Function fields

Holly Green

University College London

May 24th, 2022

Overview

- Definition
- Ring of integers
- Units
- Primes
- Class group
- Decomposition of primes

Definition of a function field

Let p be a prime and $q = p^r$.

Definition

A function field is a finitely generated field extension $K/\mathbb{F}_q$ of transcendence degree 1.

There is a correspondence between function fields over $\mathbb{F}_q$ and non-singular, projective, irreducible algebraic curves over $\mathbb{F}_q$.

The function field for $C : F(x, y) = 0$ is $\mathbb{F}_q(C) = \mathbb{F}_q(x)[y]/(F(x, y))$.

Examples

- $C_1 : y^2 = x^3 - 1$ over $\mathbb{F}_5 \;\Rightarrow\; \mathbb{F}_5(C_1) = \mathbb{F}_5(x, \sqrt{x^3 - 1})$ or $\mathbb{F}_5(y, \sqrt[3]{y^2 + 1})$
- $C_2 : \{y^2 = x^3 - 1,\; w^2 = 2\}$ over $\mathbb{F}_5 \;\Rightarrow\; \mathbb{F}_5(C_2) = \mathbb{F}_{25}(x, \sqrt{x^3 - 1})$ or $\mathbb{F}_{25}(y, \sqrt[3]{y^2 + 1})$.
- $\mathbb{F}_5(C_2) = \mathbb{F}_{25}(C_1)$.

Function fields and number fields share many properties; both are called global fields.

Notation

- p a prime, $q = p^r$
- C a non-singular, projective, irreducible algebraic curve over $\mathbb{F}_q$
- $K = \mathbb{F}_q(C)$

Definition

A *closed point* on C is the $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbit of a point $P \in C(\overline{\mathbb{F}}_q)$.

Let $C : y^2 = x^3 - x$ be a curve over $\mathbb{F}_7$. Then $(2, \sqrt{-1}) \in C(\mathbb{F}_{49})$ and the associated closed point is

$$\{(2, \sqrt{-1}), (2, -\sqrt{-1})\}.$$

- X is the set of closed points on C

Ring of integers

We think of the integers (of $\mathbb{Q}$) as having no *denominator*, i.e.

$$\mathbb{Z} = \bigcap_{p \text{ prime}} \{x \in \mathbb{Q} : |x|_p \leq 1\}.$$

For $K = \mathbb{F}_q(C)$, can we construct $\mathcal{O}_K$ in the same way?

Definition

Let $P \in C(\mathbb{F}_{q^n})$. The *absolute value of $f \in K$ at P* is $|f|_P = (q^n)^{-\mathrm{ord}_P(f)}$.

The absolute values on K correspond to closed points on C. As above,

$$\bigcap_{P \in X} \{f \in K : |f|_P \leq 1\} = \{f \in K : f \text{ has no poles}\} = \mathbb{F}_q.$$

Definition

Let $S \subset X$ be a finite set. The *ring of S-integers of K* is

$$\mathcal{O}_{K,S} = \{f \in K : f \text{ has no poles outside of } S\}.$$

Ring of integers

Definition

Let $S \subset X$ be a finite set. The *ring of S-integers of K* is

$$\mathcal{O}_{K,S} = \{f \in K : f \text{ has no poles outside of } S\}.$$

Examples

Let $C : y^2 = x^3 - x$ $(p \neq 2)$. Then

$$K = \mathbb{F}_q(x)[y]/(y^2 - x^3 + x) = \mathrm{Frac}(\{a(x) + yb(x) : a, b \in \mathbb{F}_q[x]\}).$$

- $S = \{\infty\} \Rightarrow \mathcal{O}_{K,S} = \mathbb{F}_q[x, y]/(y^2 - x^3 + x)$.
- $S = \{(0, 0)\}$, let $s = 1/x$, $t = y/x^2 \Rightarrow C : t^2 = s - s^3$, $\mathcal{O}_{K,S} = \mathbb{F}_q[s, t]/(t^2 - s + s^3)$
- $S = \{(-1, 0), (0, 0), (1, 0), \infty\} \Rightarrow \mathcal{O}_{K,S} = \mathbb{F}_q[x, y, 1/y]/(y^2 - x^3 + x)$.

More generally, if $C : F(x, y) = 0$ and $S = \{\text{points at } \infty\}$ then $\mathcal{O}_{K,S} = \mathbb{F}_q[x, y]/(F(x, y))$.

Group of units

The units of K are the invertible elements in the ring of integers.

Definition

Let $S \subset X$ be a finite set. The *S-unit group of K* is

$$\mathcal{O}_{K,S}^{\times} = \{f \in K : f \text{ has no poles or zeros outside of } S\}.$$

Examples

- Let $C = \mathbb{P}^1$ over $\mathbb{F}_5$ and $S = \{\infty, \{\pm\sqrt{2}\}\}$. Then

$$\mathcal{O}_{K,S} = \mathbb{F}_5[x, 1/(x^2-2)], \qquad \mathcal{O}_{K,S}^{\times} = \mathbb{F}_5^{\times} \oplus (x^2-2)^{\mathbb{Z}}.$$

- Let $C : y^2 = x^3 - x$ $(p \neq 2)$ and $S = \{\infty\}$. Then

$$\mathcal{O}_{K,S} = \mathbb{F}_q[x,y]/(y^2 - x^3 + x), \qquad \mathcal{O}_{K,S}^{\times} = \mathbb{F}_q^{\times}.$$

Group of units

Extended example

Let $C : y^2 = x^3 - x$ ($p \neq 2$), $S = \{P_1 = (-1, 0), P_2 = (0, 0), P_3 = (1, 0), \infty\}$. Let $f \in \mathcal{O}_{K,S}^\times$. Multiply by powers of $x + 1$, x and $x - 1$ (with double zeros at P_i), to get g with

$$\mathrm{ord}_{P_i}(g) = 0 \text{ or } 1, \qquad \mathrm{ord}_P(g) = 0 \text{ for } P \notin S.$$

We have $(g) := \mathrm{ord}_\infty(g)[\infty] + \sum_i \mathrm{ord}_{P_i}(g)[P_i] = 0 \in \mathrm{Jac}\, C$. In terms of points of C,

$$\mathrm{ord}_{P_1}(g)[P_1] + \mathrm{ord}_{P_2}(g)[P_2] + \mathrm{ord}_{P_3}(g)[P_3] = \infty \Rightarrow \begin{cases} \mathrm{ord}_{P_i} = 0 \text{ for all } i \Rightarrow g \in \mathbb{F}_q^\times \\ \mathrm{ord}_{P_i} = 1 \text{ for all } i \Rightarrow g \in \mathbb{F}_q^\times y. \end{cases}$$

So $f \in \mathbb{F}_q^\times \oplus (x+1)^{\mathbb{Z}} \oplus (x)^{\mathbb{Z}} \oplus (x-1)^{\mathbb{Z}} \oplus \{1, y\} \Rightarrow f \in \mathbb{F}_q^\times \oplus (x+1)^{\mathbb{Z}} \oplus (x)^{\mathbb{Z}} \oplus y^{\mathbb{Z}}$.

Theorem (Dirichlet's unit theorem)

$$\mathcal{O}_{K,S}^\times \cong \mathbb{F}_q^\times \oplus \mathbb{Z}^{\#S-1}$$

Prime ideals

Recall, for $p \in \mathbb{Z}$ a prime, $(p) = \{a \in \mathbb{Z} : |a|_p < 1\}$ is the prime ideal.

Definition

Fix $P \in X \backslash S$. The *prime ideal of $\mathcal{O}_{K,S}$ at P* is

$$\mathfrak{p}_{P,S} := \{f \in \mathcal{O}_{K,S} : |f|_P < 1\} = \{f \in K : f \text{ has a zero at } P \text{ and no poles outside of } S\}.$$

There's a correspondence between primes of $\mathcal{O}_{K,S}$ and points in $X \backslash S$.

Example

Let $C : y^2 = x^3 - x$ over $\mathbb{F}_7$.

- $S = \{\infty\} \Rightarrow \mathcal{O}_{K,S} = \mathbb{F}_7[x, y]/(y^2 - x^3 + x)$ and

$$\mathfrak{p}_{(0,0),S} = (x, y), \qquad \mathfrak{p}_{\{(2,\pm\sqrt{-1})\},S} = (x - 2, y^2 + 1) = (x - 2, x^3 - x + 1).$$

- $S = \{(-1, 0), (0, 0), (1, 0), \infty\} \Rightarrow (x, y)$ is no longer prime, it is generated by units.

Prime ideals

Definition

Fix $P \in X \backslash S$. The *prime ideal of* $\mathcal{O}_{K,S}$ *at* P is

$$\mathfrak{p}_{P,S} := \{f \in \mathcal{O}_{K,S} : |f|_P < 1\} = \{f \in K : f \text{ has a zero at } P \text{ and no poles outside of } S\}.$$

Example

Let $C : y^2 = x^3 - x$ over $\mathbb{F}_7$, $S = \{\infty\}$. Then $\mathfrak{p}_{\{(2,\pm\sqrt{-1})\},S} = (x-2, y^2+1)$ and

$$\mathcal{O}_{K,S}/\mathfrak{p}_{\{(2,\pm\sqrt{-1})\},S} = \mathbb{F}_7[y]/(y^2+1) = \mathbb{F}_{49}.$$

The residue degree of a prime is the size of the Galois orbit of the corresponding point.

The Chinese Remainder Theorem

Let $P, Q \in X \backslash S$ be distinct. Given $s, t \in \overline{\mathbb{F}}_q$ defined over the residue fields of P and Q respectively, there's some $f \in \mathcal{O}_{K,S}$ such that $f(P) = s$ and $f(Q) = t$.

The Class Group

The class group indicates how far we are from having unique factorisation.

Fractional ideals look like

$$\prod_{P \in X \setminus S} \mathfrak{p}_{P,S}^{n_P} \leftrightsquigarrow \sum_{P \in X \setminus S} n_P[P]$$

where $n_P \in \mathbb{Z}$, almost all are zero. Write $\mathrm{Div}_{K,S}$ for the group of these.
Principal ideals here correspond to divisors of the type

$$\sum_{P \in X \setminus S} \mathrm{ord}_P(f)[P],$$

for $f \in \mathcal{O}_{K,S}$. Write $\mathrm{Princ}_{K,S}$ for the group generated by these.

Definition

Let $S \subset X$ be a finite set. The *S-class group of K* is

$$\mathrm{Cl}_{K,S} = \mathrm{Div}_{K,S}/\mathrm{Princ}_{K,S}$$

The Class Group

Definition

Let $S \subset X$ be a finite set. The *S-class group of K* is

$$\mathrm{Cl}_{K,S} = \mathrm{Div}_{K,S}/\mathrm{Princ}_{K,S}$$

Examples

- Let $C = \mathbb{P}^1$ over $\mathbb{F}_q$, $S = \{\infty\}$. Fix $D = \sum_{\infty \neq P \in X} n_P[P]$. Let $f \in \mathcal{O}_{K,S}$ have a zero of order n_P at P when $n_P > 0$; and $g \in \mathcal{O}_{K,S}$ have a zero of order $-n_P$ at P when $n_P < 0$. Suppose f, g have no other zeros $\Rightarrow D \sim \sum_{\infty \neq P \in X}(\mathrm{ord}_P(f) - \mathrm{ord}_P(g))[P] \Rightarrow \mathrm{Cl}_{K,S} = 1$.
- Let $C : y^2 = x^3 - x$ over $\mathbb{F}_q$, $S = \{\infty\}$. Consider $D = \sum_{\infty \neq P \in X} n_P[P]$, or $\sum_{\infty \neq P \in X} n_P[P] - (\sum_{\infty \neq P \in X} n_P)[\infty]$. Equivalence classes of degree 0 divisors correspond to points in $C(\mathbb{F}_q) \Rightarrow \mathrm{Cl}_{K,S} = C(\mathbb{F}_q)$. If $q = 7$ then $\mathrm{Cl}_{K,S} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

More generally, if $S = \{\infty\} \sqcup T$ then

$$\mathrm{Cl}_{K,S} = \mathrm{Jac}_C(\mathbb{F}_q)/\langle [P] - \#P[\infty] | P \in T \rangle.$$

Factorising primes

Let $K = \mathbb{F}_q(x, y) = \mathbb{F}_q(C)$ be a finite, **separable** extension of $\mathbb{F}_q(x)$, where

- for a non-constant morphism $\phi : C \to \mathbb{P}^1$ we let $S = \phi^{-1}(\infty)$, and
- $y \in \mathcal{O}_{K,S}$ has minimum polynomial $g(t) \in \mathbb{F}_q[x][t]$

If $C : F(x, y) = 0$ then $y \in \mathbb{F}_q[x, y]/(F)$.

Take $\mathfrak{p}$ to be a prime of $\mathbb{F}_q[x]$.

Theorem (Dedekind's theorem)

Let $\overline{g}(t) = \overline{g}_1(t)^{e_1} \times \cdots \times \overline{g}_r(t)^{e_r}$ be the factorisation of $\overline{g}(t) := g(t) \bmod \mathfrak{p}$ into irreducibles, with $\overline{g}_i(t) := g_i(t) \bmod \mathfrak{p}$ for monic $g_i(t) \in \mathbb{F}_q[x][t]$, then

$$\mathfrak{p} = \mathfrak{p}_1^{e_1} \times \cdots \times \mathfrak{p}_r^{e_r}$$

where $\mathfrak{p}_i = (\mathfrak{p}, g_i(y))$. Moreover, the residue degree of $\mathfrak{p}_i$ is $f_i = \deg \overline{g}_i(t)$.

Factorising primes

Example

Let $C : y^2 = x^{q+1} - 1$ over $\mathbb{F}_q$ $(p \neq 2)$. We can deduce how a prime $\mathfrak{p} = (x - a)$ of $\mathbb{F}_q[x]$ splits in $\mathbb{F}_q[C]$. Suppose $a \in \mathbb{F}_q$.
The minimum polynomial of y is $g(t) = t^2 - (x^{q+1} - 1)$. Reducing modulo $\mathfrak{p}$ gives

$$\overline{g}(t) = t^2 - (a^{q+1} - 1) = \begin{cases} t^2 & a^{q+1} \equiv a^2 \equiv 1 \bmod q \\ t^2 - r, \;\; r \in \mathbb{F}_q^\times & a^{q+1} \equiv a^2 \not\equiv 1 \bmod q \end{cases}$$

- $a^2 \equiv 1 \Rightarrow \mathfrak{p} = (x - a, y)^2$ and $(x - a, y)$ has residue degree 1 (cf. $\{(a, 0)\} \in X$).
- $a^2 \not\equiv 1$ and $r = \square \Rightarrow \mathfrak{p} = (x - a, y - \sqrt{r})(x - a, y + \sqrt{r})$ and $(x - a, y \pm \sqrt{r})$ have residue degree 1 (cf. $\{(a, \sqrt{r})\}, \{(a, -\sqrt{r})\} \in X$).
- $a^2 \not\equiv 1$ and $r \neq \square \Rightarrow \mathfrak{p} = (x - a, y^2 - r)$ and $(x - a, y^2 - r)$ has residue degree 2 (cf. $\{(a, \sqrt{r}), (a, -\sqrt{r})\} \in X$).

Thank you for your attention!