Analytic Number Theory in Function Fields (Lecture 3)

Julio Andrade

j.c.andrade.math@gmail.com
http://julioandrade.weebly.com/

University of Oxford

TCC Graduate Course
University of Oxford, Oxford
01 May 2015 - 11 June 2015

Content

1. Algebraic Function Fields and Global Function Fields
2. Function Fields
3. Zeta Function for Function Fields
4. The Riemann Hypothesis for Function Fields

Introduction

- So far we have been working with $A = \mathbb{F}_q[T]$ inside the rational function field $k = \mathbb{F}_q(T)$.

Introduction

- So far we have been working with $A = \mathbb{F}_q[T]$ inside the rational function field $k = \mathbb{F}_q(T)$.
- In this lecture we extend our considerations to more general function fields of transcendence degree one over a general constant field.

Introduction

- So far we have been working with $A = \mathbb{F}_q[T]$ inside the rational function field $k = \mathbb{F}_q(T)$.
- In this lecture we extend our considerations to more general function fields of transcendence degree one over a general constant field.
- The Riemann-Roch theorem is the fundamental result we will need in this lecture.

Introduction

- So far we have been working with $A = \mathbb{F}_q[T]$ inside the rational function field $k = \mathbb{F}_q(T)$.
- In this lecture we extend our considerations to more general function fields of transcendence degree one over a general constant field.
- The Riemann-Roch theorem is the fundamental result we will need in this lecture.
- We will focus our attention to function fields over a finite constant field. (global function fields)

Introduction

- So far we have been working with $A = \mathbb{F}_q[T]$ inside the rational function field $k = \mathbb{F}_q(T)$.
- In this lecture we extend our considerations to more general function fields of transcendence degree one over a general constant field.
- The Riemann-Roch theorem is the fundamental result we will need in this lecture.
- We will focus our attention to function fields over a finite constant field. (global function fields)
- The other class of global fields are the algebraic number fields.

Introduction

- So far we have been working with $A = \mathbb{F}_q[T]$ inside the rational function field $k = \mathbb{F}_q(T)$.
- In this lecture we extend our considerations to more general function fields of transcendence degree one over a general constant field.
- The Riemann-Roch theorem is the fundamental result we will need in this lecture.
- We will focus our attention to function fields over a finite constant field. (global function fields)
- The other class of global fields are the algebraic number fields.
- All global fields share a great number of common features.

Introduction

- The main aim is to introduce the zeta function of a global function field and explore its properties.

Introduction

- The main aim is to introduce the zeta function of a global function field and explore its properties.
- The Riemann hypothesis will be explained in some detail.

Introduction

- The main aim is to introduce the zeta function of a global function field and explore its properties.
- The Riemann hypothesis will be explained in some detail.
- We will derive several consequences of the RH for such zeta functions (e.g. analogue of prime number theorem for arbitrary global function fields).

Introduction

- The main aim is to introduce the zeta function of a global function field and explore its properties.
- The Riemann hypothesis will be explained in some detail.
- We will derive several consequences of the RH for such zeta functions (e.g. analogue of prime number theorem for arbitrary global function fields).
- A sketch of the proof of the RH for function fields will be given in the last lecture.

Introduction

- The main aim is to introduce the zeta function of a global function field and explore its properties.
- The Riemann hypothesis will be explained in some detail.
- We will derive several consequences of the RH for such zeta functions (e.g. analogue of prime number theorem for arbitrary global function fields).
- A sketch of the proof of the RH for function fields will be given in the last lecture.
- In this lecture we prove a weak version of the RH for curves.

Introduction

- The main aim is to introduce the zeta function of a global function field and explore its properties.
- The Riemann hypothesis will be explained in some detail.
- We will derive several consequences of the RH for such zeta functions (e.g. analogue of prime number theorem for arbitrary global function fields).
- A sketch of the proof of the RH for function fields will be given in the last lecture.
- In this lecture we prove a weak version of the RH for curves.
- Before we begin. The treatment we give here is very arithmetic and analytic. The geometric underpinnings will not be much in evidence. The whole subject can be dealt with under the aspect of curves over finite fields.

Basic on Function Fields

It is not necessary to restrict the constant field F to be finite. In this first part we make no restriction on F whatsoever.

Basic on Function Fields

It is not necessary to restrict the constant field F to be finite. In this first part we make no restriction on F whatsoever.

Definition

A ***function field*** *in one variable over F is a field K, containing F and at least one element x, transcendental over F, such that $K/F(x)$ is a finite algebraic extension.*

Basic on Function Fields

It is not necessary to restrict the constant field F to be finite. In this first part we make no restriction on F whatsoever.

Definition

A ***function field*** *in one variable over F is a field K, containing F and at least one element x, transcendental over F, such that $K/F(x)$ is a finite algebraic extension.*

Such field is said to have transcendence degree one over F.

It is not hard to show that the algebraic closure of F in K is finite over F. One way to see this is to note that if E is a subfield of K, which is algebraic over F, then $[E : F] = [E(x) : F(x)] \leq [K : F(x)]$. So, replacing F with its algebraic closure in K, if neccessary, we assume that F is algebraically closed in K. In that case, F is called the **constant field** of K.

Remark

1. *If F is the constant field of K and $y \in K$ is not in F, then y is transcendental over F.*

Remark

1. *If F is the constant field of K and $y \in K$ is not in F, then y is transcendental over F.*
2. *$K/F(y)$ is a finite extension.*

Remark

1. *If F is the constant field of K and $y \in K$ is not in F, then y is transcendental over F.*
2. *$K/F(y)$ is a finite extension.*

   To see this, note that y is algebraic over $F(x)$ which shows there is a non-zero polynomial in two-variables $g(X, Y) \in F[X, Y]$ such that $g(x, y) = 0$. Since y is transcendental over F we must have that $g(X, Y) \notin F[Y]$. It follows that x is algebraic over $F(y)$. Since K is finite over $F(x, y)$ and $F(x, y)$ is finite over $F(y)$, it follows that K is finite over $F(y)$.

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

The ord function associated with R is denoted by $\mathrm{ord}_P(*)$.

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

The ord function associated with R is denoted by $\text{ord}_P(*)$.

Definition

The degree of P, $degP$, is defined to be the dimension of R/P over F.

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

The ord function associated with R is denoted by $\text{ord}_P(*)$.

Definition

The degree of P, $degP$, is defined to be the dimension of R/P over F.

Proposition

The dimension of R/P over F is finite.

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

The ord function associated with R is denoted by $\text{ord}_P(*)$.

Definition

The degree of P, deg$P$, is defined to be the dimension of R/P over F.

Proposition

The dimension of R/P over F is finite.

Proof.

Choose an element $y \in P$ which is not in F. By the previous discussion $K/F(y)$ is finite. We claim that $[R/P : F] \leq [K : F(y)]$.

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

The ord function associated with R is denoted by $\text{ord}_P(*)$.

Definition

The degree of P, $degP$, is defined to be the dimension of R/P over F.

Proposition

The dimension of R/P over F is finite.

Proof.

Choose an element $y \in P$ which is not in F. By the previous discussion $K/F(y)$ is finite. We claim that $[R/P : F] \leq [K : F(y)]$. To see this let $u_1, \ldots, u_m \in R$ be such that the residue classes modulo P, $\overline{u}_1, \ldots, \overline{u}_m$, are linearly independent over F. We claim that $u_1, \ldots, u_m$ are linearly independent over $F(y)$.

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

The ord function associated with R is denoted by $\text{ord}_P(*)$.

Definition

The degree of P, deg$P$, is defined to be the dimension of R/P over F.

Proposition

The dimension of R/P over F is finite.

Proof.

Choose an element $y \in P$ which is not in F. By the previous discussion $K/F(y)$ is finite. We claim that $[R/P : F] \leq [K : F(y)]$. To see this let $u_1, \ldots, u_m \in R$ be such that the residue classes modulo P, $\overline{u}_1, \ldots, \overline{u}_m$, are linearly independent over F. We claim that $u_1, \ldots, u_m$ are linearly independent over $F(y)$. Suppose not. Then we could find polynomials in y, $\{f_1(y), \ldots, f_m(y)\}$, such that

$$f_1(y)u_1 + \cdots + f_m(y)u_m = 0.$$

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

The ord function associated with R is denoted by $\mathrm{ord}_P(*)$.

Definition

The degree of P, $degP$, is defined to be the dimension of R/P over F.

Proposition

The dimension of R/P over F is finite.

Proof.

Choose an element $y \in P$ which is not in F. By the previous discussion $K/F(y)$ is finite. We claim that $[R/P : F] \leq [K : F(y)]$. To see this let $u_1, \ldots, u_m \in R$ be such that the residue classes modulo P, $\overline{u}_1, \ldots, \overline{u}_m$, are linearly independent over F. We claim that $u_1, \ldots, u_m$ are linearly independent over $F(y)$. Suppose not. Then we could find polynomials in y, $\{f_1(y), \ldots, f_m(y)\}$, such that

$$f_1(y)u_1 + \cdots + f_m(y)u_m = 0.$$

It is not loss of generality to assume that not all the polynomials $f_i(y)$ are divisible by y. Now, reducing this relation modulo P gives a non-trivial linear relation for the elements $\overline{u}_i$ over F, a contradiction.

Definition

*A **prime** in K is a discrete valuation ring R with maximal ideal P such that $F \subset R$ and the quotient field of R equal to K. As a shorthand such a prime is often referred to as P, the maximal ideal of R.*

The ord function associated with R is denoted by $\text{ord}_P(*)$.

Definition

The degree of P, $degP$, is defined to be the dimension of R/P over F.

Proposition

The dimension of R/P over F is finite.

Proof.

Choose an element $y \in P$ which is not in F. By the previous discussion $K/F(y)$ is finite. We claim that $[R/P : F] \leq [K : F(y)]$. To see this let $u_1, \ldots, u_m \in R$ be such that the residue classes modulo P, $\overline{u}_1, \ldots, \overline{u}_m$, are linearly independent over F. We claim that $u_1, \ldots, u_m$ are linearly independent over $F(y)$. Suppose not. Then we could find polynomials in y, $\{f_1(y), \ldots, f_m(y)\}$, such that

$$f_1(y)u_1 + \cdots + f_m(y)u_m = 0.$$

It is not loss of generality to assume that not all the polynomials $f_i(y)$ are divisible by y. Now, reducing this relation modulo P gives a non-trivial linear relation for the elements $\overline{u}_i$ over F, a contradiction. Thus, $\{u_1, \ldots, u_m\}$ is a set linearly independent over $F(y)$ and it follows that $m \leq [K : F(y)]$ which proves the assertion.

To illustrate these definitions, consider the case of the rational function field $F(x)$.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P. It is clear that P is a prime of $F(x)$ in the above sense.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P. It is clear that P is a prime of $F(x)$ in the above sense. This collection of primes can be shown to almost exhaust the set of primes of $F(x)$. In fact, there is just one more.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P. It is clear that P is a prime of $F(x)$ in the above sense. This collection of primes can be shown to almost exhaust the set of primes of $F(x)$. In fact, there is just one more.
Consider the ring $A^{'} = F[x^{-1}]$ and the prime ideal $P^{'}$ generated by x^{-1} in $A^{'}$.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P. It is clear that P is a prime of $F(x)$ in the above sense. This collection of primes can be shown to almost exhaust the set of primes of $F(x)$. In fact, there is just one more.

Consider the ring $A^{'} = F[x^{-1}]$ and the prime ideal $P^{'}$ generated by x^{-1} in $A^{'}$. The localization of $A^{'}$ at $P^{'}$ is a discrete valuation ring which defines a prime of $F(x)$ called the **prime at infinity**.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P. It is clear that P is a prime of $F(x)$ in the above sense. This collection of primes can be shown to almost exhaust the set of primes of $F(x)$. In fact, there is just one more.
Consider the ring $A^{'} = F[x^{-1}]$ and the prime ideal $P^{'}$ generated by x^{-1} in $A^{'}$. The localization of $A^{'}$ at $P^{'}$ is a discrete valuation ring which defines a prime of $F(x)$ called the **prime at infinity**. This is usually denoted by P_∞ or, more simply, "∞" alone. The corresponding ord-function, ord_∞, attaches the value $-\deg(f)$ to any polynomial $f \in A$ and thus the value $\deg(g) - \deg(f)$ to any rational function f/g where $f, g \in A$.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P. It is clear that P is a prime of $F(x)$ in the above sense. This collection of primes can be shown to almost exhaust the set of primes of $F(x)$. In fact, there is just one more.

Consider the ring $A^{'} = F[x^{-1}]$ and the prime ideal $P^{'}$ generated by x^{-1} in $A^{'}$. The localization of $A^{'}$ at $P^{'}$ is a discrete valuation ring which defines a prime of $F(x)$ called the **prime at infinity**. This is usually denoted by P_∞ or, more simply, "∞" alone. The corresponding ord-function, ord_∞, attaches the value $-\deg(f)$ to any polynomial $f \in A$ and thus the value $\deg(g) - \deg(f)$ to any rational function f/g where $f, g \in A$.

Proposition

The only primes of $F(x)$ are the ones attached to the monic irreducibles, called the finite primes, together with the prime at infinity.

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P. It is clear that P is a prime of $F(x)$ in the above sense. This collection of primes can be shown to almost exhaust the set of primes of $F(x)$. In fact, there is just one more.

Consider the ring $A^{'} = F[x^{-1}]$ and the prime ideal $P^{'}$ generated by x^{-1} in $A^{'}$. The localization of $A^{'}$ at $P^{'}$ is a discrete valuation ring which defines a prime of $F(x)$ called the **prime at infinity**. This is usually denoted by P_∞ or, more simply, "∞" alone. The corresponding ord-function, ord_∞, attaches the value $-\deg(f)$ to any polynomial $f \in A$ and thus the value $\deg(g) - \deg(f)$ to any rational function f/g where $f, g \in A$.

Proposition

The only primes of $F(x)$ are the ones attached to the monic irreducibles, called the finite primes, together with the prime at infinity.

Remark

1. *The degree of any finite prime is equal to the degree of the monic irreducible to which it corresponds.*

To illustrate these definitions, consider the case of the rational function field $F(x)$. Let $A = F[x]$. Every non-zero prime ideal in A is generated by a unique monic irreducible P. The localization of A at P, A_P, is a discrete valuation ring. We continue to use the letter P to denote the unique maximal ideal A_P. It is clear that P is a prime of $F(x)$ in the above sense. This collection of primes can be shown to almost exhaust the set of primes of $F(x)$. In fact, there is just one more.

Consider the ring $A^{'} = F[x^{-1}]$ and the prime ideal $P^{'}$ generated by x^{-1} in $A^{'}$. The localization of $A^{'}$ at $P^{'}$ is a discrete valuation ring which defines a prime of $F(x)$ called the **prime at infinity**. This is usually denoted by P_∞ or, more simply, "∞" alone. The corresponding ord-function, ord_∞, attaches the value $-\deg(f)$ to any polynomial $f \in A$ and thus the value $\deg(g) - \deg(f)$ to any rational function f/g where $f, g \in A$.

Proposition

The only primes of $F(x)$ are the ones attached to the monic irreducibles, called the finite primes, together with the prime at infinity.

Remark

1. *The degree of any finite prime is equal to the degree of the monic irreducible to which it corresponds.*
2. *The degree of the prime at infinity is* 1.

Divisors

Definition

Let K be a function field over F. The ***group of divisors*** *of K, $\mathcal{D}_K$, is the free abelian group generated by the primes.*

Divisors

Definition

Let K be a function field over F. The ***group of divisors*** *of K, $\mathcal{D}_K$, is the free abelian group generated by the primes.*

We write these additively so that a typical divisor looks like

$$D = \sum_P a(P)P.$$

Divisors

Definition

Let K be a function field over F. The ***group of divisors*** *of K, $\mathcal{D}_K$, is the free abelian group generated by the primes.*

We write these additively so that a typical divisor looks like

$$D = \sum_P a(P)P.$$

The coefficients, $a(P)$, are uniquely determined by D and we will sometimes denote them as $\mathrm{ord}_P(D)$.

Divisors

Definition

Let K be a function field over F. The ***group of divisors*** *of K, $\mathcal{D}_K$, is the free abelian group generated by the primes.*

We write these additively so that a typical divisor looks like

$$D = \sum_P a(P)P.$$

The coefficients, $a(P)$, are uniquely determined by D and we will sometimes denote them as $\mathrm{ord}_P(D)$. The **degree** of such a divisor is defined as $\deg(D) = \sum_P a(P)\deg P$.

Divisors

Definition

*Let K be a function field over F. The **group of divisors** of K, $\mathcal{D}_K$, is the free abelian group generated by the primes.*

We write these additively so that a typical divisor looks like

$$D = \sum_P a(P)P.$$

The coefficients, $a(P)$, are uniquely determined by D and we will sometimes denote them as $\mathrm{ord}_P(D)$. The **degree** of such a divisor is defined as $\deg(D) = \sum_P a(P)\deg P$. This gives a homomorphism from $\mathcal{D}_K$ to $\mathbb{Z}$ whose kernel is denoted by $\mathcal{D}_K^0$, the **group of divisors of degree zero**.

Divisors

Definition

*Let K be a function field over F. The **group of divisors** of K, $\mathcal{D}_K$, is the free abelian group generated by the primes.*

We write these additively so that a typical divisor looks like

$$D = \sum_P a(P)P.$$

The coefficients, $a(P)$, are uniquely determined by D and we will sometimes denote them as $\mathrm{ord}_P(D)$. The **degree** of such a divisor is defined as $\deg(D) = \sum_P a(P)\deg P$. This gives a homomorphism from $\mathcal{D}_K$ to $\mathbb{Z}$ whose kernel is denoted by $\mathcal{D}_K^0$, the **group of divisors of degree zero**.

Let $a \in K^*$. The divisor of a, (a), is defined to be $\sum_P \mathrm{ord}_P(a)P$.

Divisors

Definition

Let K be a function field over F. The ***group of divisors*** *of K, $\mathcal{D}_K$, is the free abelian group generated by the primes.*

We write these additively so that a typical divisor looks like

$$D = \sum_P a(P)P.$$

The coefficients, $a(P)$, are uniquely determined by D and we will sometimes denote them as $\mathrm{ord}_P(D)$. The **degree** of such a divisor is defined as $\deg(D) = \sum_P a(P)\deg P$. This gives a homomorphism from $\mathcal{D}_K$ to $\mathbb{Z}$ whose kernel is denoted by $\mathcal{D}_K^0$, the **group of divisors of degree zero**.

Let $a \in K^*$. The divisor of a, (a), is defined to be $\sum_P \mathrm{ord}_P(a)P$. It is not hard to see that (a) is actually a divisor, i.e., that $\mathrm{ord}_P(a)$ is zero for all but finitely many P.

Divisors

Definition

Let K be a function field over F. The ***group of divisors*** *of K, $\mathcal{D}_K$, is the free abelian group generated by the primes.*

We write these additively so that a typical divisor looks like

$$D = \sum_P a(P)P.$$

The coefficients, $a(P)$, are uniquely determined by D and we will sometimes denote them as $\mathrm{ord}_P(D)$. The **degree** of such a divisor is defined as $\deg(D) = \sum_P a(P)\deg P$. This gives a homomorphism from $\mathcal{D}_K$ to $\mathbb{Z}$ whose kernel is denoted by $\mathcal{D}_K^0$, the **group of divisors of degree zero**.

Let $a \in K^*$. The divisor of a, (a), is defined to be $\sum_P \mathrm{ord}_P(a)P$. It is not hard to see that (a) is actually a divisor, i.e., that $\mathrm{ord}_P(a)$ is zero for all but finitely many P. The idea of the proof will be included in the proof of the next proposition. The map $a \rightarrow (a)$ is a homomorphism from K^* to $\mathcal{D}_K$. The image of this map is denoted by $\mathcal{P}_K$ and is called the **group of principal divisors**.

If P is a prime such that $\text{ord}_P(a) = m > 0$, we say that P is a **zero of** a **of order** m.

If P is a prime such that $\operatorname{ord}_P(a) = m > 0$, we say that P is a **zero of** a **of order** m. If $\operatorname{ord}_P(a) = -n < 0$ we say that P is a **pole of** a **of order** n.

If P is a prime such that $\operatorname{ord}_P(a) = m > 0$, we say that P is a **zero of** a **of order** m. If $\operatorname{ord}_P(a) = -n < 0$ we say that P is a **pole of** a **of order** n. Let

$$(a)_0 = \sum_{\substack{P \\ \operatorname{ord}_P(a)>0}} \operatorname{ord}_P(a)P \qquad \text{and} \qquad (a)_\infty = -\sum_{\substack{P \\ \operatorname{ord}_P(a)<0}} \operatorname{ord}_P(a)P.$$

If P is a prime such that $\mathrm{ord}_P(a) = m > 0$, we say that P is a **zero of** a **of order** m. If $\mathrm{ord}_P(a) = -n < 0$ we say that P is a **pole of** a **of order** n. Let

$$(a)_0 = \sum_{\substack{P \\ \mathrm{ord}_P(a)>0}} \mathrm{ord}_P(a)P \qquad \text{and} \qquad (a)_\infty = -\sum_{\substack{P \\ \mathrm{ord}_P(a)<0}} \mathrm{ord}_P(a)P.$$

The divisor $(a)_0$ is called the **divisor of zeros** of a and the divisor $(a)_\infty$ is called the **divisor of poles** of a.

If P is a prime such that $\mathrm{ord}_P(a) = m > 0$, we say that P is a **zero of a of order** m. If $\mathrm{ord}_P(a) = -n < 0$ we say that P is a **pole of a of order** n. Let

$$(a)_0 = \sum_{\substack{P \\ \mathrm{ord}_P(a)>0}} \mathrm{ord}_P(a)P \qquad \text{and} \qquad (a)_\infty = -\sum_{\substack{P \\ \mathrm{ord}_P(a)<0}} \mathrm{ord}_P(a)P.$$

The divisor $(a)_0$ is called the **divisor of zeros** of a and the divisor $(a)_\infty$ is called the **divisor of poles** of a. Note that $(a) = (a)_0 - (a)_\infty$.

Proposition

Let $a \in K^*$. Then, $ord_P(a) = 0$ for all but finitely many primes P.

Proposition

Let $a \in K^*$. Then, $ord_P(a) = 0$ for all but finitely many primes P. Secondly, $(a) = 0$, the zero divisor, if and only if $a \in F^*$, i.e., a is a non-zero constant.

Proposition

Let $a \in K^*$. *Then,* $ord_P(a) = 0$ *for all but finitely many primes* P. *Secondly,* $(a) = 0$, *the zero divisor, if and only if* $a \in F^*$, *i.e.,* a *is a non-zero constant. Finally,* $deg(a)_0 = deg(a)_\infty = [K : F(a)]$. *It follows that* $deg(a) = 0$, *i.e., the degree of a principal divisor is zero.*

Proposition

Let $a \in K^*$. Then, $ord_P(a) = 0$ for all but finitely many primes P. Secondly, $(a) = 0$, the zero divisor, if and only if $a \in F^*$, i.e., a is a non-zero constant. Finally, $deg(a)_0 = deg(a)_\infty = [K : F(a)]$. It follows that $deg(a) = 0$, i.e., the degree of a principal divisor is zero.

Proof. (Sketch).

If $a \in F^*$, it is easy from the definition that $(a) = 0$. So, suppose $a \in K^* - F^*$. Then, as we have seen, K is finite over $F(a)$. Let R be the integral closure of $F[a]$ in K.

Proposition

Let $a \in K^*$. Then, $ord_P(a) = 0$ for all but finitely many primes P. Secondly, $(a) = 0$, the zero divisor, if and only if $a \in F^*$, i.e., a is a non-zero constant. Finally, $deg(a)_0 = deg(a)_\infty = [K : F(a)]$. It follows that $deg(a) = 0$, i.e., the degree of a principal divisor is zero.

Proof. (Sketch).

If $a \in F^*$, it is easy from the definition that $(a) = 0$. So, suppose $a \in K^* - F^*$. Then, as we have seen, K is finite over $F(a)$. Let R be the integral closure of $F[a]$ in K. R is a Dedekind domain (see the book by Samuel and Zariski, Chapter V). Let $Ra = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ be the prime decomposition of the principal ideal Ra in R. The localization of R at the prime ideals $\mathfrak{P}_i$ are primes of the field K.

Proposition

Let $a \in K^*$. Then, $ord_P(a) = 0$ for all but finitely many primes P. Secondly, $(a) = 0$, the zero divisor, if and only if $a \in F^*$, i.e., a is a non-zero constant. Finally, $deg(a)_0 = deg(a)_\infty = [K : F(a)]$. It follows that $deg(a) = 0$, i.e., the degree of a principal divisor is zero.

Proof. (Sketch).

If $a \in F^*$, it is easy from the definition that $(a) = 0$. So, suppose $a \in K^* - F^*$. Then, as we have seen, K is finite over $F(a)$. Let R be the integral closure of $F[a]$ in K. R is a Dedekind domain (see the book by Samuel and Zariski, Chapter V). Let $Ra = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ be the prime decomposition of the principal ideal Ra in R. The localization of R at the prime ideals $\mathfrak{P}_i$ are primes of the field K. If we denote by P_i the maximal ideals of these discrete valuation rings we find that $\mathrm{ord}_{P_i}(a) = e_i$. It is now not hard to show that the finite set $\{P_1, P_2, \ldots, P_g\}$ is the set of zeros of a.

Proposition

Let $a \in K^*$. Then, $ord_P(a) = 0$ for all but finitely many primes P. Secondly, $(a) = 0$, the zero divisor, if and only if $a \in F^*$, i.e., a is a non-zero constant. Finally, $deg(a)_0 = deg(a)_\infty = [K : F(a)]$. It follows that $deg(a) = 0$, i.e., the degree of a principal divisor is zero.

Proof. (Sketch).

If $a \in F^*$, it is easy from the definition that $(a) = 0$. So, suppose $a \in K^* - F^*$. Then, as we have seen, K is finite over $F(a)$. Let R be the integral closure of $F[a]$ in K. R is a Dedekind domain (see the book by Samuel and Zariski, Chapter V). Let $Ra = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ be the prime decomposition of the principal ideal Ra in R. The localization of R at the prime ideals $\mathfrak{P}_i$ are primes of the field K. If we denote by P_i the maximal ideals of these discrete valuation rings we find that $\mathrm{ord}_{P_i}(a) = e_i$. It is now not hard to show that the finite set $\{P_1, P_2, \dots, P_g\}$ is the set of zeros of a. Applying the same reasoning to a^{-1} we see that the set of poles of a is also finite.

Proposition

Let $a \in K^*$. Then, $ord_P(a) = 0$ for all but finitely many primes P. Secondly, $(a) = 0$, the zero divisor, if and only if $a \in F^*$, i.e., a is a non-zero constant. Finally, $deg(a)_0 = deg(a)_\infty = [K : F(a)]$. It follows that $deg(a) = 0$, i.e., the degree of a principal divisor is zero.

Proof. (Sketch).

If $a \in F^*$, it is easy from the definition that $(a) = 0$. So, suppose $a \in K^* - F^*$. Then, as we have seen, K is finite over $F(a)$. Let R be the integral closure of $F[a]$ in K. R is a Dedekind domain (see the book by Samuel and Zariski, Chapter V). Let $Ra = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ be the prime decomposition of the principal ideal Ra in R. The localization of R at the prime ideals $\mathfrak{P}_i$ are primes of the field K. If we denote by P_i the maximal ideals of these discrete valuation rings we find that $\mathrm{ord}_{P_i}(a) = e_i$. It is now not hard to show that the finite set $\{P_1, P_2, \ldots, P_g\}$ is the set of zeros of a. Applying the same reasoning to a^{-1} we see that the set of poles of a is also finite. This proves the first assertion. It also proves the second assertion since if a is not in F^* we see that the set of P such that $\mathrm{ord}_P(a) > 0$ is not empty. To show $[K : F(a)] = \mathrm{deg}(a)_0 = \mathrm{deg}(a)_\infty$ we use the results given by Deuring and Chevalley. □

For emphasis we point out that implicit in the previous sketch is the fact that every non-constant element of K has at least one zero and at least one pole.

For emphasis we point out that implicit in the previous sketch is the fact that every non-constant element of K has at least one zero and at least one pole.

Definition

Two divisors, D_1 and D_2, are said to be ***linearly equivalent****, $D_1 \sim D_2$ if their difference is principal, i.e., $D_1 - D_2 = (a)$ for some $a \in K^*$.*

For emphasis we point out that implicit in the previous sketch is the fact that every non-constant element of K has at least one zero and at least one pole.

Definition

*Two divisors, D_1 and D_2, are said to be **linearly equivalent**, $D_1 \sim D_2$ if their difference is principal, i.e., $D_1 - D_2 = (a)$ for some $a \in K^*$.*

We define $Cl_K = \mathcal{D}_K / \mathcal{P}_K$ to be the **group of divisor classes**.

For emphasis we point out that implicit in the previous sketch is the fact that every non-constant element of K has at least one zero and at least one pole.

Definition

Two divisors, D_1 and D_2, are said to be ***linearly equivalent****, $D_1 \sim D_2$ if their difference is principal, i.e., $D_1 - D_2 = (a)$ for some $a \in K^*$.*

We define $Cl_K = \mathcal{D}_K/\mathcal{P}_K$ to be the **group of divisor classes**. Since the degree of a principal divisor is zero, the degree function gives rise to a homomorphism from Cl_K to $\mathbb{Z}$. The kernel of this map is denoted by Cl_K^0, **the group of divisor classes of degree zero.**

For emphasis we point out that implicit in the previous sketch is the fact that every non-constant element of K has at least one zero and at least one pole.

Definition

*Two divisors, D_1 and D_2, are said to be **linearly equivalent**, $D_1 \sim D_2$ if their difference is principal, i.e., $D_1 - D_2 = (a)$ for some $a \in K^*$.*

We define $Cl_K = \mathcal{D}_K / \mathcal{P}_K$ to be the **group of divisor classes**. Since the degree of a principal divisor is zero, the degree function gives rise to a homomorphism from Cl_K to $\mathbb{Z}$. The kernel of this map is denoted by Cl_K^0, **the group of divisor classes of degree zero.**

We are almost ready to state the Riemann-Roch theorem. Just two more definitions are needed.

For emphasis we point out that implicit in the previous sketch is the fact that every non-constant element of K has at least one zero and at least one pole.

Definition

Two divisors, D_1 and D_2, are said to be ***linearly equivalent****, $D_1 \sim D_2$ if their difference is principal, i.e., $D_1 - D_2 = (a)$ for some $a \in K^*$.*

We define $Cl_K = \mathcal{D}_K/\mathcal{P}_K$ to be the **group of divisor classes**. Since the degree of a principal divisor is zero, the degree function gives rise to a homomorphism from Cl_K to $\mathbb{Z}$. The kernel of this map is denoted by Cl_K^0, **the group of divisor classes of degree zero.**

We are almost ready to state the Riemann-Roch theorem. Just two more definitions are needed.

Definition

A divisor, $D = \sum_P a(P)P$, is said to be an ***effective divisor*** *if for all P, $a(P) \geq 0$. We denote this by $D \geq 0$.*

Definition

Let D be a divisor. Define $L(D) = \{x \in K^* : (x) + D \geq 0\} \cup \{0\}$.

Definition

Let D be a divisor. Define $L(D) = \{x \in K^* : (x) + D \geq 0\} \cup \{0\}$. It is easy to see that $L(D)$ has the structure of a vector space over F and it can be proved that it is finite dimensional over F (Exercises in the problem sheet).

Definition

Let D be a divisor. Define $L(D) = \{x \in K^* : (x) + D \geq 0\} \cup \{0\}$. It is easy to see that $L(D)$ has the structure of a vector space over F and it can be proved that it is finite dimensional over F (Exercises in the problem sheet). The dimension of $L(D)$ over F is denoted by $l(D)$.

Definition

Let D be a divisor. Define $L(D) = \{x \in K^* : (x) + D \geq 0\} \cup \{0\}$. It is easy to see that $L(D)$ has the structure of a vector space over F and it can be proved that it is finite dimensional over F (Exercises in the problem sheet). The dimension of $L(D)$ over F is denoted by $l(D)$. The number $l(D)$ is sometimes referred to as the ***dimension*** *of D.*

Definition

Let D be a divisor. Define $L(D) = \{x \in K^* : (x) + D \geq 0\} \cup \{0\}$. It is easy to see that $L(D)$ has the structure of a vector space over F and it can be proved that it is finite dimensional over F (Exercises in the problem sheet). The dimension of $L(D)$ over F is denoted by $l(D)$. The number $l(D)$ is sometimes referred to as the ***dimension*** *of D.*

Lema (5.2)

If A and B are linearly equivalent divisors, then $L(A)$ and $L(B)$ are isomorphic. In particular, $l(A) = l(B)$.

Definition

*Let D be a divisor. Define $L(D) = \{x \in K^* : (x) + D \geq 0\} \cup \{0\}$. It is easy to see that $L(D)$ has the structure of a vector space over F and it can be proved that it is finite dimensional over F (Exercises in the problem sheet). The dimension of $L(D)$ over F is denoted by $l(D)$. The number $l(D)$ is sometimes referred to as the **dimension** of D.*

Lema (5.2)

If A and B are linearly equivalent divisors, then $L(A)$ and $L(B)$ are isomorphic. In particular, $l(A) = l(B)$.

Proof.

Suppose $A = B + (h)$. Then a short calculation shows that $x \to xh$ is an isomorphism from $L(A)$ with $L(B)$. □

Definition

*Let D be a divisor. Define $L(D) = \{x \in K^* : (x) + D \geq 0\} \cup \{0\}$. It is easy to see that $L(D)$ has the structure of a vector space over F and it can be proved that it is finite dimensional over F (Exercises in the problem sheet). The dimension of $L(D)$ over F is denoted by $l(D)$. The number $l(D)$ is sometimes referred to as the **dimension** of D.*

Lema (5.2)

If A and B are linearly equivalent divisors, then $L(A)$ and $L(B)$ are isomorphic. In particular, $l(A) = l(B)$.

Proof.

Suppose $A = B + (h)$. Then a short calculation shows that $x \to xh$ is an isomorphism from $L(A)$ with $L(B)$. □

Lema (5.3)

If $deg(A) \leq 0$ then $l(A) = 0$ unless $A \sim 0$ in which case $l(A) = 1$.

Riemann-Roch

Theorem (Riemann-Roch)

There is an integer $g \geq 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $A \in \mathcal{D}_K$ we have

$$l(A) = deg(A) - g + 1 + l(C - A).$$

Riemann-Roch

Theorem (Riemann-Roch)

There is an integer $g \geq 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $A \in \mathcal{D}_K$ we have

$$l(A) = deg(A) - g + 1 + l(C - A).$$

The proof can be found for example in "Algebraic Curves over Finite Fields" by Carlos Moreno.

Riemann-Roch

Theorem (Riemann-Roch)

There is an integer $g \geq 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $A \in \mathcal{D}_K$ we have

$$l(A) = deg(A) - g + 1 + l(C - A).$$

The proof can be found for example in “Algebraic Curves over Finite Fields” by Carlos Moreno.

The integer g is uniquely determined by K, as we shall see, and is called the **genus** of K.

Riemann-Roch

Theorem (Riemann-Roch)

There is an integer $g \geq 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $A \in \mathcal{D}_K$ we have

$$l(A) = deg(A) - g + 1 + l(C - A).$$

The proof can be found for example in "Algebraic Curves over Finite Fields" by Carlos Moreno.

The integer g is uniquely determined by K, as we shall see, and is called the **genus** of K. The genus of a function field is a key invariant.

Riemann-Roch

Theorem (Riemann-Roch)

There is an integer $g \geq 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $A \in \mathcal{D}_K$ we have

$$l(A) = deg(A) - g + 1 + l(C - A).$$

The proof can be found for example in “Algebraic Curves over Finite Fields” by Carlos Moreno.

The integer g is uniquely determined by K, as we shall see, and is called the **genus** of K. The genus of a function field is a key invariant. The divisor class $\mathcal{C}$ is also uniquely determined and is called the **canonical class**. It is related to differentials of K.

Riemann-Roch

Theorem (Riemann-Roch)

There is an integer $g \geq 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $A \in \mathcal{D}_K$ we have

$$l(A) = deg(A) - g + 1 + l(C - A).$$

The proof can be found for example in “Algebraic Curves over Finite Fields” by Carlos Moreno.

The integer g is uniquely determined by K, as we shall see, and is called the **genus** of K. The genus of a function field is a key invariant. The divisor class $\mathcal{C}$ is also uniquely determined and is called the **canonical class**. It is related to differentials of K. We give now a series of corollaries to the Riemann-Roch theorem.

Corollary (Riemann's inequality)

For all divisors A, we have $l(A) \geq deg(A) - g + 1$.

Corollary (Riemann's inequality)

For all divisors A, we have $l(A) \geq deg(A) - g + 1$.

Corollary (2)

For $C \in \mathcal{C}$ we have $l(C) = g$.

Corollary (Riemann's inequality)

For all divisors A, we have $l(A) \geq deg(A) - g + 1$.

Corollary (2)

For $C \in \mathcal{C}$ we have $l(C) = g$.

Proof.

Set $A = 0$ in the theorem. □

Corollary (Riemann's inequality)

For all divisors A, we have $l(A) \geq deg(A) - g + 1$.

Corollary (2)

For $C \in \mathcal{C}$ we have $l(C) = g$.

Proof.

Set $A = 0$ in the theorem. □

Corollary (3)

For $C \in \mathcal{C}$ we have $deg(C) = 2g - 2$.

Corollary (Riemann's inequality)

For all divisors A, we have $l(A) \geq deg(A) - g + 1$.

Corollary (2)

For $C \in \mathcal{C}$ we have $l(C) = g$.

Proof.

Set $A = 0$ in the theorem. □

Corollary (3)

For $C \in \mathcal{C}$ we have $deg(C) = 2g - 2$.

Proof.

Set $A = C$ in the theorem, and use Corollary 2. □

Corollary (Riemann's inequality)

For all divisors A, we have $l(A) \geq deg(A) - g + 1$.

Corollary (2)

For $C \in \mathcal{C}$ we have $l(C) = g$.

Proof.

Set $A = 0$ in the theorem. □

Corollary (3)

For $C \in \mathcal{C}$ we have $deg(C) = 2g - 2$.

Proof.

Set $A = C$ in the theorem, and use Corollary 2. □

Corollary (4)

If $deg(A) \geq 2g - 2$, then $l(A) = deg(A) - g + 1$ except in the case $deg(A) = 2g - 2$ and $A \in \mathcal{C}$.

Corollary (Riemann's inequality)

For all divisors A, we have $l(A) \geq deg(A) - g + 1$.

Corollary (2)

For $C \in \mathcal{C}$ we have $l(C) = g$.

Proof.

Set $A = 0$ in the theorem. □

Corollary (3)

For $C \in \mathcal{C}$ we have $deg(C) = 2g - 2$.

Proof.

Set $A = C$ in the theorem, and use Corollary 2. □

Corollary (4)

If $deg(A) \geq 2g - 2$, then $l(A) = deg(A) - g + 1$ except in the case $deg(A) = 2g - 2$ and $A \in \mathcal{C}$.

Proof.

If $\deg(A) \geq 2g - 2$, then $\deg(C - A) \leq 0$. Now we use Lemma 5.3. □

Corollary (5)

Suppose that $g^{'}$ and $C^{'}$ have the same properties as those of g and C stated in the theorem. Then, $g = g^{'}$ and $C \sim C^{'}$.

Corollary (5)

Suppose that $g^{'}$ and $C^{'}$ have the same properties as those of g and C stated in the theorem. Then, $g = g^{'}$ and $C \sim C^{'}$.

Proof.

Find a divisor A whose degree is larger than $\max(2g - 2, 2g^{'} - 2)$ (a large positive multiple of a prime will do).

Corollary (5)

Suppose that g' and C' have the same properties as those of g and C stated in the theorem. Then, $g = g'$ and $C \sim C'$.

Proof.

Find a divisor A whose degree is larger than $\max(2g-2, 2g'-2)$ (a large positive multiple of a prime will do). By Corollary 4,
$l(A) = \deg(A) - g + 1 = \deg(A) - g' + 1$. Thus, $g = g'$.

Corollary (5)

Suppose that $g^{'}$ and $C^{'}$ have the same properties as those of g and C stated in the theorem. Then, $g = g^{'}$ and $C \sim C^{'}$.

Proof.

Find a divisor A whose degree is larger than $\max(2g - 2, 2g^{'} - 2)$ (a large positive multiple of a prime will do). By Corollary 4, $l(A) = \deg(A) - g + 1 = \deg(A) - g^{'} + 1$. Thus, $g = g^{'}$. Now set $A = C^{'}$ in the statement of the theorem. Using Corollaries 2 and 3, applied to $C^{'}$, we see that $l(C - C^{'}) = 1$. There is an $x \in K^*$ such that $(x) + C - C^{'} \geq 0$. On the other hand, $(x) + C - C^{'}$ has degree zero by Corollary 3.

Corollary (5)

Suppose that g' and C' have the same properties as those of g and C stated in the theorem. Then, $g = g'$ and $C \sim C'$.

Proof.

Find a divisor A whose degree is larger than $\max(2g-2, 2g'-2)$ (a large positive multiple of a prime will do). By Corollary 4, $l(A) = \deg(A) - g + 1 = \deg(A) - g' + 1$. Thus, $g = g'$. Now set $A = C'$ in the statement of the theorem. Using Corollaries 2 and 3, applied to C', we see that $l(C - C') = 1$. There is an $x \in K^*$ such that $(x) + C - C' \geq 0$. On the other hand, $(x) + C - C'$ has degree zero by Corollary 3. Thus, it is the zero divisor, and $C \sim C'$. □

As an example of these results, consider the rational function field $F(x)$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\mathrm{ord}_\infty(f) = -\mathrm{deg}(f)$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\mathrm{ord}_\infty(f) = -\deg(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\mathrm{ord}_\infty(f) = -\mathrm{deg}(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\text{ord}_\infty(f) = -\text{deg}(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\mathrm{ord}_\infty(f) = -\mathrm{deg}(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\text{ord}_\infty(f) = -\text{deg}(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\text{ord}_\infty(f) = -\text{deg}(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2. It can be shown that $Cl_K^0 = (1)$ so there is only one class of degree -2 and we can choose any divisor of degree -2 for C. A conventional choice is $C = -2P_\infty$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\mathrm{ord}_\infty(f) = -\deg(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2. It can be shown that $Cl_K^0 = (1)$ so there is only one class of degree -2 and we can choose any divisor of degree -2 for C. A conventional choice is $C = -2P_\infty$. We can characterize the rational function field intrinsically as follows.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\text{ord}_\infty(f) = -\text{deg}(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2. It can be shown that $Cl_K^0 = (1)$ so there is only one class of degree -2 and we can choose any divisor of degree -2 for C. A conventional choice is $C = -2P_\infty$. We can characterize the rational function field intrinsically as follows.

Proposition

K/F is a rational function field if and only if there exists a prime P of K of degree 1 and the genus of K is 0.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\text{ord}_\infty(f) = -\text{deg}(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2. It can be shown that $Cl_K^0 = (1)$ so there is only one class of degree -2 and we can choose any divisor of degree -2 for C. A conventional choice is $C = -2P_\infty$. We can characterize the rational function field intrinsically as follows.

Proposition

K/F is a rational function field if and only if there exists a prime P of K of degree 1 and the genus of K is 0.

Proof.

We have seen that rational function fields have this property.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\mathrm{ord}_\infty(f) = -\mathrm{deg}(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2. It can be shown that $Cl_K^0 = (1)$ so there is only one class of degree -2 and we can choose any divisor of degree -2 for C. A conventional choice is $C = -2P_\infty$.
We can characterize the rational function field intrinsically as follows.

Proposition

K/F is a rational function field if and only if there exists a prime P of K of degree 1 and the genus of K is 0.

Proof.

We have seen that rational function fields have this property. Now, assume these conditions and consider $l(P)$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\mathrm{ord}_\infty(f) = -\deg(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2. It can be shown that $Cl_K^0 = (1)$ so there is only one class of degree -2 and we can choose any divisor of degree -2 for C. A conventional choice is $C = -2P_\infty$. We can characterize the rational function field intrinsically as follows.

Proposition

K/F is a rational function field if and only if there exists a prime P of K of degree 1 and the genus of K is 0.

Proof.

We have seen that rational function fields have this property. Now, assume these conditions and consider $l(P)$. Since $g = 0$ we have
$l(D) = \deg(D) - g + 1 = \deg(D) + 1$ for $\deg(D) > 2g - 2 = -2$.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\mathrm{ord}_\infty(f) = -\deg(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2. It can be shown that $Cl_K^0 = (1)$ so there is only one class of degree -2 and we can choose any divisor of degree -2 for C. A conventional choice is $C = -2P_\infty$. We can characterize the rational function field intrinsically as follows.

Proposition

K/F is a rational function field if and only if there exists a prime P of K of degree 1 and the genus of K is 0.

Proof.

We have seen that rational function fields have this property. Now, assume these conditions and consider $l(P)$. Since $g = 0$ we have
$l(D) = \deg(D) - g + 1 = \deg(D) + 1$ for $\deg(D) > 2g - 2 = -2$. Thus,
$l(P) = 2$ and we can find a non-constant function x such that $(x) + P \geq 0$.
Since $\deg((x) + P) = 1$, it follows that $(x) + P = Q$, a prime of degree 1.

As an example of these results, consider the rational function field $F(x)$. Let (R_∞, P_∞) be the prime which is, as we have seen, the localization of the ring $F[1/x]$ at the prime ideal generated by $1/x$. The corresponding ord function is $\text{ord}_\infty(f) = -\deg(f)$. By Corollary 4, for n large and positive we must have $l(nP_\infty) = n - g + 1$. On the other hand, one can prove that $f \in L(nP_\infty)$ if and only if f is a polynomial in T of degree $\leq n$. Thus, $l(nP_\infty) = n + 1$. It follows that $g = 0$. From this and Corollary 3 one sees that $\mathcal{C}$ has degree -2. It can be shown that $Cl_K^0 = (1)$ so there is only one class of degree -2 and we can choose any divisor of degree -2 for C. A conventional choice is $C = -2P_\infty$. We can characterize the rational function field intrinsically as follows.

Proposition

K/F is a rational function field if and only if there exists a prime P of K of degree 1 and the genus of K is 0.

Proof.

We have seen that rational function fields have this property. Now, assume these conditions and consider $l(P)$. Since $g = 0$ we have $l(D) = \deg(D) - g + 1 = \deg(D) + 1$ for $\deg(D) > 2g - 2 = -2$. Thus, $l(P) = 2$ and we can find a non-constant function x such that $(x) + P \geq 0$. Since $\deg((x) + P) = 1$, it follows that $(x) + P = Q$, a prime of degree 1. Thus, $(x) = Q - P$ and it follows that $[K : F(x)] = 1$. Thus, $K = F(x)$ as asserted. □

For the rest of the lecture we assume $F = \mathbb{F}_q$ is a finite field with q elements.

For the rest of the lecture we assume $F = \mathbb{F}_q$ is a finite field with q elements.

Definition

A function field in one variable over a finite constant field is called a ***global function field****.*

For the rest of the lecture we assume $F = \mathbb{F}_q$ is a finite field with q elements.

Definition

A function field in one variable over a finite constant field is called a ***global function field****.*

Our next goal is to define the zeta function of a global function field $K/\mathbb{F}_q$ and to investigate its properties.

For the rest of the lecture we assume $F = \mathbb{F}_q$ is a finite field with q elements.

Definition

A function field in one variable over a finite constant field is called a ***global function field****.*

Our next goal is to define the zeta function of a global function field $K/\mathbb{F}_q$ and to investigate its properties.
It was proven by F.K. Schmidt that a function field over a finite field always has divisors of degree 1. Using Schmidt's theorem, we have an exact sequence

$$(0) \to Cl_K^0 \to Cl_K \to \mathbb{Z} \to (0).$$

For the rest of the lecture we assume $F = \mathbb{F}_q$ is a finite field with q elements.

Definition

A function field in one variable over a finite constant field is called a ***global function field****.*

Our next goal is to define the zeta function of a global function field $K/\mathbb{F}_q$ and to investigate its properties.
It was proven by F.K. Schmidt that a function field over a finite field always has divisors of degree 1. Using Schmidt's theorem, we have an exact sequence

$$(0) \to Cl_K^0 \to Cl_K \to \mathbb{Z} \to (0).$$

We will prove that the group Cl_K^0 is finite. Denote its order by h_K. The number h_K is called the class number of the field K. This number is an important invariant of K. The above exact sequence shows that for any integer n there are exactly h_K classes of degree n.

Lema (5.5)

For any integer $n \geq 0$ the number of effective divisors of degree n is finite.

Lema (5.5)

For any integer $n \geq 0$ the number of effective divisors of degree n is finite.

Proof. (Sketch).

Choose an $x \in K$ such that x is transcendental over $\mathbb{F}$. $K/\mathbb{F}(x)$ is finite.

Lema (5.5)

For any integer $n \geq 0$ the number of effective divisors of degree n is finite.

Proof. (Sketch).

Choose an $x \in K$ such that x is transcendental over $\mathbb{F}$. $K/\mathbb{F}(x)$ is finite. The primes of $\mathbb{F}(x)$ are in one to one correspondence with the monic irreducibles polynomials in $\mathbb{F}[x]$ with the one exception of the prime at infinity.

Lema (5.5)

For any integer $n \geq 0$ the number of effective divisors of degree n is finite.

Proof. (Sketch).

Choose an $x \in K$ such that x is transcendental over $\mathbb{F}$. $K/\mathbb{F}(x)$ is finite. The primes of $\mathbb{F}(x)$ are in one to one correspondence with the monic irreducibles polynomials in $\mathbb{F}[x]$ with the one exception of the prime at infinity. Thus, there are only finitely many primes of $\mathbb{F}(x)$ of any fixed degree. By standard theorems on extensions of primes one sees that there are only finitely many primes of K of fixed degree.

Lema (5.5)

For any integer $n \geq 0$ the number of effective divisors of degree n is finite.

Proof. (Sketch).

Choose an $x \in K$ such that x is transcendental over $\mathbb{F}$. $K/\mathbb{F}(x)$ is finite. The primes of $\mathbb{F}(x)$ are in one to one correspondence with the monic irreducibles polynomials in $\mathbb{F}[x]$ with the one exception of the prime at infinity. Thus, there are only finitely many primes of $\mathbb{F}(x)$ of any fixed degree. By standard theorems on extensions of primes one sees that there are only finitely many primes of K of fixed degree. If $\sum_P a(P)P$ is an effective divisor of degree n then each prime that occurs with positive coefficient must have degree $\leq n$.

Lema (5.5)

For any integer $n \geq 0$ the number of effective divisors of degree n is finite.

Proof. (Sketch).

Choose an $x \in K$ such that x is transcendental over $\mathbb{F}$. $K/\mathbb{F}(x)$ is finite. The primes of $\mathbb{F}(x)$ are in one to one correspondence with the monic irreducibles polynomials in $\mathbb{F}[x]$ with the one exception of the prime at infinity. Thus, there are only finitely many primes of $\mathbb{F}(x)$ of any fixed degree. By standard theorems on extensions of primes one sees that there are only finitely many primes of K of fixed degree. If $\sum_P a(P)P$ is an effective divisor of degree n then each prime that occurs with positive coefficient must have degree $\leq n$. There are only finitely many such primes. Moreover the coefficients must be $\leq n$, so there are at most finitely many such effective divisors. □

Lema (5.5)

For any integer $n \geq 0$ the number of effective divisors of degree n is finite.

Proof. (Sketch).

Choose an $x \in K$ such that x is transcendental over $\mathbb{F}$. $K/\mathbb{F}(x)$ is finite. The primes of $\mathbb{F}(x)$ are in one to one correspondence with the monic irreducibles polynomials in $\mathbb{F}[x]$ with the one exception of the prime at infinity. Thus, there are only finitely many primes of $\mathbb{F}(x)$ of any fixed degree. By standard theorems on extensions of primes one sees that there are only finitely many primes of K of fixed degree. If $\sum_P a(P)P$ is an effective divisor of degree n then each prime that occurs with positive coefficient must have degree $\leq n$. There are only finitely many such primes. Moreover the coefficients must be $\leq n$, so there are at most finitely many such effective divisors. □

We define a_n to be the **number of primes of degree** n and b_n to be the **number of effective divisors of degree** n. Both these numbers are of considerable interest.

Lema (5.6)

The number of divisors classes of degree zero, h_K, is finite.

Lema (5.6)

The number of divisors classes of degree zero, h_K, is finite.

This lemma proves that the class number $h_K = |Cl_K^0|$ is finite.

Lema (5.6)

The number of divisors classes of degree zero, h_K, is finite.

This lemma proves that the class number $h_K = |Cl_K^0|$ is finite. Later we will give estimates for the size of h_K derived from the Riemann hypothesis for function fields.

Lema (5.6)

The number of divisors classes of degree zero, h_K, is finite.

This lemma proves that the class number $h_K = |Cl_K^0|$ is finite. Later we will give estimates for the size of h_K derived from the Riemann hypothesis for function fields.

Lema (5.7)

For any divisor A, the number of effective divisors in $\overline{A}$ is $\frac{q^{l(A)}-1}{q-1}$.

Zeta Functions for Function Fields

For $A \in \mathcal{D}_K$ define the norm of A, $NA = q^{\deg(A)}$.

Zeta Functions for Function Fields

For $A \in \mathcal{D}_K$ define the norm of A, $NA = q^{\deg(A)}$. Note that NA is a positive integer and that for any two divisors A and B we have $N(A + B) = NANB$.

Zeta Functions for Function Fields

For $A \in \mathcal{D}_K$ define the norm of A, $NA = q^{\deg(A)}$. Note that NA is a positive integer and that for any two divisors A and B we have $N(A+B) = NANB$.

Definition

The zeta function of K, $\zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_{A \geq 0} NA^{-s}.$$

Zeta Functions for Function Fields

For $A \in \mathcal{D}_K$ define the norm of A, $NA = q^{\deg(A)}$. Note that NA is a positive integer and that for any two divisors A and B we have $N(A + B) = NANB$.

Definition

The zeta function of K, $\zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_{A \geq 0} NA^{-s}.$$

Over the rational function field $k = \mathbb{F}(T)$ we did not have discussed the zeta function of k but rather the zeta function associated to the ring $A = \mathbb{F}[T]$.

Zeta Functions for Function Fields

For $A \in \mathcal{D}_K$ define the norm of A, $NA = q^{\deg(A)}$. Note that NA is a positive integer and that for any two divisors A and B we have $N(A+B) = NANB$.

Definition

The zeta function of K, $\zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_{A \geq 0} NA^{-s}.$$

Over the rational function field $k = \mathbb{F}(T)$ we did not have discussed the zeta function of k but rather the zeta function associated to the ring $A = \mathbb{F}[T]$. These are closely related. In fact, it is not hard to prove that $\zeta_A(s) = \zeta_k(s)(1 - q^{-s})$ (exercise), so $\zeta_k(s) = (1 - q^{1-s})^{-1}(1 - q^{-s})^{-1}$.

Zeta Functions for Function Fields

For $A \in \mathcal{D}_K$ define the norm of A, $NA = q^{\deg(A)}$. Note that NA is a positive integer and that for any two divisors A and B we have $N(A+B) = NANB$.

Definition

The zeta function of K, $\zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_{A \geq 0} NA^{-s}.$$

Over the rational function field $k = \mathbb{F}(T)$ we did not have discussed the zeta function of k but rather the zeta function associated to the ring $A = \mathbb{F}[T]$. These are closely related. In fact, it is not hard to prove that $\zeta_A(s) = \zeta_k(s)(1 - q^{-s})$ (exercise), so $\zeta_k(s) = (1 - q^{1-s})^{-1}(1 - q^{-s})^{-1}$. The term NA^{-s} in the definition of the zeta function is equal to q^{-ns} where n is the degree of A.

Zeta Functions for Function Fields

For $A \in \mathcal{D}_K$ define the norm of A, $NA = q^{\deg(A)}$. Note that NA is a positive integer and that for any two divisors A and B we have $N(A + B) = NANB$.

Definition

The zeta function of K, $\zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_{A \geq 0} NA^{-s}.$$

Over the rational function field $k = \mathbb{F}(T)$ we did not have discussed the zeta function of k but rather the zeta function associated to the ring $A = \mathbb{F}[T]$. These are closely related. In fact, it is not hard to prove that $\zeta_A(s) = \zeta_k(s)(1 - q^{-s})$ (exercise), so $\zeta_k(s) = (1 - q^{1-s})^{-1}(1 - q^{-s})^{-1}$. The term NA^{-s} in the definition of the zeta function is equal to q^{-ns} where n is the degree of A. Thus the zeta function can be rewritten in the form

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{b_n}{q^{ns}}.$$

Using the multiplicativity of the norm and the fact that $\mathcal{D}_K$ is a free abelian group on the set of primes we see, at least formally, that

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{NP^s}\right)^{-1}.$$

Using the multiplicativity of the norm and the fact that $\mathcal{D}_K$ is a free abelian group on the set of primes we see, at least formally, that

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{NP^s}\right)^{-1}.$$

Recalling that a_n is the number of primes of degree n, we observe that this expression can be rewritten as follows:

$$\zeta_K(s) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-a_n}.$$

Using the multiplicativity of the norm and the fact that $\mathcal{D}_K$ is a free abelian group on the set of primes we see, at least formally, that

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{NP^s}\right)^{-1}.$$

Recalling that a_n is the number of primes of degree n, we observe that this expression can be rewritten as follows:

$$\zeta_K(s) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-a_n}.$$

We shall soon see that all these expressions converge absolutely for $\mathfrak{R}(s) > 1$ and define analytic functions in this region.

Using the multiplicativity of the norm and the fact that $\mathcal{D}_K$ is a free abelian group on the set of primes we see, at least formally, that

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{NP^s}\right)^{-1}.$$

Recalling that a_n is the number of primes of degree n, we observe that this expression can be rewritten as follows:

$$\zeta_K(s) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-a_n}.$$

We shall soon see that all these expressions converge absolutely for $\Re(s) > 1$ and define analytic functions in this region.

Lema (5.8)

Let $h = h_K$. For every integer n, there are h divisor classes of degree n. Suppose $n \geq 0$ and that $\left\{\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_h\right\}$ are the divisors classes of degree n.

Using the multiplicativity of the norm and the fact that $\mathcal{D}_K$ is a free abelian group on the set of primes we see, at least formally, that

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{NP^s}\right)^{-1}.$$

Recalling that a_n is the number of primes of degree n, we observe that this expression can be rewritten as follows:

$$\zeta_K(s) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-a_n}.$$

We shall soon see that all these expressions converge absolutely for $\Re(s) > 1$ and define analytic functions in this region.

Lema (5.8)

Let $h = h_K$. For every integer n, there are h divisor classes of degree n. Suppose $n \geq 0$ and that $\left\{\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_h\right\}$ are the divisors classes of degree n. Then the number of effective divisors of degree n, b_n, is given by $\sum_{i=1}^{h} \frac{q^{l(A_i)}-1}{q-1}$.

Using the multiplicativity of the norm and the fact that $\mathcal{D}_K$ is a free abelian group on the set of primes we see, at least formally, that

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{NP^s}\right)^{-1}.$$

Recalling that a_n is the number of primes of degree n, we observe that this expression can be rewritten as follows:

$$\zeta_K(s) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-a_n}.$$

We shall soon see that all these expressions converge absolutely for $\Re(s) > 1$ and define analytic functions in this region.

Lema (5.8)

Let $h = h_K$. For every integer n, there are h divisor classes of degree n. Suppose $n \geq 0$ and that $\left\{\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_h\right\}$ are the divisors classes of degree n. Then the number of effective divisors of degree n, b_n, is given by $\sum_{i=1}^{h} \frac{q^{l(A_i)}-1}{q-1}$.

Proof.

The first assertion follows directly from Lemma 5.6 and the remarks preceding Lemma 5.5.

Using the multiplicativity of the norm and the fact that $\mathcal{D}_K$ is a free abelian group on the set of primes we see, at least formally, that

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{NP^s}\right)^{-1}.$$

Recalling that a_n is the number of primes of degree n, we observe that this expression can be rewritten as follows:

$$\zeta_K(s) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-a_n}.$$

We shall soon see that all these expressions converge absolutely for $\mathfrak{R}(s) > 1$ and define analytic functions in this region.

Lema (5.8)

Let $h = h_K$. For every integer n, there are h divisor classes of degree n. Suppose $n \geq 0$ and that $\left\{\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_h\right\}$ are the divisors classes of degree n. Then the number of effective divisors of degree n, b_n, is given by $\sum_{i=1}^{h} \frac{q^{l(A_i)}-1}{q-1}$.

Proof.

The first assertion follows directly from Lemma 5.6 and the remarks preceding Lemma 5.5. The second follows just as directly from Lemmas 5.6 and 5.7. □

By Lemma 5.7 and Corollary 4 to Riemann-Roch Theorem we see that if $n > 2g - 2$, then $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$.

By Lemma 5.7 and Corollary 4 to Riemann-Roch Theorem we see that if $n > 2g - 2$, then $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. It follows that $b_n = O(q^n)$. From this fact, and the expression $\zeta_K(s) = \sum_{n=0}^{\infty} b_n q^{-ns}$, it follows that $\zeta_K(s)$ converges absolutely for all s with $\Re(s) > 1$.

By Lemma 5.7 and Corollary 4 to Riemann-Roch Theorem we see that if $n > 2g - 2$, then $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. It follows that $b_n = O(q^n)$. From this fact, and the expression $\zeta_K(s) = \sum_{n=0}^{\infty} b_n q^{-ns}$, it follows that $\zeta_K(s)$ converges absolutely for all s with $\mathfrak{R}(s) > 1$.

In the same way we can prove the product expression for $\zeta_K(s)$ converges absolutely for $\mathfrak{R}(s) > 1$.

By Lemma 5.7 and Corollary 4 to Riemann-Roch Theorem we see that if $n > 2g - 2$, then $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. It follows that $b_n = O(q^n)$. From this fact, and the expression $\zeta_K(s) = \sum_{n=0}^{\infty} b_n q^{-ns}$, it follows that $\zeta_K(s)$ converges absolutely for all s with $\Re(s) > 1$.

In the same way we can prove the product expression for $\zeta_K(s)$ converges absolutely for $\Re(s) > 1$. To do this it suffices, by the theory of infinite products, to show that $\sum_{n=1}^{\infty} a_n |q^{-ns}|$ converges in this region. This follows immediately since $a_n \leq b_n = O(q^n)$.

By Lemma 5.7 and Corollary 4 to Riemann-Roch Theorem we see that if $n > 2g - 2$, then $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. It follows that $b_n = O(q^n)$. From this fact, and the expression $\zeta_K(s) = \sum_{n=0}^{\infty} b_n q^{-ns}$, it follows that $\zeta_K(s)$ converges absolutely for all s with $\Re(s) > 1$.

In the same way we can prove the product expression for $\zeta_K(s)$ converges absolutely for $\Re(s) > 1$. To do this it suffices, by the theory of infinite products, to show that $\sum_{n=1}^{\infty} a_n |q^{-ns}|$ converges in this region. This follows immediately since $a_n \leq b_n = O(q^n)$.

The next thing to do is to investigate wheter $\zeta_K(s)$ can be analytically continued to all of $\mathbb{C}$ and wheter it satisfies a functional equation, etc. The next theorem shows that the answer to both these questions is yes, and that a lot more is true as well.

Theorem (5.9)

Let K be a function field in one variable with a finite constant field $\mathbb{F}$ with q elements. Suppose that the genus of K is g.

Theorem (5.9)

Let K be a function field in one variable with a finite constant field $\mathbb{F}$ with q elements. Suppose that the genus of K is g. Then there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$ such that

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

Theorem (5.9)

Let K be a function field in one variable with a finite constant field $\mathbb{F}$ with q elements. Suppose that the genus of K is g. Then there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$ such that

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

This holds for all s such that $\Re(s) > 1$ and the right-hand side provides an analytic continuation of $\zeta_K(s)$ to all of $\mathbb{C}$. $\zeta_k(s)$ has simple poles at $s = 0$ and $s = 1$.

Theorem (5.9)

Let K be a function field in one variable with a finite constant field $\mathbb{F}$ with q elements. Suppose that the genus of K is g. Then there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$ such that

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

This holds for all s such that $\Re(s) > 1$ and the right-hand side provides an analytic continuation of $\zeta_K(s)$ to all of $\mathbb{C}$. $\zeta_k(s)$ has simple poles at $s = 0$ and $s = 1$. One has $L_K(0) = 1$,

Theorem (5.9)

Let K be a function field in one variable with a finite constant field $\mathbb{F}$ with q elements. Suppose that the genus of K is g. Then there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$ such that

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

This holds for all s such that $\Re(s) > 1$ and the right-hand side provides an analytic continuation of $\zeta_K(s)$ to all of $\mathbb{C}$. $\zeta_k(s)$ has simple poles at $s = 0$ and $s = 1$. One has $L_K(0) = 1$, $L_K^{'}(0) = a_1 - 1 - q$,

Theorem (5.9)

Let K be a function field in one variable with a finite constant field $\mathbb{F}$ with q elements. Suppose that the genus of K is g. Then there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$ such that

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

This holds for all s such that $\Re(s) > 1$ and the right-hand side provides an analytic continuation of $\zeta_K(s)$ to all of $\mathbb{C}$. $\zeta_k(s)$ has simple poles at $s = 0$ and $s = 1$. One has $L_K(0) = 1$, $L_K^{'}(0) = a_1 - 1 - q$, and $L_K(1) = h_K$.

Theorem (5.9)

Let K be a function field in one variable with a finite constant field $\mathbb{F}$ with q elements. Suppose that the genus of K is g. Then there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$ such that

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

This holds for all s such that $\Re(s) > 1$ and the right-hand side provides an analytic continuation of $\zeta_K(s)$ to all of $\mathbb{C}$. $\zeta_k(s)$ has simple poles at $s = 0$ and $s = 1$. One has $L_K(0) = 1$, $L_K^{'}(0) = a_1 - 1 - q$, and $L_K(1) = h_K$. Finally, set $\xi_K(s) = q^{(g-1)s}\zeta_K(s)$. Then for all s one has $\xi_K(1-s) = \xi_K(s)$ (this relationship is referred to as the functional equation for $\zeta_K(s)$).

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$.

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

We noted earlier that for $n > 2g - 2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$.

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

We noted earlier that for $n > 2g-2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. Substituting this into the above formula and summing the geometric series, yields

$$Z_K(u) = \sum_{n=0}^{2g-2} b_n u^n + \frac{h_K}{q-1}\left(\frac{q^g}{1-qu} - \frac{1}{1-u}\right)u^{2g-1}. \tag{3.1}$$

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

We noted earlier that for $n > 2g - 2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. Substituting this into the above formula and summing the geometric series, yields

$$Z_K(u) = \sum_{n=0}^{2g-2} b_n u^n + \frac{h_K}{q-1} \left(\frac{q^g}{1-qu} - \frac{1}{1-u} \right) u^{2g-1}. \tag{3.1}$$

From this, simple algebraic manipulation shows

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)} \qquad \text{with } L_K(u) \in \mathbb{Z}[u]. \tag{3.2}$$

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

We noted earlier that for $n > 2g-2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. Substituting this into the above formula and summing the geometric series, yields

$$Z_K(u) = \sum_{n=0}^{2g-2} b_n u^n + \frac{h_K}{q-1} \left(\frac{q^g}{1-qu} - \frac{1}{1-u} \right) u^{2g-1}. \qquad (3.1)$$

From this, simple algebraic manipulation shows

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)} \qquad \text{with } L_K(u) \in \mathbb{Z}[u]. \qquad (3.2)$$

From (3.2), we see the expression for $\zeta_k(s)$ given in the theorem is correct. We will show that $L_K(1)$ and $L_K(q^{-1})$ are both non-zero.

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

We noted earlier that for $n > 2g-2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. Substituting this into the above formula and summing the geometric series, yields

$$Z_K(u) = \sum_{n=0}^{2g-2} b_n u^n + \frac{h_K}{q-1}\left(\frac{q^g}{1-qu} - \frac{1}{1-u}\right) u^{2g-1}. \tag{3.1}$$

From this, simple algebraic manipulation shows

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)} \qquad \text{with } L_K(u) \in \mathbb{Z}[u]. \tag{3.2}$$

From (3.2), we see the expression for $\zeta_k(s)$ given in the theorem is correct. We will show that $L_K(1)$ and $L_K(q^{-1})$ are both non-zero. Thus, $\zeta_K(s)$ has a pole at 0 and 1. The fact that $\deg L_K(u) \leq 2g$ also follows from this calculation.

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

We noted earlier that for $n > 2g - 2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. Substituting this into the above formula and summing the geometric series, yields

$$Z_K(u) = \sum_{n=0}^{2g-2} b_n u^n + \frac{h_K}{q-1}\left(\frac{q^g}{1-qu} - \frac{1}{1-u}\right) u^{2g-1}. \qquad (3.1)$$

From this, simple algebraic manipulation shows

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)} \qquad \text{with } L_K(u) \in \mathbb{Z}[u]. \qquad (3.2)$$

From (3.2), we see the expression for $\zeta_k(s)$ given in the theorem is correct. We will show that $L_K(1)$ and $L_K(q^{-1})$ are both non-zero. Thus, $\zeta_K(s)$ has a pole at 0 and 1. The fact that $\deg L_K(u) \leq 2g$ also follows from this calculation. Substituting $u = 0$ yields $L_K(0) = 1$.

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

We noted earlier that for $n > 2g - 2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. Substituting this into the above formula and summing the geometric series, yields

$$Z_K(u) = \sum_{n=0}^{2g-2} b_n u^n + \frac{h_K}{q-1}\left(\frac{q^g}{1-qu} - \frac{1}{1-u}\right) u^{2g-1}. \tag{3.1}$$

From this, simple algebraic manipulation shows

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)} \qquad \text{with } L_K(u) \in \mathbb{Z}[u]. \tag{3.2}$$

From (3.2), we see the expression for $\zeta_k(s)$ given in the theorem is correct. We will show that $L_K(1)$ and $L_K(q^{-1})$ are both non-zero. Thus, $\zeta_K(s)$ has a pole at 0 and 1. The fact that $\deg L_K(u) \leq 2g$ also follows from this calculation. Substituting $u = 0$ yields $L_K(0) = 1$. Comparing the coefficients of u on both sides yields $b_1 = L_K^{'}(0) + 1 + q$.

Proof of Theorem 5.9

We work with the variable $u = q^{-s}$. Then

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

We noted earlier that for $n > 2g-2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. Substituting this into the above formula and summing the geometric series, yields

$$Z_K(u) = \sum_{n=0}^{2g-2} b_n u^n + \frac{h_K}{q-1}\left(\frac{q^g}{1-qu} - \frac{1}{1-u}\right) u^{2g-1}. \tag{3.1}$$

From this, simple algebraic manipulation shows

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)} \qquad \text{with } L_K(u) \in \mathbb{Z}[u]. \tag{3.2}$$

From (3.2), we see the expression for $\zeta_k(s)$ given in the theorem is correct. We will show that $L_K(1)$ and $L_K(q^{-1})$ are both non-zero. Thus, $\zeta_K(s)$ has a pole at 0 and 1. The fact that $\deg L_K(u) \leq 2g$ also follows from this calculation. Substituting $u = 0$ yields $L_K(0) = 1$. Comparing the coefficients of u on both sides yields $b_1 = L_K^{'}(0) + 1 + q$. It is easy to see that $b_1 = a_1 =$ the number of primes of K of degree one.

Continuation of the Proof

From Equation (3.1), we see that $\lim_{u \to 1}(u-1)Z_K(u) = h_K/(q-1)$.

Continuation of the Proof

From Equation (3.1), we see that $\lim_{u\to 1}(u-1)Z_K(u) = h_K/(q-1)$. From Equation (3.2) we see

$$\lim_{u\to 1}(u-1)Z_K(u) = -\frac{L_K(1)}{1-q}.$$

Continuation of the Proof

From Equation (3.1), we see that $\lim_{u\to 1}(u-1)Z_K(u) = h_K/(q-1)$. From Equation (3.2) we see

$$\lim_{u\to 1}(u-1)Z_K(u) = -\frac{L_K(1)}{1-q}.$$

Thus, $L_K(1) = h_K$, as asserted.

Continuation of the Proof

From Equation (3.1), we see that $\lim_{u\to 1}(u-1)Z_K(u) = h_K/(q-1)$. From Equation (3.2) we see

$$\lim_{u\to 1}(u-1)Z_K(u) = -\frac{L_K(1)}{1-q}.$$

Thus, $L_K(1) = h_K$, as asserted.

As for the functional equation, recall that $b_n = \sum_{\deg \overline{A}=n}(q^{l(\overline{A})}-1)/(q-1)$. Then,

Continuation of the Proof

From Equation (3.1), we see that $\lim_{u\to 1}(u-1)Z_K(u) = h_K/(q-1)$. From Equation (3.2) we see

$$\lim_{u\to 1}(u-1)Z_K(u) = -\frac{L_K(1)}{1-q}.$$

Thus, $L_K(1) = h_K$, as asserted.

As for the functional equation, recall that $b_n = \sum_{\deg \overline{A}=n}(q^{l(\overline{A})}-1)/(q-1)$. Then,

$$(q-1)Z_K(u) \quad = \quad \sum_{n=0}^{\infty}\left(\sum_{\deg \overline{A}=n} q^{l(\overline{A})} - 1\right)u^n = \sum_{\deg \overline{A}\geq 0} q^{l(\overline{A})}u^{\deg \overline{A}} - h_K\frac{1}{1-u}$$

Continuation of the Proof

From Equation (3.1), we see that $\lim_{u\to 1}(u-1)Z_K(u) = h_K/(q-1)$. From Equation (3.2) we see

$$\lim_{u\to 1}(u-1)Z_K(u) = -\frac{L_K(1)}{1-q}.$$

Thus, $L_K(1) = h_K$, as asserted.

As for the functional equation, recall that $b_n = \sum_{\deg\overline{A}=n}(q^{l(\overline{A})}-1)/(q-1)$. Then,

$$\begin{aligned}(q-1)Z_K(u) &= \sum_{n=0}^{\infty}\left(\sum_{\deg\overline{A}=n} q^{l(\overline{A})} - 1\right)u^n = \sum_{\deg\overline{A}\geq 0} q^{l(\overline{A})}u^{\deg\overline{A}} - h_K\frac{1}{1-u} \\ &= \sum_{0\leq\deg\overline{A}\leq 2g-2} q^{l(\overline{A})}u^{\deg\overline{A}} - h_K\frac{1}{1-u} + \sum_{2g-2\leq\deg\overline{A}<\infty} q^{l(\overline{A})}u^{\deg\overline{A}}\end{aligned}$$

Continuation of the Proof

From Equation (3.1), we see that $\lim_{u\to 1}(u-1)Z_K(u) = h_K/(q-1)$. From Equation (3.2) we see

$$\lim_{u\to 1}(u-1)Z_K(u) = -\frac{L_K(1)}{1-q}.$$

Thus, $L_K(1) = h_K$, as asserted.

As for the functional equation, recall that $b_n = \sum_{\deg \overline{A}=n}(q^{l(\overline{A})}-1)/(q-1)$. Then,

$$\begin{aligned}
(q-1)Z_K(u) &= \sum_{n=0}^{\infty}\left(\sum_{\deg \overline{A}=n} q^{l(\overline{A})} - 1\right)u^n = \sum_{\deg \overline{A}\geq 0} q^{l(\overline{A})}u^{\deg \overline{A}} - h_K\frac{1}{1-u} \\
&= \sum_{0\leq \deg \overline{A}\leq 2g-2} q^{l(\overline{A})}u^{\deg \overline{A}} - h_K\frac{1}{1-u} + \sum_{2g-2\leq \deg \overline{A}<\infty} q^{l(\overline{A})}u^{\deg \overline{A}} \\
&= \sum_{0\leq \deg \overline{A}\leq 2g-2} q^{l(\overline{A})}u^{\deg \overline{A}} - h_K\frac{1}{1-u} + h_K\frac{q^g u^{2g-1}}{1-qu}.
\end{aligned}$$

Continuation of the Proof

Multiplying both sides by u^{1-g} we have $(q-1)u^{1-g}Z_K(u) = R(u)+S(u)$ where

$$R(u) = \sum_{0\le \deg \overline{A} \le 2g-2} q^{l(\overline{A})} u^{\deg \overline{A} - g+1} \qquad \text{and} \quad S(u) = -h_K \frac{u^{1-g}}{1-u} + h_K \frac{q^g u^g}{1-qu}.$$

Continuation of the Proof

Multiplying both sides by u^{1-g} we have $(q-1)u^{1-g}Z_K(u) = R(u) + S(u)$ where

$$R(u) = \sum_{0 \leq \deg \overline{A} \leq 2g-2} q^{l(\overline{A})} u^{\deg \overline{A} - g + 1} \qquad \text{and} \quad S(u) = -h_K \frac{u^{1-g}}{1-u} + h_K \frac{q^g u^g}{1-qu}.$$

A direct calculation shows that $R(u)$ and $S(u)$ are invariant under $u \to q^{-1}u^{-1}$.

Continuation of the Proof

Multiplying both sides by u^{1-g} we have $(q-1)u^{1-g}Z_K(u) = R(u) + S(u)$ where

$$R(u) = \sum_{0 \leq \deg \overline{A} \leq 2g-2} q^{l(\overline{A})} u^{\deg \overline{A} - g + 1} \qquad \text{and} \quad S(u) = -h_K \frac{u^{1-g}}{1-u} + h_K \frac{q^g u^g}{1-qu}.$$

A direct calculation shows that $R(u)$ and $S(u)$ are invariant under $u \to q^{-1}u^{-1}$. To see this, first note that

$$R(q^{-1}u^{-1}) = \sum_{\deg \overline{A} \leq 2g-2} q^{l(\overline{A}) + g - 1 - \deg \overline{A}} u^{-\deg \overline{A} + g - 1}.$$

Continuation of the Proof

Multiplying both sides by u^{1-g} we have $(q-1)u^{1-g}Z_K(u) = R(u) + S(u)$ where

$$R(u) = \sum_{0 \leq \deg \overline{A} \leq 2g-2} q^{l(\overline{A})} u^{\deg \overline{A} - g + 1} \qquad \text{and} \quad S(u) = -h_K \frac{u^{1-g}}{1-u} + h_K \frac{q^g u^g}{1-qu}.$$

A direct calculation shows that $R(u)$ and $S(u)$ are invariant under $u \to q^{-1}u^{-1}$. To see this, first note that

$$R(q^{-1}u^{-1}) = \sum_{\deg \overline{A} \leq 2g-2} q^{l(\overline{A}) + g - 1 - \deg \overline{A}} u^{-\deg \overline{A} + g - 1}.$$

From the Riemann-Roch Theorem and Corollary 3, we see

$$l(\mathcal{C} - \overline{A}) = deg(\mathcal{C} - A) - g + 1 + l(\overline{A}) = g - 1 - \deg \overline{A} + l(\overline{A}).$$

Continuation of the Proof

Multiplying both sides by u^{1-g} we have $(q-1)u^{1-g}Z_K(u) = R(u) + S(u)$ where

$$R(u) = \sum_{0 \leq \mathrm{deg}\overline{A} \leq 2g-2} q^{l(\overline{A})} u^{\mathrm{deg}\overline{A} - g + 1} \qquad \text{and} \quad S(u) = -h_K \frac{u^{1-g}}{1-u} + h_K \frac{q^g u^g}{1-qu}.$$

A direct calculation shows that $R(u)$ and $S(u)$ are invariant under $u \to q^{-1}u^{-1}$. To see this, first note that

$$R(q^{-1}u^{-1}) = \sum_{\mathrm{deg}\overline{A} \leq 2g-2} q^{l(\overline{A}) + g - 1 - \mathrm{deg}\overline{A}} u^{-\mathrm{deg}\overline{A} + g - 1}.$$

From the Riemann-Roch Theorem and Corollary 3, we see

$$l(\mathcal{C} - \overline{A}) = deg(\mathcal{C} - A) - g + 1 + l(\overline{A}) = g - 1 - \mathrm{deg}\overline{A} + l(\overline{A}).$$

Substituting this expression into the formula for $R(q^{-1}u^{-1})$ yields

$$R(q^{-1}u^{-1}) = \sum_{\mathrm{deg}\overline{A} \leq 2g-2} q^{l(\mathcal{C} - \overline{A})} u^{\mathrm{deg}(\mathcal{C} - \overline{A}) - g + 1}.$$

Continuation of the Proof

Since $\overline{A} \to \mathcal{C} - \overline{A}$ is a permutation of the divisor classes of degree d with $0 \leq d \leq 2g-2$ it follows that $R(q^{-1}u^{-1}) = R(u)$ as asserted. We have now completed the proof that $u^{1-g}Z_K(u)$ is invariant under the transformation $u \to q^{-1}u^{-1}$.

Continuation of the Proof

Since $\overline{A} \to \mathcal{C} - \overline{A}$ is a permutation of the divisor classes of degree d with $0 \leq d \leq 2g - 2$ it follows that $R(q^{-1}u^{-1}) = R(u)$ as asserted. We have now completed the proof that $u^{1-g}Z_K(u)$ is invariant under the transformation $u \to q^{-1}u^{-1}$.

Since $u^{1-g}Z_K(u)$ is invariant under $u \to q^{-1}u^{-1}$, it follows easily that $q^{-g}u^{-2g}L_K(u) = L_K(q^{-1}u^{-1})$.

Continuation of the Proof

Since $\overline{A} \to \mathcal{C} - \overline{A}$ is a permutation of the divisor classes of degree d with $0 \leq d \leq 2g - 2$ it follows that $R(q^{-1}u^{-1}) = R(u)$ as asserted. We have now completed the proof that $u^{1-g}Z_K(u)$ is invariant under the transformation $u \to q^{-1}u^{-1}$.

Since $u^{1-g}Z_K(u)$ is invariant under $u \to q^{-1}u^{-1}$, it follows easily that $q^{-g}u^{-2g}L_K(u) = L_K(q^{-1}u^{-1})$. Letting $u \to \infty$ we see that $\deg L_K(u) = 2g$ and that the highest degree term is $q^g u^{2g}$.

Continuation of the Proof

Since $\overline{A} \to \mathcal{C} - \overline{A}$ is a permutation of the divisor classes of degree d with $0 \leq d \leq 2g - 2$ it follows that $R(q^{-1}u^{-1}) = R(u)$ as asserted. We have now completed the proof that $u^{1-g}Z_K(u)$ is invariant under the transformation $u \to q^{-1}u^{-1}$.

Since $u^{1-g}Z_K(u)$ is invariant under $u \to q^{-1}u^{-1}$, it follows easily that $q^{-g}u^{-2g}L_K(u) = L_K(q^{-1}u^{-1})$. Letting $u \to \infty$ we see that $\deg L_K(u) = 2g$ and that the highest degree term is $q^g u^{2g}$.

Finally, recalling that $u = q^{-s}$, we see that $u^{1-g} = q^{(g-1)s}$ and the transformation $u \to q^{-1}u^{-1}$ is the same as the transformation $s \to 1 - s$.

Continuation of the Proof

Since $\overline{A} \to \mathcal{C} - \overline{A}$ is a permutation of the divisor classes of degree d with $0 \leq d \leq 2g-2$ it follows that $R(q^{-1}u^{-1}) = R(u)$ as asserted. We have now completed the proof that $u^{1-g}Z_K(u)$ is invariant under the transformation $u \to q^{-1}u^{-1}$.

Since $u^{1-g}Z_K(u)$ is invariant under $u \to q^{-1}u^{-1}$, it follows easily that $q^{-g}u^{-2g}L_K(u) = L_K(q^{-1}u^{-1})$. Letting $u \to \infty$ we see that $\deg L_K(u) = 2g$ and that the highest degree term is $q^g u^{2g}$.

Finally, recalling that $u = q^{-s}$, we see that $u^{1-g} = q^{(g-1)s}$ and the transformation $u \to q^{-1}u^{-1}$ is the same as the transformation $s \to 1-s$. So passing from the u language to the s language we see we have shown $\xi_K(s)$ is invariant under $s \to 1-s$, as asserted. This completes the proof of the theorem.

□

The polynomial $L_K(u)$ defined in the theorem carries a lot of information.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g}(1 - \pi_i u).$$

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g} (1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g} (1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g}(1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$. Since $\zeta_K(s)$ has a convergent Euler product whose factors have no zeros in the region $\Re(s) > 1$, it follows that $\zeta_K(s)$ has no zeros there.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g}(1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$. Since $\zeta_K(s)$ has a convergent Euler product whose factors have no zeros in the region $\mathfrak{R}(s) > 1$, it follows that $\zeta_K(s)$ has no zeros there. Consequently, $L_K(u)$ has no zeros in the region $\left\{u \in \mathbb{C} : |u| < q^{-1}\right\}$.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g}(1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$. Since $\zeta_K(s)$ has a convergent Euler product whose factors have no zeros in the region $\Re(s) > 1$, it follows that $\zeta_K(s)$ has no zeros there. Consequently, $L_K(u)$ has no zeros in the region $\left\{u \in \mathbb{C} : |u| < q^{-1}\right\}$. For the inverse roots, π_i, the consequence is that $|\pi_i| \leq q$.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g}(1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$. Since $\zeta_K(s)$ has a convergent Euler product whose factors have no zeros in the region $\Re(s) > 1$, it follows that $\zeta_K(s)$ has no zeros there. Consequently, $L_K(u)$ has no zeros in the region $\left\{u \in \mathbb{C} : |u| < q^{-1}\right\}$. For the inverse roots, π_i, the consequence is that $|\pi_i| \leq q$. We will prove later that $|\pi_i| < q$ for all i and this will have a number of important applications.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g}(1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$. Since $\zeta_K(s)$ has a convergent Euler product whose factors have no zeros in the region $\Re(s) > 1$, it follows that $\zeta_K(s)$ has no zeros there. Consequently, $L_K(u)$ has no zeros in the region $\left\{u \in \mathbb{C} : |u| < q^{-1}\right\}$. For the inverse roots, π_i, the consequence is that $|\pi_i| \leq q$. We will prove later that $|\pi_i| < q$ for all i and this will have a number of important applications.

However, much more is true about the π_i.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g} (1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$. Since $\zeta_K(s)$ has a convergent Euler product whose factors have no zeros in the region $\Re(s) > 1$, it follows that $\zeta_K(s)$ has no zeros there. Consequently, $L_K(u)$ has no zeros in the region $\left\{u \in \mathbb{C} : |u| < q^{-1}\right\}$. For the inverse roots, π_i, the consequence is that $|\pi_i| \leq q$. We will prove later that $|\pi_i| < q$ for all i and this will have a number of important applications.

However, much more is true about the π_i. The classical generalized Riemann hypothesis states that the zeros of $\zeta_K(s)$, the Dedekind zeta function of a number field K, has all its non-trivial zeros on the line $\Re(s) = 1/2$.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g} (1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$. Since $\zeta_K(s)$ has a convergent Euler product whose factors have no zeros in the region $\Re(s) > 1$, it follows that $\zeta_K(s)$ has no zeros there. Consequently, $L_K(u)$ has no zeros in the region $\left\{u \in \mathbb{C} : |u| < q^{-1}\right\}$. For the inverse roots, π_i, the consequence is that $|\pi_i| \leq q$. We will prove later that $|\pi_i| < q$ for all i and this will have a number of important applications.

However, much more is true about the π_i. The classical generalized Riemann hypothesis states that the zeros of $\zeta_K(s)$, the Dedekind zeta function of a number field K, has all its non-trivial zeros on the line $\Re(s) = 1/2$. Riemann conjectured this for $\zeta(s)$, the Riemann zeta function. Neither Riemann's conjecture nor its generalizations are known to be true. In fact, these are among the most important unsolved problems in all of mathematics.

The polynomial $L_K(u)$ defined in the theorem carries a lot of information. Since the coefficients are in $\mathbb{Z}$ we can factor this polynomial over the complex numbers,

$$L_K(u) = \prod_{i=1}^{2g} (1 - \pi_i u).$$

It is worth pointing out that the relation $L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u)$ implies that the set $\{\pi_1, \pi_2, \ldots, \pi_{2g}\}$ is permuted by the transformation $\pi \to q/\pi$. This is easily seen to be equivalent to the functional equation for $\zeta_K(s)$. Since $\zeta_K(s)$ has a convergent Euler product whose factors have no zeros in the region $\Re(s) > 1$, it follows that $\zeta_K(s)$ has no zeros there. Consequently, $L_K(u)$ has no zeros in the region $\left\{u \in \mathbb{C} : |u| < q^{-1}\right\}$. For the inverse roots, π_i, the consequence is that $|\pi_i| \leq q$. We will prove later that $|\pi_i| < q$ for all i and this will have a number of important applications.

However, much more is true about the π_i. The classical generalized Riemann hypothesis states that the zeros of $\zeta_K(s)$, the Dedekind zeta function of a number field K, has all its non-trivial zeros on the line $\Re(s) = 1/2$. Riemann conjectured this for $\zeta(s)$, the Riemann zeta function. Neither Riemann's conjecture nor its generalizations are known to be true. In fact, these are among the most important unsolved problems in all of mathematics. However, the analogous statement over global function fields was proved by A. Weil in the 1940s.

The Riemann Hypothesis for Function Fields

Theorem (The Riemann Hypothesis for Function Fields)

Let K be a global function field whose constant field $\mathbb{F}$ has q elements. All the roots of $\zeta_K(s)$ lie on the line $\Re(s) = 1/2$. Equivalently, the inverse roots of $L_K(u)$ all have absolute value $\sqrt{q}$.

The Riemann Hypothesis for Function Fields

Theorem (The Riemann Hypothesis for Function Fields)

Let K be a global function field whose constant field $\mathbb{F}$ has q elements. All the roots of $\zeta_K(s)$ lie on the line $\Re(s) = 1/2$. Equivalently, the inverse roots of $L_K(u)$ all have absolute value $\sqrt{q}$.

1. The case $g = 1$ was proved by H. Hasse.

The Riemann Hypothesis for Function Fields

Theorem (The Riemann Hypothesis for Function Fields)

Let K be a global function field whose constant field $\mathbb{F}$ has q elements. All the roots of $\zeta_K(s)$ lie on the line $\Re(s) = 1/2$. Equivalently, the inverse roots of $L_K(u)$ all have absolute value $\sqrt{q}$.

1. The case $g = 1$ was proved by H. Hasse.
2. Weil gave two proofs: (i) geometry of algebraic surfaces and theory of correspondences; (ii) theory of abelian varieties.

The Riemann Hypothesis for Function Fields

Theorem (The Riemann Hypothesis for Function Fields)

Let K be a global function field whose constant field $\mathbb{F}$ has q elements. All the roots of $\zeta_K(s)$ lie on the line $\Re(s) = 1/2$. Equivalently, the inverse roots of $L_K(u)$ all have absolute value $\sqrt{q}$.

1. The case $g = 1$ was proved by H. Hasse.
2. Weil gave two proofs: (i) geometry of algebraic surfaces and theory of correspondences; (ii) theory of abelian varieties.
3. Stepanov and Bombieri gave more elementary proofs.

The Riemann Hypothesis for Function Fields

Theorem (The Riemann Hypothesis for Function Fields)

Let K be a global function field whose constant field $\mathbb{F}$ has q elements. All the roots of $\zeta_K(s)$ lie on the line $\Re(s) = 1/2$. Equivalently, the inverse roots of $L_K(u)$ all have absolute value $\sqrt{q}$.

1. The case $g = 1$ was proved by H. Hasse.
2. Weil gave two proofs: (i) geometry of algebraic surfaces and theory of correspondences; (ii) theory of abelian varieties.
3. Stepanov and Bombieri gave more elementary proofs.
4. No analytic proof is known. (A. Connes)

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K, a_1, *satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$. *Also,* $(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}$.

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K, a_1, *satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$. *Also,* $(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}$.

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$.

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K, a_1, *satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$. *Also,* $(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}$.

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$. From the above factorization of $L_K(u)$ we see $-L_K^{'}(0) = \pi_1 + \pi_2 + \cdots + \pi_{2g}$.

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K, a_1, *satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$. *Also,* $(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}$.

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$. From the above factorization of $L_K(u)$ we see $-L_K^{'}(0) = \pi_1 + \pi_2 + \cdots + \pi_{2g}$. The first assertion is immediate from this and the R.H. for function fields.

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K, a_1, *satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$. *Also,* $(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}$.

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$. From the above factorization of $L_K(u)$ we see $-L_K^{'}(0) = \pi_1 + \pi_2 + \cdots + \pi_{2g}$. The first assertion is immediate from this and the R.H. for function fields.

And for the second assertion, we have $h_K = L_K(1) = \prod_{i=1}^{2g}(1 - \pi_i)$, by Theorem 5.9. Now use the R.H for function fields. □

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K, a_1, *satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$. *Also,* $(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}$.

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$. From the above factorization of $L_K(u)$ we see $-L_K^{'}(0) = \pi_1 + \pi_2 + \cdots + \pi_{2g}$. The first assertion is immediate from this and the R.H. for function fields.

And for the second assertion, we have $h_K = L_K(1) = \prod_{i=1}^{2g}(1 - \pi_i)$, by Theorem 5.9. Now use the R.H for function fields. □

Remark

1. *If* q *is big compared to the genus, then there must exist primes of degree one.*

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K, a_1, *satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$. *Also,* $(\sqrt{q}-1)^{2g} \leq h_K \leq (\sqrt{q}+1)^{2g}$.

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$. From the above factorization of $L_K(u)$ we see $-L_K^{'}(0) = \pi_1 + \pi_2 + \cdots + \pi_{2g}$. The first assertion is immediate from this and the R.H. for function fields.

And for the second assertion, we have $h_K = L_K(1) = \prod_{i=1}^{2g}(1-\pi_i)$, by Theorem 5.9. Now use the R.H for function fields. □

Remark

1. *If* q *is big compared to the genus, then there must exist primes of degree one.*
2. $a_1/q \to 1$ *if we fix* g *and let* q *grow.*

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K, a_1, *satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$. *Also,* $(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}$.

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$. From the above factorization of $L_K(u)$ we see $-L_K^{'}(0) = \pi_1 + \pi_2 + \cdots + \pi_{2g}$. The first assertion is immediate from this and the R.H. for function fields.
And for the second assertion, we have $h_K = L_K(1) = \prod_{i=1}^{2g}(1 - \pi_i)$, by Theorem 5.9. Now use the R.H for function fields. □

Remark

1. *If* q *is big compared to the genus, then there must exist primes of degree one.*
2. $a_1/q \to 1$ *if we fix* g *and let* q *grow.*
3. *If* $q > 4$ *we must have* $h_K > 1$.

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K*,* a_1*, satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$*. Also,* $(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}$*.*

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$. From the above factorization of $L_K(u)$ we see $-L_K^{'}(0) = \pi_1 + \pi_2 + \cdots + \pi_{2g}$. The first assertion is immediate from this and the R.H. for function fields.

And for the second assertion, we have $h_K = L_K(1) = \prod_{i=1}^{2g}(1 - \pi_i)$, by Theorem 5.9. Now use the R.H for function fields. □

Remark

1. *If* q *is big compared to the genus, then there must exist primes of degree one.*
2. $a_1/q \to 1$ *if we fix* g *and let* q *grow.*
3. *If* $q > 4$ *we must have* $h_K > 1$*.*
4. *If we fix* g *and let* $q \to \infty$ *then* $h_K/q^g \to 1$*.*

Consequences of R.H.

Proposition (5.11)

The number of prime divisors of degree 1 *of* K*,* a_1*, satisfies the inequality* $|a_1 - q - 1| \leq 2g\sqrt{q}$*. Also,* $(\sqrt{q}-1)^{2g} \leq h_K \leq (\sqrt{q}+1)^{2g}$*.*

Proof.

By Theorem 5.9, $L_K^{'}(0) = a_1 - q - 1$. From the above factorization of $L_K(u)$ we see $-L_K^{'}(0) = \pi_1 + \pi_2 + \cdots + \pi_{2g}$. The first assertion is immediate from this and the R.H. for function fields.
And for the second assertion, we have $h_K = L_K(1) = \prod_{i=1}^{2g}(1-\pi_i)$, by Theorem 5.9. Now use the R.H for function fields. □

Remark

1. *If* q *is big compared to the genus, then there must exist primes of degree one.*
2. $a_1/q \to 1$ *if we fix* g *and let* q *grow.*
3. *If* $q > 4$ *we must have* $h_K > 1$*.*
4. *If we fix* g *and let* $q \to \infty$ *then* $h_K/q^g \to 1$*.*
5. *If we fix* $q > 4$ *and let* $g \to \infty$ *then* $h_K \to \infty$*.*

Prime Number Theorem for Function Fields

We now present a generalization of the prime number theorem, i.e, the prime number theorem for general function fields.

Prime Number Theorem for Function Fields

We now present a generalization of the prime number theorem, i.e, the prime number theorem for general function fields.

Theorem (5.12)

$$a_N = \# \{P : deg(P) = N\} = \frac{q^N}{N} + O\left(\frac{q^{\frac{N}{2}}}{N}\right).$$

Proof of Prime Number Theorem for Function Fields

Using Euler products decomposition and Theorem 5.9, we see

$$Z_K(u) = \frac{\prod_{i=1}^{2g}(1-\pi_i u)}{(1-u)(1-qu)} = \prod_{d=1}^{\infty}(i-u^d)^{-a_d}.$$

Proof of Prime Number Theorem for Function Fields

Using Euler products decomposition and Theorem 5.9, we see

$$Z_K(u) = \frac{\prod_{i=1}^{2g}(1-\pi_i u)}{(1-u)(1-qu)} = \prod_{d=1}^{\infty}(i-u^d)^{-a_d}.$$

Take the logarithmic derivative of both sides, multiply the result by u, and equate the coefficients of u^N on both sides. We find

$$q^N + 1 - \sum_{i=1}^{2g} \pi_i^N = \sum_{d|N} da_d.$$

Proof of Prime Number Theorem for Function Fields

Using Euler products decomposition and Theorem 5.9, we see

$$Z_K(u) = \frac{\prod_{i=1}^{2g}(1-\pi_i u)}{(1-u)(1-qu)} = \prod_{d=1}^{\infty}(i-u^d)^{-a_d}.$$

Take the logarithmic derivative of both sides, multiply the result by u, and equate the coefficients of u^N on both sides. We find

$$q^N + 1 - \sum_{i=1}^{2g}\pi_i^N = \sum_{d|N} da_d.$$

Using the Möbius inversion formula, yields

$$Na_N = \sum_{d|N}\mu(d)q^{\frac{N}{d}} + 0 + \sum_{d|N}\mu(d)\left(\sum_{i=1}^{2g}\pi_i^{\frac{N}{d}}\right).$$

Proof of Prime Number Theorem for Function Fields

Using Euler products decomposition and Theorem 5.9, we see

$$Z_K(u) = \frac{\prod_{i=1}^{2g}(1-\pi_i u)}{(1-u)(1-qu)} = \prod_{d=1}^{\infty}(i-u^d)^{-a_d}.$$

Take the logarithmic derivative of both sides, multiply the result by u, and equate the coefficients of u^N on both sides. We find

$$q^N + 1 - \sum_{i=1}^{2g} \pi_i^N = \sum_{d|N} da_d.$$

Using the Möbius inversion formula, yields

$$Na_N = \sum_{d|N} \mu(d) q^{\frac{N}{d}} + 0 + \sum_{d|N} \mu(d) \left(\sum_{i=1}^{2g} \pi_i^{\frac{N}{d}} \right).$$

Let $e(N)$ be -1 if N is even and 0 if N is odd. Then, as we saw in the proof of the PNT in $\mathbb{F}_q[T]$,

$$\sum_{d|N} \mu(d) q^{\frac{N}{d}} = q^N - e(N) q^{N/2} + O(Nq^{N/3}).$$

Continuation of the Proof

Similarly, using the R.H., we see

$$\left|\sum_{d|N}\mu(d)\left(\sum_{i=1}^{2g}\pi_i^{N/d}\right)\right| \leq 2gq^{N/2}+2gNq^{N/4}.$$

Continuation of the Proof

Similarly, using the R.H., we see

$$\left| \sum_{d|N} \mu(d) \left(\sum_{i=1}^{2g} \pi_i^{N/d} \right) \right| \leq 2gq^{N/2} + 2gNq^{N/4}.$$

Putting the last three equations together, we find

$$Na_N = q^N + O(q^{N/2}).$$

This completes the proof.

We derive now another expression for the zeta function. To this end consider once more the equation

$$Z_K(u) = \prod_{d=1}^{\infty}(1 - u^d)^{-a_d}.$$

We derive now another expression for the zeta function. To this end consider once more the equation

$$Z_K(u) = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Take the logarithm of both sides and write the result as power series in u.

$$\log Z_K(u) = \sum_{m=1}^{\infty} \frac{N_m}{m} u^m,$$

where the number $N_m = \sum_{d|m} da_d$.

We derive now another expression for the zeta function. To this end consider once more the equation

$$Z_K(u) = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Take the logarithm of both sides and write the result as power series in u.

$$\log Z_K(u) = \sum_{m=1}^{\infty} \frac{N_m}{m} u^m,$$

where the number $N_m = \sum_{d|m} da_d$.

These numbers have a very appealing geometric interpretation. Roughly speaking, what is going on is that the function field $K/\mathbb{F}$ is associated to a complete, non-singular curve X defined over $\mathbb{F}$.

We derive now another expression for the zeta function. To this end consider once more the equation

$$Z_K(u) = \prod_{d=1}^{\infty}(1-u^d)^{-a_d}.$$

Take the logarithm of both sides and write the result as power series in u.

$$\log Z_K(u) = \sum_{m=1}^{\infty} \frac{N_m}{m} u^m,$$

where the number $N_m = \sum_{d|m} da_d$.

These numbers have a very appealing geometric interpretation. Roughly speaking, what is going on is that the function field $K/\mathbb{F}$ is associated to a complete, non-singular curve X defined over $\mathbb{F}$. The number N_m is the number of rational points on X over the unique field extension $\mathbb{F}_m$ of $\mathbb{F}$ of degree m.

We derive now another expression for the zeta function. To this end consider once more the equation

$$Z_K(u) = \prod_{d=1}^{\infty} (1-u^d)^{-a_d}.$$

Take the logarithm of both sides and write the result as power series in u.

$$\log Z_K(u) = \sum_{m=1}^{\infty} \frac{N_m}{m} u^m,$$

where the number $N_m = \sum_{d|m} d a_d$.
These numbers have a very appealing geometric interpretation. Roughly speaking, what is going on is that the function field $K/\mathbb{F}$ is associated to a complete, non-singular curve X defined over $\mathbb{F}$. The number N_m is the number of rational points on X over the unique field extension $\mathbb{F}_m$ of $\mathbb{F}$ of degree m. In any case, using these numbers, the zeta function of the curve X is given by

$$Z_K(u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} u^m\right).$$

We have showed that

$$N_m = q^m + 1 - \sum_{i=1}^{2g} \pi_i^m.$$

We have showed that

$$N_m = q^m + 1 - \sum_{i=1}^{2g} \pi_i^m.$$

This equality plays an important role in the proof of the R.H. for function fields. If we assume the R.H., another consequence is

$$|N_m - q^m - 1| \leq 2gq^{m/2}.$$