_P| \leq \frac{1}{q^{n\alpha} - 1} \leq \frac{2}{q^{n\alpha}}$$

Now, when $n > 2g - 2$ for the genus $g$, we have that

$$|\{\mathfrak{P} : \deg(\mathfrak{P}) = n\}| \leq A_n = h_F \left( \frac{q^{n-g+1} - 1}{q - 1} \right)$$

Hence we have

$$\sum_{n>0} |a_P| \leq \frac{h_F}{q - 1} q^{-g+1} \sum_{n=0}^{\infty} \frac{2}{q^n(\alpha - 1)} - \frac{h_F}{q - 1} \sum_{n=0}^{\infty} \frac{2}{q^{n\alpha}} < \infty$$

which in turn implies that $\prod_{\mathfrak{P} \in |F|}(1 - N(\mathfrak{P})^{-s})^{-1}$ converges absolutely.

Now all we need is to show that the zeta function can indeed take this form. this is clear though by considering the following

$$\prod_{\mathfrak{P} \in |F|} (1 - N(\mathfrak{P})^{-s})^{-1} = \prod \left( \frac{1}{1 - N(\mathfrak{P})^{-s}} \right)$$

$$= \prod \left( \sum_{n_P = 0}^{\infty} (N(\mathfrak{P})^{-n_P s}) \right)$$

$$= \sum_{\text{over all } r \text{ and all } a_i} N(a_1 \mathfrak{P}_1 + \ldots + a_r \mathfrak{P}_r)^{-s}$$

$$= \sum_{D \in \mathcal{D}_F} \frac{1}{N(D)^s} = \zeta_F(s)$$

3.3 A Functional Equation for $\zeta_F$

We will see that the class number formula depends on a polynomial, namely the $L$-polynomial whose existence and form is shown in (4.2). In our attempt to find this polynomial for specific function fields with finite constant field, we will need the following equation which will simplify work done with the zeta function. Material here draws from pages 161 – 165 in [15], but also with a similar approach from Salvador in [14].

33
Proposition 3.7.
For a function field $F/F_q$ where $q = p^n$, $p$ being prime, we have

1. If the genus $g = 0$ then
   \begin{align*}
   \zeta_F(s) &= \frac{1}{q-1} \left( \frac{q}{1-(qs)^\rho} - \frac{1}{1-s^\rho} \right)
   \end{align*}

2. If $g \geq 1$ then $\zeta_F(s) = F(s) + G(s)$ where
   \begin{align*}
   F(s) &= \frac{1}{q-1} \sum_{[\mathcal{C}] \in \text{Cl}_F \atop 0 \leq \text{deg}([\mathcal{C}]) \leq 2g-2} q^{l([\mathcal{C}])} s^\text{deg}([\mathcal{C}]) \\
   G(s) &= \frac{h_F}{q-1} \left( q^{1-g} q^{2g-2+\rho} \frac{1}{1-(qs)^\rho} - \frac{1}{1-s^\rho} \right)
   \end{align*}

Proof
1) From (2.15) we have that $h_F = 1$ and so now, using (3.4) we have
   \begin{align*}
   \zeta_F(s) &= \sum_{n=0}^{\infty} A_n s^n = \sum_{n=0}^{\infty} A_{\rho n} s^{\rho n} \\
   &= \sum_{n=0}^{\infty} \frac{1}{q-1} (q^{n\rho+1} - 1) s^{\rho n} \\
   &= \frac{1}{q-1} \left( q \sum_{n=0}^{\infty} (qs)^{\rho n} - \sum_{n=0}^{\infty} s^{\rho n} \right) \\
   &= \frac{1}{q-1} \left( \frac{q}{1-(qs)^\rho} - \frac{1}{1-s^\rho} \right)
   \end{align*}

2) In a similar manner, we have for $g \geq 1$, and the sums being over all $[\mathcal{C}] \in \text{Cl}_F$
   \begin{align*}
   \zeta_F(s) &= \sum_{\text{deg}([\mathcal{C}]) \geq 0} |\{A \in [\mathcal{C}] : A \geq 0\}| s^\text{deg}([\mathcal{C}]) = \sum_{\text{deg}([\mathcal{C}]) \geq 0} \frac{q^{l([\mathcal{C}])}}{q-1} s^\text{deg}([\mathcal{C}]) \\
   &= \frac{1}{q-1} \sum_{0 \leq \text{deg}([\mathcal{C}]) \leq 2g-2} q^{l([\mathcal{C}])} s^\text{deg}([\mathcal{C}]) \\
   &\quad + \frac{1}{q-1} \sum_{\text{deg}([\mathcal{C}]) > 2g-2} q^\text{deg}([\mathcal{C}]+1-g) s^\text{deg}([\mathcal{C}]) \\
   &\quad - \frac{1}{q-1} \sum_{\text{deg}([\mathcal{C}]) \geq 0} s^\text{deg}([\mathcal{C}])
   \end{align*}
which we can see is equal to $F(s) + G(s)$ since due to (3.4), we have

\[
(q - 1)G(s) = \sum_{n=0}^{\infty} h_F q^{n\rho} + 1 - g s^{n\rho} - \sum_{n=0}^{\infty} h_F t^{n\rho}
\]

\[
= h_F \left( q^{1-g(qt^{2g-2+\rho})} \frac{1}{1-(qs)^\rho} - \frac{1}{1-s^\rho} \right)
\]

4 The Class Number Formula

4.1 Background and Final Preparation

Having covered a significant amount of background material, we are now almost ready to proceed to the essence of this project, a formula for computing the class number of a given function field $F/K$. Notation used so far will continue to be used throughout this chapter as well. Note also that work is done on finite fields of order $q = p^n$, $p$ being a prime.

Number theory provides different methods for determining the class number of a given number field and one can resort to [2] or [12] for various class number formulas. However, this section draws from [14], [13] and [15].

4.2 The Class Number Formula In Function Fields

Recall that $\text{Cl}_F$ denotes the quotient group $\mathcal{D}_F/\mathcal{P}_F$ of divisors over principal divisors. Also, $\text{Cl}_F^0$ is the group of divisor classes of degree 0. Some final background material is necessary before we state and prove the class number formula.

Let $u = q^{-\rho s}$ and $B_n = A_{\rho n}$. We then have the following formula for the zeta function

\[
\zeta_F(s) = \sum_{n=0}^{\infty} B_n u^n
\]

(4.2.1)

Our next aim is to find a recurrence relation between the $B_n$.

Proposition 4.1.
Let \( t = \frac{2g-2}{\rho} \). The following hold

\[
\begin{cases}
B_j - (q^\rho + 1)B_{j-1} + q^\rho B_{j-2} = 0, & \text{for } j > t + 2 \\
B_{t+2} - (q^\rho + 1)B_{t+1} + q^\rho B_t = q^{g+\rho-1}
\end{cases}
\] (4.2.2)

**Proof**

For \( j > t + 2 \), the following hold

\[
\begin{align*}
(j\rho) &> (t + 2)\rho = t\rho + 2\rho = 2g - 2 + 2\rho \geq 2g \\
(j - 1)\rho &> (t + 1)\rho = t\rho + \rho = 2g - 2 + \rho \geq 2g - 1 \\
(j - 2)\rho &> t\rho = 2g - 2
\end{align*}
\]

We thus have the necessary condition to use (3.4) and hence from the fact that \( B_n = A_{\rho n} = h_F \frac{q^{\rho n+1}-1}{q-1} \) the result follows with substitutions.

**Theorem 4.2.**

In a function field \( F/K \) where \( K = \mathbb{F}_q \), such that \( q = p^n \) for some prime \( p \), with genus \( g \), there is a polynomial \( L_F(x) \in \mathbb{Z}[x] \) such that \( \deg(L_F) = \frac{2g-2}{\rho} + 2 \) and the following holds for \( u = q^{-s} \)

\[
\zeta_F(s) = \frac{L_F(q^{-s})}{(1-q^{-s})(1-q^{\rho-s})} = \frac{L_F(u)}{(1-u)(1-q^\rho u)}
\]

**Proof**

Let \( B_{-1} = B_{-2} = 0 \) in the following expression

\[
(1 - u)(1 - q^\rho u)\zeta_F(u) = (1 - (1 + q^\rho)u + q^\rho u^2) \zeta_F(s)
\]

\[
= \sum_{n=0}^{\infty} B_n u^n - \sum_{n=0}^{\infty} (1 + q^\rho) B_n u^{n+1} + \sum_{n=0}^{\infty} q^\rho B_n u^{n+2}
\]

\[
= \sum_{n=0}^{\infty} (B_n - (1 + q^\rho)B_{n-1} + q^\rho B_{n-2})u^n
\]

\[
= \sum_{n=0}^{t+2} (B_n - (1 + q^\rho)B_{n-1} + q^\rho B_{n-2})u^n
\]

\[
= 1 + (B_1 - (q^\rho + 1))u + \sum_{n=2}^{t+2} (B_n - (1 + q^\rho)B_{n-1} + q^\rho B_{n-2})u^n
\]
Which is an integer polynomial of degree \( t + 2 = \frac{2g-2}{\rho} + 2 \).

The class number formula is finally given by the following theorem.

**Theorem 4.3. (Class Number Formula)**

For a function field \( F/K \) with finite constant field and \( K = \mathbb{F}_q \) where \( q = p^n \) for some prime integer \( p \), it holds that

\[
L_F(1) = h_F q^\rho - 1
\]

\[
q - 1
\]

**Proof**

Let \( B_{-1} = B_{-2} = 0 \) in the following

\[
L_F(1) = \sum_{n=0}^{t+2} (B_n - (1 + q^\rho)B_{n-1} + q^n B_{n-2})
\]

\[
= \sum_{n=0}^{t+2} (B_n - B_{n-1} - q^\rho B_{n-1} + q^n B_{n-2})
\]

\[
= B_{t+2} - B_{-1} - q^\rho (B_{t+1} - B_{-2}) = A_{t+2} - q^\rho A_{t+1}
\]

\[
= A_{2g-2+2\rho} - q^\rho A_{2g-2+\rho}
\]

\[
= h_F \frac{q^{2g-2+2\rho-g+1} - 1}{q - 1} - q^\rho h_F \frac{q^{2g-2+\rho-g+1} - 1}{q - 1}
\]

\[
= \frac{h_F}{q - 1} \left( q^{g+2\rho-1} - 1 - q^{g+2\rho-1} + q^\rho \right) = h_F \frac{q^\rho - 1}{q - 1}
\]

4.3 Finding the \( L \)-Polynomial

Equipped now with Schmidt’s theorem, we can show the existence of another functional equation for \( \zeta_F(s) \) which in turn will allow us to prove some facts about the \( L \)-polynomial of a function field.
Proposition 4.5.

The zeta function for the function field $F/F_q$ satisfies the following functional equation

$$ \zeta_F(s) = q^{g-1}s^{2g-2}\zeta_F \left( \frac{1}{qs} \right) $$

Proof

When $g = 0$ we have from (3.7) and Schmidt’s theorem that

$$ \zeta_F(s) = \frac{1}{(1-s)(1-qqs)} $$

from which the result follows easily.

When $g \geq 1$ from Schmidt’s theorem, our previously calculated functional equation in (3.7) now becomes $\zeta_F(s) = F(s) + G(s)$ where

$$ F(s) = \frac{1}{q-1} \sum_{[\mathcal{C}] \in \text{Cl}_F} q^l([\mathcal{C}]) s^\deg([\mathcal{C}]) $$

$$ G(s) = \frac{h_F}{q-1} \left( q^{1-g}qs^{2g-1} \frac{1}{1-qqs} - \frac{1}{1-s} \right) $$

Now, let $\mathfrak{M}$ be a divisor in the canonical divisor class of $\text{Cl}_F$. We have from the Riemann-Roch theorem that

$$ (q-1)F(s) = \sum_{[\mathcal{C}] \in \text{Cl}_F} q^l([\mathcal{C}]) s^\deg([\mathcal{C}]) $$

$$ = \sum_{0 \leq \deg([\mathcal{C}]) \leq 2g-2} q^\deg([\mathcal{C}]) + 1 - g + l([\mathfrak{M} - \mathcal{C}]) s^\deg([\mathcal{C}]) $$

$$ = q^{g-1}s^{2g-2} \sum_{0 \leq \deg([\mathcal{C}]) \leq 2g-2} q^\deg([\mathcal{C}]) -(2g-2) + l([\mathfrak{M} - \mathcal{C}]) s^\deg([\mathcal{C}]) -(2g-2) $$

$$ = q^{g-1}s^{2g-2} \sum_{0 \leq \deg([\mathcal{C}]) \leq 2g-2} q^l([\mathfrak{M} - \mathcal{C}]) \left( \frac{1}{qs} \right)^\deg([\mathfrak{M} - \mathcal{C}]) $$

$$ = q^{g-1}s^{2g-2} (q-1)F \left( \frac{1}{qs} \right) $$

38
Similarly, for $G(s)$ we have

\[
q^{g-1}s^{2g-2}G\left(\frac{1}{qs}\right) = \frac{h_F}{q-1}q^{g-1}s^{2g-2} \left( q^g \left(\frac{1}{qs}\right)^{2g-1} \frac{1}{1-q^{-1}} - \frac{1}{1-q^{-1}} \right)
\]

\[
= \frac{h_F}{q-1} \left( \frac{1}{s} \frac{1}{1-s} - \frac{q^g s^{2g-1}}{qs(1-\frac{1}{qs})} \right) = G(s)
\]

Adding the two formulas gives the result.

\[\square\]

**Theorem 4.6.**

For the $L$-polynomial $L_F$ of the function field $F/K$ the following hold

1. $L_F(1) = h_F$
2. We have $L_F(s) = q^g s^{2g} L_F(1/(qs))$
3. If $L_F(s) = a_0 + a_1 s + \ldots + a_{2g} s^{2g}$, with $a_i \in \mathbb{Z}$ then
   i) $a_0 = 1$ and $a_{2g} = q^g$
   ii) $a_{2g-i} = q^{g-i} a_i$ for $0 \leq i \leq g$
   iii) $a_1 = \Psi - (q + 1)$ where $\Psi$ is the number of places of degree 1
4. $L_F(s)$ factors in $\mathbb{C}[s]$ as

\[
L_F(s) = \prod_{i=1}^{2g} (1 - \alpha_i s)
\]

Where $\alpha_1, \ldots, \alpha_{2g}$ complex numbers which are algebraic integers and can be arranged in such a way that $\alpha_i \alpha_{g+i} = q$ for $i = 1, \ldots, g$

**Proof**

We assume that $g > 0$ since in the case $g = 0$, the results follows trivially.

1) Follows directly from (4.4) and (4.3).
2) Follows from the functional equation for the zeta function in (4.5).
3) The functional equation from part 2 gives that

\[
L_F(s) = q^g s^{2g} L\left(\frac{1}{qs}\right) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}} s + \ldots + q^g a_0 s^{2g}
\]

39
and so that \( a_{2g-i} = q^{0-i}a_i \) for \( i = 0, \ldots, g \). Now, comparing the coefficients of the above representation for \( L_F \) and the fact that

\[
L_F(s) = (1 - s)(1 - qs) \sum_{n=0}^{\infty} A_n s^n
\]

we get that \( a_0 = A_0 \) and \( a_1 = A_1 - (q + 1)A_0 \). However \( A_0 = 1 \), from the definition of \( A_n \), and \( A_1 = \Psi \), and thus that \( a_0 = 1 \) and \( a_1 = \Psi - (q + 1) \). Finally, \( a_{2g} = q^g a_0 = q^3 \).

4) Consider the reciprocal polynomial

\[
L'_F(s) = s^{2g} L_F \left( \frac{1}{s} \right) = a_0 + a_1 s^{2g-1} + \ldots + a_{2g} = s^{2g} + a_1 s^{2g-1} + \ldots + q^g \tag{4.3.1}
\]

This is a monic \( bZ \)-polynomial, so its roots \( \alpha_i \in \mathbb{C}, i = 1, \ldots, 2g \), are algebraic integers and we have \( L'_F(s) = \prod_{i=1}^{2g} (s - \alpha_i) \) and so that

\[
L_F(s) = t^{2g} L'_F \left( \frac{1}{t} \right) = \prod_{i=1}^{2g} (1 - \alpha_i s)
\]

The roots \( \alpha_i \) of \( L'_F(s) \) are the inverses of the roots of \( L_F(s) \) and the functional equation implies that \( L'_F(\alpha) = 0 \) if and only if \( L'_F(q/\alpha) = 0 \) and so we can arrange the roots as

\[
\alpha_1, \frac{q}{\alpha_1}, \ldots, \alpha_k, \frac{q}{\alpha_k}, q^{1/2}, \ldots, q^{1/2}, -q^{1/2}, \ldots, -q^{1/2}
\]

However, (4.3.1) now gives us that

\[
\frac{q}{\alpha_1} \ldots \frac{q}{\alpha_k} \left( q^{1/2} \right)^m \left( -q^{1/2} \right)^n = q^g
\]

Thus it must be that \( n \) is even. Also, since \( n + m + 2k = 2g \), \( m \) must also be even and so the \( \alpha_1, \ldots, \alpha_{2g} \) can be rearranged so that \( \alpha_i \alpha_{g+i} = q \) holds for \( i = 1, \ldots, g \). 

Part 1. of this theorem is essentially the class number formula. It implies that when we seek the class number for a function field, we need to compute the \( L \)-polynomial. This necessarily implies that one needs the genus of a function field which, as we saw, is not simple to calculate.
5 On Particular Function Fields

5.1 Quadratic Extensions of the Rational Function Field

For now, assume that $F/K$ is a function field such that $[F : K(x)] = 2$ and that $char(K) \neq 2$. The material here draws from [14].

Lemma 5.1.
We have $F = K(x, y)$ where $y^2 = f(x)$ and $f(x) \in K[x]$ is square free of degree $m$.

**Proof**
For $y \in F \setminus K(x)$ we have that $K(x) \subseteq K(x)(y) \subseteq F$ and also that $[K(x, y) : K(x)] \geq 2 = [F : K(x)]$. Hence, it must be that $F = K(x, y)$.

Now, $y$ is of degree 2 over $K(x)$, the irreducible polynomial of $y$ is of degree 2 and has the form $y^2 + ay + b$, with $a, b \in K(x)$. Since $char(K) \neq 2$, we can complete the square and get

$$\left( y + \frac{a}{2} \right)^2 = \frac{a^2}{4} - b$$

Let $z = y + a/2$ and we still have that $F = K(x, z)$. It also holds that $z^2 = c \in K(x)$. Hence, one can write $c = h(x)/g(x)$ for some relatively prime elements $h, g \in K[x]$. This now gives that $(g(x)z)^2 = h(x)g(x)$ and we can put $u = g(x)z$ and $t(x) = h(x)g(x)$ to get that $F = K(x, u)$ and $u^2 = t(x)$. Finally, $t(x) = r(x)^2f(x)$ where $f(x)$ is square free and so by setting $v = u/r(x)$ we have $F = K(x, v)$ and $v^2 = f(x)$. \qed

Now, since $[F : K(x)] = 2$ and $char(K) \neq 2$ we have that $F/K(x)$ is a Galois extension with Galois group of order 2. Say that $\Gamma(F/K(x)) = \{1, \sigma\}$ and clearly if $F = K(x, y)$, we have that $\sigma(y) = -y$.

Now, let $\mathfrak{p}$ be an arbitrary place and let $\mathcal{O}_\mathfrak{p}$ be its corresponding valuation ring and $v_\mathfrak{p}$ the valuation. We define

$$v_\mathfrak{p}(z) = v_\mathfrak{p}(\sigma(z)) = v_\mathfrak{p}(\sigma^{-1}(z))$$

And this can be extended naturally to act on a divisor $\mathfrak{A} \in \mathcal{D}_F$ as

$$\mathfrak{A} = \sum_{\mathfrak{p} \in |F|} n_\mathfrak{p}\mathfrak{p} \Rightarrow \mathfrak{A}^\sigma = \sum_{\mathfrak{p} \in |F|} n_\mathfrak{p}\mathfrak{p}^\sigma$$

Now, the following result is easy to prove.
Lemma 5.2.
We have that \( v_{\mathfrak{p}} \) is a valuation with maximal ideal \( \mathfrak{p}^* = \{ \sigma(a) : a \in \mathfrak{p} \} \) and valuation ring \( \mathcal{O}_{\mathfrak{p}}^* \).

In what follows we will use the notation

\[
(z) = \mathfrak{z}_z - \mathfrak{r}_z
\]

where \( \mathfrak{z}_z, \mathfrak{r}_z \) are the zero and pole divisor respectively of \( z \).

Lemma 5.3.
If \( z \in F^* \) then \( (z)_F^* = (z)^* \).

Proof
Following the agreed notation from above, we have that \( v_{\mathfrak{p}}(\sigma(z)) = v_{\mathfrak{p}}(z) \), or that \( \mathfrak{z}_z^* = \mathfrak{z}_{\sigma(z)} \), and that \( \mathfrak{r}_z^* = \mathfrak{r}_{\sigma(z)} \). We hence have that

\[
(z)^* = \mathfrak{z}_z^* - \mathfrak{r}_z^* = \mathfrak{z}_{\sigma(z)} - \mathfrak{r}_{\sigma(z)} = (\sigma(z)) = (z)^*
\]

Lemma 5.4.
Let \( t \in \mathbb{N} \) and let \( \mathfrak{r}_x \) be the pole divisor of \( x \in F \). If \( z \in L(t\mathfrak{r}_x) \), then \( \sigma(z) \in L(t\mathfrak{r}_x) \). In particular, we have that if \( z = a(x) - yb(x) \) with \( a(x), b(x) \in K(x) \) and \( z \in L(t\mathfrak{r}_x) \), then \( \sigma(z) = a(x) - yb(x) \in L(t\mathfrak{r}_x) \).

Proof
For \( 0 \neq z \in L(t\mathfrak{r}_x) \) we have \( (z) = \mathfrak{a} - t\mathfrak{r}_x \) for some \( \mathfrak{a} \in \mathfrak{d}_F \) such that \( \mathfrak{a} \leq 0 \). Therefore we also have that \( \mathfrak{a}^* \leq 0 \) and that

\[
(z)^* = (\sigma(z)) = \mathfrak{a}^* - t\mathfrak{r}_x^* = \mathfrak{a}^* - t\mathfrak{r}_{\sigma(x)} = \mathfrak{a}^* - t\mathfrak{r}_x
\]

and so \( \sigma(z) \in L(t\mathfrak{r}_x) \).

The proof for the following is somewhat long and not of particular interest, but can however, be found in [14], pages 106 – 108. Note however that Salvador has defined \( L(\mathfrak{a}) \) differently to the way that I have.

Proposition 5.5.
For \( t \in \mathbb{N} \) we have that

\[
L(t\mathfrak{r}_x) = \{ a(x) + yb(x) : a(x), b(x) \in K[x], \deg(a(x)) \leq t, \deg(b(x)) \leq t - \frac{m}{2} \}
\]
Corollary 5.6.
In the function field $F = K(x, y)/K$ where $y^2 = f(x)$, we have for $m = \deg(f(x))$

$$l(t R_x) = \begin{cases} 
0 & \text{if } t < 0 \\
t + 1 & \text{if } 0 \leq t \leq \left[ \frac{m+1}{2} \right] - 1 \\
2t + 2 - \left[ \frac{m+1}{2} \right] & \text{if } t \geq \left[ \frac{m+1}{2} \right]
\end{cases}$$

Proof
If $t < 0$ we have that $t R_x < 0$ and so $\mathcal{L}(t R_x) = \{0\}$ which gives $l(t R_x) = 0$. Now, assume that $t \geq 0$. We have from the previous proposition that

$$\mathcal{L}(t R_x) = \left\{ a(x) + yb(x) : \deg(a(x)) \leq t, \deg(b(x)) \leq t - \frac{m}{2} \right\}$$

If

$$t \leq \left[ \frac{m+1}{2} \right] - 1 = \left[ \frac{m+1-2}{2} \right] = \left[ \frac{m-1}{2} \right] < \frac{m}{2}$$

then $t - m/2 < 0$ and so $b(x) = 0$. We thus get that

$$\mathcal{L}(t R_x) = \{a(x) : \deg(a(x)) \leq t\}$$

and that $l(t R_x) = t + 1$.

If $t \geq \left[ \frac{m+1}{2} \right] \geq \frac{m}{2}$ we have

$$\deg(b(x)) \leq \left[ t - \frac{m}{2} \right] = \begin{cases} 
\frac{t - m}{2} & \text{if } m \text{ is even} \\
\frac{t - 1 - \frac{m-1}{2}}{2} & \text{if } m \text{ is odd}
\end{cases}$$

and so that

$$l(t R_x) = t + 1 + \left[ t - \frac{m}{2} \right] + 1 = \begin{cases} 
2t + 2 - \frac{m}{2} & \text{if } m \text{ is even} \\
2t + 2 - \frac{m+1}{2} & \text{if } m \text{ is odd}
\end{cases}$$

Corollary 5.7.
For the genus $g_F$, we have

$$g_F = \left[ \frac{m+1}{2} \right] - 1$$

43
Proof
We have that \([F : K(x)] = 2 = \deg(R_x)\). If \(t > g\) then \(t \in \mathbb{N}\) and \(\deg(tR_x) = t \deg(R_x) = 2t > 2g - 2\). Hence, by corollary (2.13) we have \(l(tR_x) = \deg(tR_x) - g + 1\). Therefore for \(t > \max\{0, g, \lceil \frac{m+1}{2} \rceil\}\) we have that
\[
l(tR_x) = 2t + 2 - \left\lfloor \frac{m+1}{2} \right\rfloor = \deg(tR_x) - g + 1 = 2t - g + 1
\]
and so that \(g = 2t + 1 - (2t + 2) + \left\lfloor \frac{m+1}{2} \right\rfloor = \left\lfloor \frac{m+1}{2} \right\rfloor - 1\).

I finally include two theorems, the first from [17], which will aid in classifying which places ramify in an elliptic function field.

**Theorem 5.8.**
For \(\text{char}(K) \neq 2\), suppose that \(F = K(x, y)\) such that \(y^2 = f(x) \in K[x]\) where \(f(x)\) is a square free polynomial of degree 3. Suppose also that
\[
f(x) = c \prod_{i=1}^{r} p_i(x)
\]
where \(p_i(x)\) are irreducible polynomials of degree 1, 2 or 3 and \(c \neq 0\). Denote now by \(\mathfrak{P}_i \in |K(x)|\) the place of the rational function field corresponding to the polynomial \(p_i(x)\) and by \(\mathfrak{P}_\infty\) the place at infinity in \(K(x)\). In this case, the following holds

i) \(K\) is the full constant field of \(F\), and \(F/K\) is an elliptic function field.

ii) The extension \(F/K(x)\) is cyclic of degree 2. Also, the places \(\mathfrak{P}_i\), \(i = \{1, \ldots, r\}\) and \(\mathfrak{P}_\infty\) are ramified in \(F/K(x)\) and each of them has a unique extension in \(K\), say \(\mathfrak{P}'_i\) and \(\mathfrak{P}'_\infty\) such that the index of ramification is \(e(\mathfrak{P}'_i|\mathfrak{P}_i) = e(\mathfrak{P}'_\infty|\mathfrak{P}_\infty) = 2\), \(\deg(\mathfrak{P}'_i) = \deg(\mathfrak{P}_i)\) for all \(i\), and \(\deg(\mathfrak{P}'_\infty) = 1\).

The following is a corollary of Kummer’s theorem, which is very useful in classifying the degree of the places lying over places of a rational function field. This and Kummer’s theorem come directly from Stichtenoth. We assume here nothing other than what is stated in the theorem itself. [15].

**Theorem 5.9.**
Let \(\phi(T) = T^n + f_{n-1}(x)T^{n-1} + \ldots + f_0(x) \in K(x)[T]\) be an irreducible polynomial over the rational function field \(K(x)\). We consider the function field \(K(x, y)/K\) where \(y\) satisfies the equation \(\phi(y) = 0\), and an element \(\alpha \in K\) such that \(f_j(\alpha) \neq \infty\)
for any $0 \leq j \leq n - 1$. Denote by $\Psi_\alpha \in |K(x)|$ the zero of $x - \alpha$ in $K(x)$. Suppose that the polynomial
\[
\phi_\alpha(T) = T^n + f_{n-1}(\alpha)T^{n-1} + \ldots + f_0(\alpha) \in K[T]
\]
decomposes in $K[T]$ as follows
\[
\phi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T)
\]
where $\psi_i(T)$ are monic, irreducible and pair-wise distinct polynomials in $K[T]$. We then have the following

i) For any $i = 1, \ldots, r$, there is a uniquely determined place $\Psi_i \in |K(x,y)|$ such that $x - \alpha, \psi_i(y) \in \Psi_i$. The element $x - \alpha$ is a prime element of $\Psi_i$, that is $e(\Psi_i[\alpha]) = 1$, and the residue class field of $\Psi_i$ is isomorphic to $K[T]/(\psi_i(T))$. Hence $f(\Psi_i[\alpha]) = \deg(\psi_i(T))$.

ii) If $\deg(\psi_i(T)) = 1$ for at least one $i \in \{1, \ldots, r\}$, then $K$ is the full constant field of $K(x,y)$.

iii) If $\phi_\alpha(T)$ has $n = \deg(\phi_\alpha(T))$ distinct roots in $K$, then there is, for any $\beta$ such that $\phi_\alpha(\beta) = 0$, a unique place $\Psi_{\alpha,\beta} \in |K(x,y)|$ such that
\[
x - \alpha \in \Psi_{\alpha,\beta} \text{ and } y - \beta \in \Psi_{\alpha,\beta}
\]
and $\Psi_{\alpha,\beta}$ is a place of $K(x,y)$ of degree 1.

5.2 A Worked Example

**Proposition 5.10.**

The function field $F = \mathbb{F}_5(x)(y)$ where $y^2 = x^3 + 2x$, is such that $g_F = 1$ and has class number $h_F = 2$.

**Proof**

We have that $|F : \mathbb{F}_5(x)| = 2$ and that $\text{char}(\mathbb{F}_5) \neq 2$, hence we can use corollary (5.7) and also the fact that $\deg(x^3 + 2x) = 3$ to deduce that
\[
g_F = \left[\frac{3+1}{2}\right] - 1 = 1
\]

Our aim now is to find the class number, the $L$-polynomial of $F/K$ and finally the zeta function.
From (4.2) we have that \( \text{deg}(L(u)) = 2g_F = 2 \), but also from (4.6) and that \( q = 5 \) we have that
\[
L(u) = 5u^2 + a_1u + 1
\]
where \( a_1 = \Psi - 6 \) where \( \Psi \) is the number of divisors of degree 1. However, due to (2.18), the number of divisor classes of degree one is simply the number of points (places) which have degree 1, and in turn, this is the class number \( h_F \) of the function field we are considering, since there are \( h_F \) divisor classes of degree \( n \) for any \( n \) (discussed in the section about the class group).

We now need to consider which places have degree 1 in the function field \( \mathbb{F}_5(x)/\mathbb{F}_5 \) and see how many places of \( \mathbb{F}_5(x,y)/\mathbb{F}_5 \) lie over them. The places of the rational function field \( \mathbb{F}_5(x)/\mathbb{F}_5 \) are determined by irreducible polynomials and thus we need only consider the polynomials \( p_i(x) = x - i \) for \( i \in \mathbb{F}_5 \).

The fact that \( p_0(x) = x \) is ramified comes as an immediate consequence from theorem (5.8), since it’s an irreducible factor of \( f(x) = x^3 + 2x \) and it is of degree 1. Note here that we need not check \( x^2 + 2 \), since this has degree 2 and thus so does its corresponding place, so any place of \( F \) lying over it will have degree at least 2 from the ramification formula (1.38).

Now, an alternative route using Eisenstein’s criterion will also show that \( p_0(x) = x \) is ramified. I present it here to show how this theorem can be used. Let \( \phi(T) = T^2 - x^3 - 2x \in \mathbb{F}_5(x)[T] \). We have that \( \phi \) is a degree 2 polynomial which is satisfied by \( y \). So, our aim is now to satisfy the necessary conditions for Eisenstein’s Criterion (1.39). We can see that for \( a_2 = 1, a_1 = 0, a_0 = -x(x^2 + 2) \) and the place \( \mathfrak{P}_x \in |\mathbb{F}_5(x)| \), that
\[
\mathcal{O}_{\mathfrak{P}_x} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_5[x], x \nmid g(x) \right\}
\]
\[
\mathfrak{P}_x = \left\{ \frac{xf(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_5[x], x \nmid g(x) \right\}
\]
and so, \( v_{\mathfrak{P}_x}(a_2) = v_{\mathfrak{P}_x}(1) = 0, v_{\mathfrak{P}_x}(a_1) = v_{\mathfrak{P}_x}(0) = \infty \) and \( v_{\mathfrak{P}_x}(-x(x^2 + 2)) = v_{\mathfrak{P}_x}(x) + v_{\mathfrak{P}_x}(x^2 + 2) = 1 + v_{\mathfrak{P}_x}(x^2 + 2) \). However \( x^2 + 2, (x^2 + 2)^{-1} \in \mathcal{O}_{\mathfrak{P}_x} \) and so \( x^2 + 2 \in \mathcal{O}_{\mathfrak{P}_x} \) so \( x^2 + 2 = x^3(x^2 + 2) \) and \( v_{\mathfrak{P}_x}(x^2 + 2) = 0 \). Hence \( v_{\mathfrak{P}_x}(a_0) = 1 \) which is coprime to \( \text{deg}(\phi(T)) = 2 \). Thus, Eisenstein’s criterion gives us that there exists a unique place \( \mathfrak{P}'_x \) of \( \mathbb{F}(x,y) \) such that \( f(\mathfrak{P}'_x|\mathfrak{P}_x) = [\mathfrak{P}_x : \mathfrak{P}'_x] = 1 \). This in turn implies that \( \text{deg}(\mathfrak{P}'_x) = \text{deg}(\mathfrak{P}_x) = 1 \) and so this is the only place of degree 1 that lies over \( \mathfrak{P}_x \).
Our aim now, is to show that the remaining \( p_i(x) \), namely for \( i = 1, 2, 3, 4 \), have no places of degree 1 lying over them. This however follows from Kummer’s theorem (5.9), as for \( \alpha = 1, 2, 3, 4 \), the polynomials we get are

\[
\begin{align*}
\phi_1(T) &= T^2 + 2 \\
\phi_2(T) &= T^2 + 3 \\
\phi_3(T) &= T^2 + 2 \\
\phi_4(T) &= T^2 + 3
\end{align*}
\]

which are all monic, irreducible over \( \mathbb{F}_5[T] \), since squares modulo 5 are 0, 1, 4. Thus, any place of \( \mathbb{F}_5(x, y) \) lying over these will have degree equal to the degree of these polynomials, that is degree 2. A point here must be made on why Kummer’s theorem does not apply to \( p_0(x) \). This is simply because \( \phi_0(T) = T^2 \) does not decompose into distinct polynomials, since \( T^2 = TT \).

Note also that we must consider the place at infinity. This however is covered by theorem (5.8), which gives us that this is indeed another place of degree 1.

Finally we can now conclude that we have 2 places of degree 1 in \( \mathbb{F}_5(x, y) / \mathbb{F}_5 \) and so that \( h_F = 2 \) and since \( L(1) = h_F = 2 \), we get \( a_1 = -4 \). Hence, \( L(u) = 5u^2 - 4u + 1 \). Finally the zeta function for \( F / \mathbb{F}_5 \) is

\[
\zeta_f(s) = \frac{5u^2 - 4u + 1}{(1-u)(1-5u)} = \frac{5u^2 - 4u + 1}{5u^2 - 6u + 1}
\]
6 Appendix

6.1 Background Material

Definition 6.1.
Given morphisms $f_j$, with $0 < j \in \mathbb{N}$, a sequence

$$\ldots A \xrightarrow{f_i} B \xrightarrow{f_{i+1}} C \ldots$$

is exact if $\text{Ker}(f_{i+1}) = \text{Im}(f_i)$ for all $i$.

Definition 6.2.
A short exact sequence is a sequence of the form

$$\{0\} \xrightarrow{f_1} A \xrightarrow{f_2} B \xrightarrow{f_3} C \xrightarrow{f_4} \{0\}$$

Example 6.3.
Consider the following example

$$\{0\} \xrightarrow{f_1} \mathbb{Z} \xrightarrow{f_2} \mathbb{Z} \xrightarrow{f_3} \mathbb{Z}/2\mathbb{Z} \xrightarrow{f_4} \{0\}$$

where

- $f_1$ is the zero map
- $f_2$ is multiplication by 2
- $f_3$ is reduction modulo 2
- $f_4$ is the zero map

Definition 6.4.
A free abelian group $G$ is an abelian group generated by a subset $S \subset G$, with integer coefficients. The cardinality of $S$ is defined as the rank of $G$.

For example, if $\{g_0, g_1, \ldots, g_n\}$ is a subset of $G$ then $\forall g \in G$ we have $g = \sum_i a_i g_i$ with $a_i \in \mathbb{Z}$.

Definition 6.5.
A ring $R$ is said to be local if it has exactly one maximal ideal $I$. 
6.2 Worked Example in MAGMA

We begin by initialising the function field with the following

```plaintext
> Y<t>:=PolynomialRing(Integers());
> R<x>:=FunctionField(GF(5));
> P<y>:=PolynomialRing(R);
> F<alpha>:=FunctionField(y^2-x^3-2*x);
```

One can then easily proceed to retrieving any relevant information about the function field, such the following, which verify our results from section 5.2

```plaintext
> Genus(F);
1
> LPolynomial(F);
5*t^2 - 4*t + 1
> ClassNumber(F);
2
> NumberOfPlacesDegECF(F,1);
2
```
### Table of Notation

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K(x)$</td>
<td>The rational function field over $K$</td>
<td>1</td>
</tr>
<tr>
<td>$\mathcal{O}, \mathcal{O}_v, \mathcal{O}_v$</td>
<td>A valuation ring</td>
<td>1</td>
</tr>
<tr>
<td>$v$</td>
<td>A discrete valuation</td>
<td>2</td>
</tr>
<tr>
<td>$\mathfrak{P}$</td>
<td>A place</td>
<td>3</td>
</tr>
<tr>
<td>$</td>
<td>F</td>
<td>$</td>
</tr>
<tr>
<td>$K$</td>
<td>The constant field of $F/K$</td>
<td>4</td>
</tr>
<tr>
<td>$F_{\mathfrak{P}}$</td>
<td>The residue class ring</td>
<td>7</td>
</tr>
<tr>
<td>$\mathfrak{P}_\infty$</td>
<td>The place at infinity</td>
<td>13</td>
</tr>
<tr>
<td>$\mathcal{D}_F$</td>
<td>The group of divisors</td>
<td>14</td>
</tr>
<tr>
<td>$\mathfrak{D}, \mathfrak{A}, \mathfrak{M}, \mathfrak{Q}$</td>
<td>A divisor</td>
<td>14</td>
</tr>
<tr>
<td>$(x)$</td>
<td>A principal divisor</td>
<td>15</td>
</tr>
<tr>
<td>$\mathcal{P}_F$</td>
<td>The group of principal divisors</td>
<td>15</td>
</tr>
<tr>
<td>$\mathfrak{L}(\mathfrak{D})$</td>
<td>The section of a divisor $\mathfrak{D}$</td>
<td>16</td>
</tr>
<tr>
<td>$l(\mathfrak{D})$</td>
<td>The dimension of a divisor $\mathfrak{D}$</td>
<td>16</td>
</tr>
<tr>
<td>$e(\mathfrak{P}'</td>
<td>\mathfrak{P})$</td>
<td>The ramification index of $\mathfrak{P}'$ over $\mathfrak{P}$</td>
</tr>
<tr>
<td>$f(\mathfrak{P}'</td>
<td>\mathfrak{P})$</td>
<td>The relative degree of $\mathfrak{P}'$ over $\mathfrak{P}$</td>
</tr>
<tr>
<td>$\mathcal{C}l_F$</td>
<td>The divisor class group</td>
<td>20</td>
</tr>
<tr>
<td>$\mathcal{C}l^n_F$</td>
<td>The divisor classes of degree $n$</td>
<td>20</td>
</tr>
<tr>
<td>$h_F$</td>
<td>The class number of $F/K$</td>
<td>20</td>
</tr>
<tr>
<td>$g_F$</td>
<td>The genus of the function field $F/K$</td>
<td>24</td>
</tr>
<tr>
<td>$A_n$</td>
<td>The number of integral divisors of degree $n$</td>
<td>28</td>
</tr>
<tr>
<td>$\rho$</td>
<td>The minimum degree of an integral divisor</td>
<td>28</td>
</tr>
<tr>
<td>$N(\mathfrak{P})$</td>
<td>The cardinality of the residue class field $F_{\mathfrak{P}}$</td>
<td>29</td>
</tr>
<tr>
<td>$\zeta_F(s)$</td>
<td>The zeta function of $F/K$</td>
<td>30</td>
</tr>
<tr>
<td>$L_F(s)$</td>
<td>The $L$-polynomial of $F/K$</td>
<td>36</td>
</tr>
</tbody>
</table>
References


