# Algebraic Curves for Coding Theory

**Kazunari Sugiyama**

**August 3, 2003**

**Talk at the Summer School, Datensicherheit**

## Purpose of the Talk is

**Give an Overview of the Theory**

**of Algebraic Curves**

**(necessary for the construction of Goppa's codes)**

## Our Main Problem

**What is a Curve over a Finite Field?**

**How do we investigate it?**

**What kind of structure does it have?**

# The Plan of the Talk

**I. Review of the Theory of Algebraic Curves over the Complex Number Field**

**II. Algebraic Curves over an Arbitrary Field**

**III. Function Fields and the Theorem of Riemann-Roch**

**IV. Zeta Functions of a Curve over a Finite Field**

# I. Review of the Theory of Algebraic Curves over the Complex Number Field

$\mathbb{R}$ denotes the real number field.

$\mathbb{C}$ denotes the complex number field.

**Definition (affine plane curve)**

$f(x, y) \in \mathbb{C}[x, y]$ an irreducible polynomial.

Then,

$$\Gamma = \Gamma_f = \{(x_0, y_0) \in \mathbb{C}^2 \ ; \ f(x_0, y_0) = 0\}$$

is called an *affine plane curve*.

Example: $f(x, y) = y^2 - x(x-1)(x+1)$.

The picture of $\Gamma_f$ itself can not be seen. But $\{(x_0, y_0) \in \mathbb{R}^2 \ ; \ f(x_0, y_0) = 0\}$ is as follows:

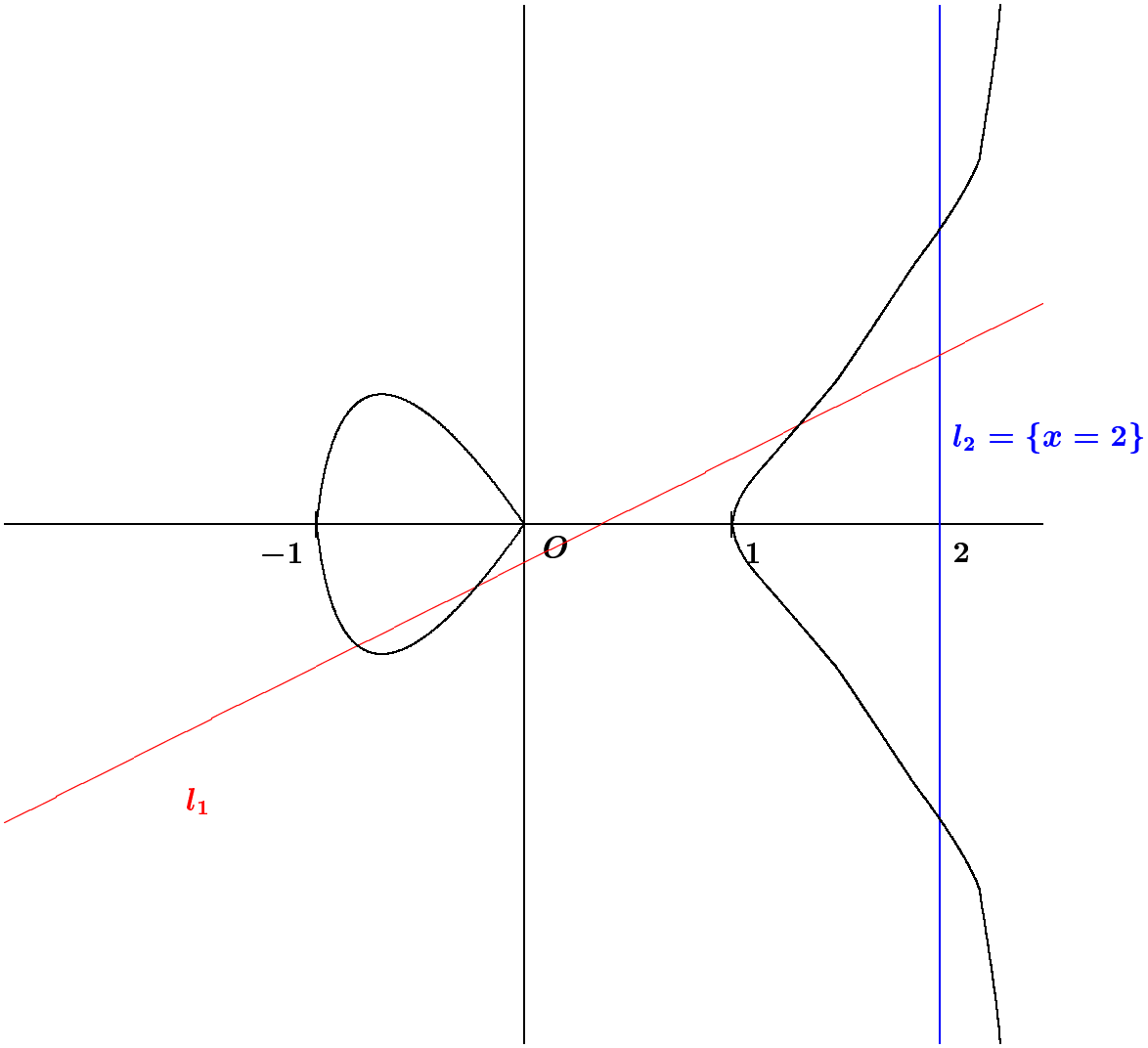


Figure 1: $y^2 = x(x-1)(x+1)$

# $l_2$ intersects $\Gamma$ at infinity!

**Definition (projective plane)**

**Let** $(X_0, Y_0, Z_0), (X_1, Y_1, Z_1) \in \mathbb{C}^3 \backslash \{(0,0,0)\}$.

**Then,** $(X_0, Y_0, Z_0) \sim (X_1, Y_1, Z_1)$

$\overset{\text{def}}{\iff}$ $\exists \alpha \in \mathbb{C}, \alpha \neq 0$ **such that**

$$X_1 = \alpha X_0,\ Y_1 = \alpha Y_0,\ Z_1 = \alpha Z_0.$$

**We call the set of equivalence classes**

$$\mathbb{P}^2(\mathbb{C}) = \left(\mathbb{C}^3 \setminus \{(0,0,0)\}\right) / \sim$$

*the projective plane* **over** $\mathbb{C}$.

**We write a point of** $\mathbb{P}^2(\mathbb{C})$ **as** $(X_0 : Y_0 : Z_0)$.

**Definition (projective plane curve)**

$F(X, Y, Z) \in \mathbb{C}[X, Y, Z]$ **a homogeneous irreducible polynomial.**

**Then,**

$$\widehat{\Gamma} = \widehat{\Gamma}_F$$

$$= \{(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(\mathbb{C}) \ ; \ F(X_0, Y_0, Z_0) = 0\}$$

**is called a** *projective plane curve*.

Let $k$ be a field.

## Definition (homogeneous polynomial)

$F(X,Y,Z) \in k[X,Y,Z]$ is *homogeneous of degree* $d$

$$\overset{\text{def}}{\iff} \quad F(X,Y,Z) = \sum_{i_1+i_2+i_3=d} \gamma_{i_1,i_2,i_3} X^{i_1} Y^{i_2} Z^{i_3}$$

$$(\gamma_{i_1,i_2,i_3} \in k)$$

## Homogenization

To $f(x,y) \in k[x,y]$ with degree $d$, we associate

$$F(X,Y,Z) = Z^d \cdot f\left(\frac{X}{Z}, \frac{Y}{Z}\right) \in k[X,Y,Z].$$

Then,

- $f(x_0,y_0) = 0 \iff F(x_0,y_0,1) = 0.$
- For any $\alpha \in k^\times = k - \{0\}$,

$$F(\alpha X, \alpha Y, \alpha Z) = \alpha^d F(X,Y,Z).$$

So, $F(X_0,Y_0,Z_0) = 0$

$\iff F(\alpha X_0, \alpha Y_0, \alpha Z_0) = 0$ for any $\alpha \in k^\times$.

**Example:**

$f(x,y) = y^2 - x(x-1)(x+1)$ leads to

$$F(X,Y,Z) = Y^2Z - X(X-Z)(X+Z).$$

Then, $\widehat{\Gamma} = \{F = 0\} \subset \mathbb{P}^2(\mathbb{C})$ contains

$\Gamma = \{f = 0\} (\subset \mathbb{C}^2)$ as a subset.

However, some points $\widehat{\Gamma}_\infty$ with $Z_0 = 0$

are added: Here we have $\widehat{\Gamma}_\infty = \{(0:1:0)\}$.

Consider the affine line $l = \{x = 2\} \subset \mathbb{C}^2$.

$l$ defines the projective line

$$\widehat{l} = \{X = 2Z\} \subset \mathbb{P}^2(\mathbb{C}).$$

We observe that $\widehat{l}$ intersects $\widehat{\Gamma}$ at $\widehat{\Gamma}_\infty$.

(There are three points of intersection:

$(2 : \pm\sqrt{6} : 1)$ and $(0:1:0)$.)

**Definition (non-singular curve)**

**Let $\Gamma = \{f = 0\}$ be an affine plane curve.**

- **A point $(x_0, y_0) \in \Gamma$ is** *singular*

$$\overset{\text{def}}{\iff} \left(\frac{\partial f}{\partial x}\right)(x_0, y_0) = \left(\frac{\partial f}{\partial y}\right)(x_0, y_0) = 0.$$

- **$\Gamma$ is** *non-singular* **or** *smooth*

$$\overset{\text{def}}{\iff}$$ **$\Gamma$ has no singular point.**

**Let $\widehat{\Gamma} = \{F = 0\}$ be a projective plane curve.**

- **A point $(X_0 : Y_0 : Z_0) \in \widehat{\Gamma}$ is** *singular*

$$\overset{\text{def}}{\iff} \left(\frac{\partial F}{\partial X}\right)(X_0, Y_0, Z_0) = 0,$$
$$\left(\frac{\partial F}{\partial Y}\right)(X_0, Y_0, Z_0) = 0,$$
$$\left(\frac{\partial F}{\partial Z}\right)(X_0, Y_0, Z_0) = 0.$$

- **$\widehat{\Gamma}$ is** *non-singular* **or** *smooth*

$$\overset{\text{def}}{\iff}$$ **$\widehat{\Gamma}$ has no singular point.**

# The Coordinate Ring

**Idea:** **Consider the Totality of Polynomial Functions on the Curve $\Gamma$ (or $\widehat{\Gamma}$)**

**Definition (congruence)**

**Take an irreducible $f(x,y) \in \mathbb{C}[x,y]$.**

**If $g(x,y), h(x,y) \in \mathbb{C}[x,y]$ satisfy**

$$g(x,y) - h(x,y) = q(x,y)f(x,y)$$

**for some $q(x,y) \in \mathbb{C}[x,y]$, we say that $g(x,y)$ and $h(x,y)$ are *congruent* modulo $f(x,y)$, and denote it by $g(x,y) \equiv h(x,y) \pmod{f(x,y)}$.**

**Let**

$$\mathbb{C}[x,y]/(f(x,y))$$

**be the set of congruence classes of $\mathbb{C}[x,y]$ modulo $f(x,y)$. Then it has a ring-structure and is said to be *the residue class ring* of $\mathbb{C}[x,y]$ modulo $f(x,y)$.**

**Let $\Gamma = \{f(x,y) = 0\}$ be an affine plane curve.**

**Assume that $g(x,y) \equiv h(x,y) \pmod{f(x,y)}$.**

**Take a point $(x_0, y_0) \in \Gamma$. Then,**

$$\begin{aligned} g(x_0,y_0) &= h(x_0,y_0) - q(x_0,y_0)f(x_0,y_0) \\ &= h(x_0,y_0). \end{aligned}$$

**Namely, $g(x,y)$ and $h(x,y)$ define the same polynomial function on $\Gamma$ iff they determine the same element in $\mathbb{C}[x,y]/(f(x,y))$.**

**Definition (coordinate ring)**

**Let $\Gamma = \{f(x,y) = 0\}$ be an affine plane curve.**

**We call**

$$R(\Gamma) = \mathbb{C}[x,y]/(f(x,y))$$

*the coordinate ring* **of $\Gamma$.**

**Let $\widetilde{x}$, $\widetilde{y}$ be the congruence classes modulo $f(x,y)$ associated to $x, y$. Then**

$$R(\Gamma) = \mathbb{C}[\widetilde{x}, \widetilde{y}].$$

$\boldsymbol{R(\Gamma)}$ **is an integral domain.**

**(i.e.,** $g, h \in R(\Gamma)$, $g \cdot h = 0 \implies g$ **or** $h = 0$**)**

**So we can take the quotient field of** $\boldsymbol{R(\Gamma)}$**.**

**Definition (function field, affine case)**

**We set**

$$\begin{aligned}\mathbb{C}(\Gamma) &= \mathrm{Qf}\,(R(\Gamma)) \\ &= \left\{ \frac{g(\widetilde{x}, \widetilde{y})}{h(\widetilde{x}, \widetilde{y})} \;\middle|\; \begin{array}{l} g(\widetilde{x}, \widetilde{y}), h(\widetilde{x}, \widetilde{y}) \in R(\Gamma) \\ h(\widetilde{x}, \widetilde{y}) \neq 0 \end{array} \right\}.\end{aligned}$$

$\mathbb{C}(\Gamma)$ **is called the** *function field* **of** $\Gamma$**.**

$\mathbb{C}(\Gamma)$ **can be regarded as the set of rational functions on the affine plane curve** $\Gamma$**.**

# The Projective Case

**Let $\widehat{\Gamma}$ be a projective plane curve defined by a homogeneous polynomial $F(X, Y, Z)$:**

$$\widehat{\Gamma} = \{(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(\mathbb{C}) \ ; \ F(X_0, Y_0, Z_0) = 0\}.$$

**Definition (coordinate ring)**

**We call**

$$R(\widehat{\Gamma}) = \mathbb{C}[X, Y, Z]/(F(X, Y, Z))$$

*the coordinate ring* **of $\widehat{\Gamma}$.**

**However, the Definition of Function Fields for Projective Curves is a little bit involved.**

**Since $F$ is homogeneous, $R(\widehat{\Gamma})$ becomes a graded ring:**

$$R(\widehat{\Gamma}) = \bigoplus_{d=0}^{\infty} R_d,$$

**where $R_d$ is the "$d$-homogeneous" part.**

**Definition (function field, projective case)**

$$\mathbb{C}(\widehat{\Gamma}) = \left\{ \frac{G(\widetilde{X},\widetilde{Y},\widetilde{Z})}{H(\widetilde{X},\widetilde{Y},\widetilde{Z})} \;\middle|\; \begin{array}{l} G, H \text{ belongs to} \\ \text{the same } R_d \end{array} \right\}$$

Let $\varphi \in \mathbb{C}(\widehat{\Gamma})$ and $P = (X_0 : Y_0 : Z_0) \in \widehat{\Gamma}$.

We say that $\varphi$ is defined at $P$ if

$$\varphi = \frac{G(\widetilde{X},\widetilde{Y},\widetilde{Z})}{H(\widetilde{X},\widetilde{Y},\widetilde{Z})} \quad \text{with } H(X_0,Y_0,Z_0) \neq 0$$

Then we set

$$\varphi(P) = \frac{G(X_0,Y_0,Z_0)}{H(X_0,Y_0,Z_0)}.$$

Note that

$$\begin{aligned} \frac{G(\alpha X_0,\alpha Y_0,\alpha Z_0)}{H(\alpha X_0,\alpha Y_0,\alpha Z_0)} &= \frac{\alpha^d \cdot G(X_0,Y_0,Z_0)}{\alpha^d \cdot H(X_0,Y_0,Z_0)} \\ &= \frac{G(X_0,Y_0,Z_0)}{H(X_0,Y_0,Z_0)}. \end{aligned}$$

# Valuation Rings

Let $\widehat{\Gamma}$ be a projective plane curve.

Take a point $P \in \widehat{\Gamma}$. We define

$\mathcal{O}_P(\widehat{\Gamma}) = \{\varphi \in \mathbb{C}(\widehat{\Gamma})\ ;\ \varphi \text{ is defined at } P\}$.

Then, if $P$ is non-singular,

(1) $\mathbb{C} \subsetneqq \mathcal{O}_P(\widehat{\Gamma}) \subsetneqq \mathbb{C}(\widehat{\Gamma})$, and

(2) If $\varphi \in \mathbb{C}(\widehat{\Gamma})$, then

$$\varphi \in \mathcal{O}_P(\widehat{\Gamma}), \text{ or } \varphi^{-1} \in \mathcal{O}_P(\widehat{\Gamma}).$$

Definition (valuation ring)

A subring $\mathcal{O} \subset \mathbb{C}(\widehat{\Gamma})$ with the properties (1) and (2) is called a *valuation ring* of the function field $\mathbb{C}(\widehat{\Gamma})$.

# Main Theorem

*Let* $\widehat{\mathbf{\Gamma}}$ *be a non-singular projective plane curve. Then there exists a one-to-one correspondence between the points of* $\widehat{\mathbf{\Gamma}}$ *and the valuation rings of* $\mathbb{C}(\widehat{\mathbf{\Gamma}})$.

$$\left\{\textbf{points of } \widehat{\mathbf{\Gamma}}\right\} \overset{1-1}{\longleftrightarrow} \left\{\textbf{valuation rings } \mathbb{C}(\widehat{\mathbf{\Gamma}})\right\}$$

$$\boldsymbol{P} \longleftrightarrow \boldsymbol{\mathcal{O}_P}(\widehat{\mathbf{\Gamma}})$$

# II. Algebraic Curves over an Arbitrary Field

We can define an algebraic curve over an arbitrary field in the same way as in Chapter I. However, there is a big problem.

**Definition (rational points)**

Let $k$ be a field, and $\Gamma$ the affine plane curve defined by a polynomial $f(x, y) \in k[x, y]$.

For any field $K$ containing $k$, we define

$$\Gamma(K) = \{(x_0, y_0) \in K^2 \ ; \ f(x_0, y_0) = 0\}.$$

An element of $\Gamma(K)$ is called a K-*rational point* of $\Gamma$.

**Problem:** $\Gamma(K) \neq \emptyset$?

Example: $f(x,y) = x^2 + y^2 + 1$.

Let $k = K = \mathbb{R}$ (the real number field).

Clearly $\Gamma(\mathbb{R}) = \emptyset$. We can not draw the picture of $\Gamma(\mathbb{R})$.

## So how do we do?

We consider the coordinate ring as in Chap. I:

$$\mathbb{R}[x,y]/(x^2 + y^2 + 1)$$

and its quotient field

$$F = \mathrm{Qf}\left(\mathbb{R}[x,y]/(x^2 + y^2 + 1)\right).$$

Now we can define the set of valuations

$\mathcal{M} = \{\mathcal{O}\ ;\ \mathcal{O}$ is a valuation ring of $F\}$.

Hope: $\mathcal{M}$ might be a substitute of the points of $\Gamma(\mathbb{R})$ !

**Note that, if $(\alpha, \beta) \in \mathbb{C}^2$ is a solution of the equation $f(x, y) = x^2 + y^2 + 1 = 0$, then $(\bar{\alpha}, \bar{\beta}) \in \mathbb{C}^2$ is also a solution. Here $\bar{\alpha}, \bar{\beta}$ are the complex conjugates of $\alpha, \beta$.**

**Fact:** *There exists a one-to-one correspondence between the pairs* $\{(\alpha, \beta), (\bar{\alpha}, \bar{\beta})\}$ *of the points of* $\Gamma(\mathbb{C})$ *and the valuation rings* $\mathcal{O}$ *of* $F$ *such that* $\mathcal{O} \supset \mathbb{R}[\widetilde{x}, \widetilde{y}]$.

$$\left\{ \begin{array}{l} \text{pair } \{(\alpha, \beta), (\bar{\alpha}, \bar{\beta})\} \\ \text{of the points of } \Gamma(\mathbb{C}) \end{array} \right\}$$

$$\overset{1-1}{\longleftrightarrow} \qquad \left\{ \begin{array}{l} \text{valuation ring } \mathcal{O} \text{ of } F \\ \text{such that } \mathcal{O} \supset \mathbb{R}[\widetilde{x}, \widetilde{y}] \end{array} \right\}$$

**Remark:** **If we drop the condition $\mathcal{O} \supset \mathbb{R}[\widetilde{x}, \widetilde{y}]$, then the point at infinity appears.**

# III. Function Fields and the Theorem of Riemann-Roch

• Let $F/K$ be a field extension. Then $x \in F$ is said to be *transcendental* over $K$ if $x$ is not algebraic over $K$.

**Definition (function field)**

A *function field* $F/K$ is a field extension s.t. $F$ is a finite algebraic extension of $K(z)$ for some element $z \in F$ which is transcendental over $K$.

**Definition (valuation ring)**

A *valuation ring* $\mathcal{O}$ of a function field $F/K$ is a ring with the following properties:

(1) $K \subsetneq \mathcal{O} \subsetneq F$, and

(2) for any $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

**Fact:** Let $\mathcal{O}$ be a valuation ring of the function field $F/K$. Then, $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O} \setminus \mathcal{O}^*$, where

$$\mathcal{O}^* = \{z \in \mathcal{O} \; ; \; \exists w \in \mathcal{O} \text{ with } zw = 1\}.$$

**Definition (place):** A *place* $P$ of the function field $F/K$ is the maximal ideal of some valuation ring $\mathcal{O}$ of $F/K$.
We define $\mathbb{P}_F := \{P \; ; \; P \text{ is a place of } F/K\}$.

If $\mathcal{O}$ is a valuation ring of $F/K$ and $P$ its maximal ideal, then $\mathcal{O}$ is uniquely determined by $P$: $\mathcal{O} = \{z \in F \; ; \; z^{-1} \notin P\}$.
We write $\mathcal{O}_P := \mathcal{O}$.

**Idea:** $(F/K, \mathbb{P}_F)$ **is our "algebraic curve" and a place** $P \in \mathbb{P}_F$ **is a "point".**

# Valuations

**Motivation:** $\Gamma = \{x^2 + y^2 - 1 = 0\}$ $(\subset \mathbb{C}^2)$.

Take a rational function $\varphi \in \mathbb{C}(\Gamma)$ defined by

$\varphi(x, y) = \dfrac{x(x-1)^2}{(y-1)^2}$. Then $P = (1, 0) \in \Gamma$ is a zero of $\varphi$ of order 2, and $Q = (0, 1) \in \Gamma$ is a pole of order 1.

We write as $\nu_P(\varphi) = 2$ and $\nu_Q(\varphi) = -1$.

**Fact:** Let $\mathcal{O}$ be a valuation ring of the function field $F/K$ and $P$ its maximal ideal. Then,

(1) $\exists\, t \in \mathcal{O}$ such that $P = t\mathcal{O}$.

(2) Any $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ $(n \in \mathbb{Z},\ u \in \mathcal{O}^*)$.

**Definition (valuation):** For any $P \in \mathbb{P}_F$, we associate a function $\nu_P : F \to \mathbb{Z} \cup \{\infty\}$ by $\nu_P(z) = n$ if $z \neq 0$, $z = t^n u$ as above, and $\nu_P(0) = \infty$.

**In this case, we have**

$$\mathcal{O}_P = \{z \in F \; ; \; \nu_P(z) \geq 0\},$$
$$\mathcal{O}_P^* = \{z \in F \; ; \; \nu_P(z) = 0\},$$
$$P = \{z \in F \; ; \; \nu_P(z) > 0\}.$$

**Definition (zeros, poles):** **Let $z \in F$ and $P \in \mathbb{P}_F$.**

- **$P$ is a *zero* of $z$ of order $m$**

$\overset{\text{def}}{\Longleftrightarrow}$ $\nu_P(z) = m > 0.$

- **$P$ is a *pole* of $z$ of order $m$**

$\overset{\text{def}}{\Longleftrightarrow}$ $\nu_P(z) = -m < 0.$

**Theorem:** *Any element $0 \neq z \in F$ has only finitely many zeros and poles.*

# Residue Class Fields and Degrees

Idea: An element $z$ of $F$ should be a "rational function" on the curve.

Let $P$ be a place of $F/K$ and $\mathcal{O}_P$ be its valuation ring. Then $F_P := \mathcal{O}_P/P$ is a field. For $z \in \mathcal{O}_P$, we define $z(P)$ to be the residue class of $z$ modulo $P$:

$$\begin{array}{ccc} \mathcal{O}_P & \longrightarrow & \mathcal{O}_P/P \\ z & \longmapsto & z(P) \end{array}$$

For $z \in F \setminus \mathcal{O}_P$, we define $z(P) := \infty$.

Definition (residue class field):

(1) $F_P$ is called the *residue class field* of $P$.

(2) The map $x \mapsto x(P)$ from $F$ to $F_P \cup \{\infty\}$ is called the *residue class map* w.r.t. $P$.

**Since $K \cap P = \{0\}$, we can regard $K$ as a subfield of $F_P = O_P/P$.**

**Let $[F_P : K]$ be the degree of $F_P/K$.**

**Definition (degree):**

**$\deg P := [F_P : K]$ is called the *degree* of $P$.**

**Remark:** **If $F/K$ is the function field of some non-singular projective plane curve $\widehat{\Gamma}$ defined over $K$, then the places of $F/K$ of degree one are in one-to-one correspondence with the $K$-rational points $\widehat{\Gamma}(K)$ of $\widehat{\Gamma}$.**

**Example:** Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_q(x)$ where $x$ is transcendental over $\mathbb{F}_q$. Then $F$ is said to be the *rational function field* over $\mathbb{F}_q$. Every irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ defines a valuation ring

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \;\middle|\; \begin{array}{l} f(x), g(x) \in \mathbb{F}_q[x], \\ p(x) \nmid g(x) \end{array} \right\}$$

of $\mathbb{F}_q(x)/\mathbb{F}_q$ with maximal ideal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \;\middle|\; \begin{array}{l} f(x), g(x) \in \mathbb{F}_q[x], \\ p(x) | f(x),\ p(x) \nmid g(x) \end{array} \right\}.$$

We have $\deg P_{p(x)} = \deg p(x)$.

In particular, if $p(x) = x - \alpha$ with $\alpha \in \mathbb{F}_q$, the degree of $P_{x-\alpha}$ is one, and the residue class map is given by

$$z(P) = z(\alpha) \qquad \text{(evaluation map)}$$

for $z \in F$.

**However, you miss one place, the *infinite place*.**

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; \begin{array}{l} f(x), g(x) \in \mathbb{F}_q[x], \\ \deg f(x) \leq \deg g(x) \end{array} \right\}$$

**with maximal ideal**

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; \begin{array}{l} f(x), g(x) \in \mathbb{F}_q[x], \\ \deg f(x) < \deg g(x) \end{array} \right\}.$$

**Theorem:** *There are no places of* $\mathbb{F}_q(x)/\mathbb{F}_q$ *other than* $P_{p(x)}$*'s and* $P_\infty$.

**Corollary:** *The places of* $\mathbb{F}_q(x)/\mathbb{F}_q$ *of degree one are in one-to-one correspondence with* $\mathbb{F}_q \cup \{\infty\}$.

# Divisors

Let $F/K$ be a function field and $\mathbb{P}_F$ the set of the places of $F/K$

**Definition (divisor):** A *divisor* is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} n_P P \quad \text{with } n_P \in \mathbb{Z}, \quad \text{almost all } n_P = 0.$$

A divisor of the form $D = P$ with $P \in \mathbb{P}_F$ is called a *prime divisor*.

If $D = \sum n_P P$ and $D' = \sum n'_P P$, we put

$$D + D' \stackrel{\text{def}}{=} \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

The totality $\mathcal{D}_F$ of the divisors of $F/K$ becomes a group and is called the *divisor group* of $F/K$.

For $Q \in \mathbb{P}_F$ and a divisor $D = \sum n_P P \in \mathcal{D}_F$, we define $\nu_Q(D) := n_Q$.

- $D_1 \leq D_2 \overset{\text{def}}{\iff} \nu_P(D_1) \leq \nu_P(D_2)$ for $\forall P \in \mathbb{P}_F$

The *degree* of a divisor $D$ is defined by

$$\deg D = \sum_{P \in \mathbb{P}_F} \nu_P(D) \cdot \deg P.$$

**Definition (principal divisor):** Let $x \in F \setminus \{0\}$ and denote by $Z$ (resp. $N$) the set of zeros (resp. poles) of $x$ in $\mathbb{P}_F$. Then we define

$$(x) := \sum_{P \in Z} \nu_P(x) P + \sum_{Q \in N} \nu_Q(x) Q.$$

Since $x$ has only finitely many zeros and poles, $(x)$ defines a divisor (the *principal divisor* of $x$).

**Theorem:** *Any principal divisor has degree zero. Namely, we have* $\deg(x) = 0$ *for any* $x \in F$.

**Example:** Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_q(x)$

For $0 \neq z \in \mathbb{F}_q(x)$, we have $z = a \cdot f(x)/g(x)$ with $a \in \mathbb{F}_q \setminus \{0\}$, and $f(x), g(x) \in \mathbb{F}_q[x]$ are monic and relatively prime. Let

$$f(x) = \prod_{i=1}^{r} p_i(x)^{n_i}, \qquad g(x) = \prod_{i=1}^{s} q_j(x)^{m_j}$$

with pairwise distinct irreducible monic polynomials $p_i(x), q_j(x) \in \mathbb{F}_q[x]$. Then the principal divisor of $z$ is

$$(z) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (\deg g - \deg f) P_\infty$$

where $P_i$ and $Q_j$ are the places corresponding to $p_i(x)$ and $q_j(x)$. Therefore, we have

$$\deg(x) = \sum_{i=1}^{r} n_i \deg p_i(x) - \sum_{j=1}^{s} m_j \deg q_j(x)$$
$$+(\deg g - \deg f) \cdot 1 = 0.$$

# Theorem of Riemann-Roch

**Definition:** For a divisor $A \in \mathcal{D}_F$, we set

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

Then $\mathcal{L}(A)$ is a vector space over $K$.

**Meaning:** If

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

with $n_i > 0$, $m_j > 0$, then $\mathcal{L}(A)$ consisits of all elements $x \in F$ such that

(1) $x$ has zeros of order $\geq m_j$ at $Q_j$, for $j = 1, \ldots, s$, and

(2) $x$ may have poles only at the places $P_1, \ldots, P_r$ with the pole order at $P_i$ being bounded by $n_i$ $(i = 1, \ldots, r)$.

**Let $F/K$ be a function field.**

**Definition (dimension): For $A \in \mathcal{L}(A)$, we set $\dim A := \dim \mathcal{L}(A)$ and call it the *dimension* of $A$.**

**Theorem (Riemann-Roch):**

**(1)** *For any* $A \in \mathcal{D}_F$, $\dim A$ *is finite.*

**(2)** *For any* $A \in \mathcal{D}_F$, *we have*

$$\dim A = \deg A + 1 - g + l^*(A).$$

*Here* $g$ *is the genus of* $F/K$ *and* $l^*(A)$ *is some correction term which is always* $\geq 0$.

**(3)** *If* $A \in \mathcal{D}_F$ *is of degree* $\geq 2g - 1$, *then*

$$\dim A = \deg A + 1 - g.$$

## How to calculate the genus ?

If $F/\mathbb{F}_q$ comes from a non-singular projective plane curve defined by a homogeneous irreducible polynomial $f(X, Y, Z)$, then

$$g = \frac{(d-1)(d-2)}{2}$$

where $d$ is the degree of $f$.

# IV. Zeta Functions of a Curve over a Finite Field

In this chapter, we discuss the zeta function of a function field $F/\mathbb{F}_q$.

We are mainly interested in places $P \in \mathbb{P}_F$ of degree one. For this purpose, we consider more general divisors which are positive.

**Lemma 1.** *For every $n \in \mathbb{Z}$, $n \geq 0$, there exist only finitely many positive divisors of degree $n$.*

We introduce the divisor class group.

Let $\mathcal{P}_F = \{(x)\ ;\ x \in F, x \neq 0\}$ be the set of principal divisors. Clearly $\mathcal{P}_F$ is a subgroup of $\mathcal{D}_F$. The quotient group $\mathcal{C}_F = \mathcal{D}_F/\mathcal{P}_F$ is called the **divisor class group** of $F$.

We denote by $[A]$ the class to which $A$ belongs. Then we have $\deg[A] = \deg A$ and $\dim[A] = \dim A$.

The set

$$\mathcal{D}_F^0 = \{A \in \mathcal{D}_F\ ;\ \deg A = 0\}$$

is a subgroup of $\mathcal{D}_F$, and called **the group of divisors of degree zero**. Further, the set

$$\mathcal{C}_F^0 = \{[A] \in \mathcal{C}_F\ ;\ \deg A = 0\}$$

is called **the group of divisor class of degree 0**.

**Proposition 2.** *The group $\mathcal{C}_F^0$ is a finite group. Its order $h = h_F$ is called* ***the class number*** *of $F/\mathbb{F}_q$.*

We consider the numbers

$$A_n = |\{A \in \mathcal{D}_F\ ;\ A \geq 0,\ \deg A = n\}|$$

for $n = 0, 1, 2, \ldots$. Then clearly $A_0 = 1$, $A_1 =$ the number of prime divisors of $F$ or $\mathbb{P}_F$ of degree 1.

**Definition 3.** *The power series*

$$Z(t) = Z_F(t) = \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]]$$

*is called* ***the zeta function*** *of* $F/\mathbb{F}_q$.

Observe that $Z(t)$ is considered as a power series over the complex number field $\mathbb{C}$. The idea is that properties of the complex function $Z(t)$ will give informations on the numbers $A_n$.

From the Theorem of Riemann-Roch, we can determine the form of $Z(t)$.

**Theorem 4.** *(a) If* $F/\mathbb{F}_q$ *has genus* $g = 0$, *then*

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-qt} - \frac{1}{1-t}\right).$$

*(b) If* $g \geq 1$, *then* $Z(t) = F(t) + G(t)$ *with*

$$F(t) = \frac{1}{q-1} \sum_{\substack{[C]\in\mathcal{C}_F,\\ 0\leq \deg[C]\leq 2g-2}} q^{\dim[C]} \cdot t^{\deg[C]},$$

*and*

$$G(t) = \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-1}\frac{1}{1-qt} - \frac{1}{1-t}\right).$$

In particular, the theorem above shows that $Z(t)$ is a rational function, more precisely, it is of the form

$$Z(t) = \frac{L_F(t)}{(1-t)(1-qt)},$$

where $L_F(t)$ is a polynomial with complex coefficients. We call $L_F(t)$ **the $L$-polynomial** of $F/\mathbb{F}_q$.

By definition, we have

$$L_F(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n. \tag{1}$$

This shows that $L_F(t)$ contains all important informations. Now the following theorem holds.

**Theorem 5.** *(1)* $L_F(t) \in \mathbb{Z}[t]$ *and* $\deg L_F(t) = 2g$.

*(2)* $L_F(t) = q^g t\ 2gLF(1/qt)$.

*(3)* $L_F(1) = h$, *the class number of* $F/\mathbb{F}_q$.

*(4) We write* $L_F(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$. *Then the following holds:*

- *(a)* $a_0 = 1$ *and* $a_{2g} = q^g$.
- *(b)* $a_{2g-i} = q\ g - ia_i$ *for* $0 \leq i \leq g$.
- *(c)* $a_1 = N - (q+1)$ *where* $N$ *is the number of prime divisors* $P$ *of degree one.*

*(5)* $L_F(t)$ *factors in* $\mathbb{C}[t]$ *in the form*

$$L_F(t) = \prod_{i=1}^{2g} (1 - \alpha_i t). \tag{2}$$

*The complex numbers* $\alpha_1, \cdots, \alpha_{2g}$ *are algebraic integers, and they can be arranged in such a way that* $\alpha_i \alpha_{g+i} = g$ *holds for* $i = 1, \ldots, g$.

We are interested in controling the number $N = A_1 =$ the number of places of $F/\mathbb{F}_q$ of degree one. By comparing (1) with (2), we obtain

$$N = A_1 = q + 1 - \sum_{i=1}^{2g} \alpha_i$$

and thus

$$|N - (q+1)| \leq \left| \sum_{i=1}^{2g} \alpha_i \right| \leq \sum_{i=1}^{2g} |\alpha_i|.$$

The main result is the following.

**Theorem 6 (Hasse-Weil).** *The reciprocals of the roots of $L_F(t)$ satisfy*

$$|\alpha_i| = q^{1/2} \quad \textit{for} \quad i = 1, \ldots, 2g.$$

**Remark:** The Hasse-Weil Theorem is often referred to as the *Riemann Hypothesis for Algebraic Function Fields*. Let us briefly explain this notation. One can regard the Zeta function $Z_F(t)$ as an analogue of the classical Riemann $\zeta$-function

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} \tag{3}$$

(where $s \in \mathbb{C}$ and $\mathrm{Re}(s) > 1$) in the following manner. Define the *absolute norm* of a divisor $A \in \mathcal{D}_F$ by

$$\mathcal{N}(A) := q^{\deg A}.$$

For instance, the absolute norm $\mathcal{N}(P)$ of a prime divisor $P \in \mathcal{P}_F$ is the cardinarity of its residue field $F_P$. Then the function

$$\zeta_F(s) := Z_F(q^{-s})$$

can be written as

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{\mathcal{A} \in \mathcal{D}_F,\ A \geq 0} \mathcal{N}(A)^{-s},$$

which is the appropriate analogue to (3). It is well-known for number theory for the Riemann zeta function (3) has an analytic continuation as a meromorphic function on $\mathbb{C}$. The classical Riemann Hypothesis (which is still unproven) states that - besides the so-called trivial zeros $s = -2, -4, -6, \ldots$, - all zeros of $\zeta(s)$ lie on the line $\mathrm{Re}(s) = 1/2$.

In the function field case, the Hasse-Weil Theorem states that

$$\zeta_F(s) = 0 \Rightarrow Z_F(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{-1/2}.$$

Since $|q^{-s}| = q^{-\mathrm{Re}(s)}$, this means that

$$\zeta_F(s) = 0 \Rightarrow \mathrm{Re}(s) = 1/2.$$

Therefore, Theorem 6 can be viewed as an analogue of the classical Riemann Hypothesis.

**Theorem 7 (Hasse-Weil Bound).** *The number $N = N(F)$ of places of $F/\mathbb{F}_q$ of degree one can be estimated by*

$$|N - (q+1)| \leq 2gq^{1/2}.$$

The estimate above is used in the construction of Goppa's codes.

## References


[1] W. Fulton, *Algebraic curves. An introduction to algebraic geometry*, Benjamin, 1969.

[2] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, 1993.


Fulton's book [1] is a good introduction to algebraic curves. The main theorem of Chapter I of this note is proved in [1, CHAPTER 7]. The chapters III and IV of this note is a summary of Stichtenoth [2]. Stichtenoth's book is highly recommended if you want to learn Goppa's code.