The ring of integers of a function field and its primes

Holly Green

University College London

November 5th, 2021

Goal and motivation

Let $q = p^r$. A function field is

- a finitely generated field $K/\mathbb{F}_q$ of transcendence degree 1
- $\mathbb{F}_q(C)$ for a smooth projective curve $C/\mathbb{F}_q$: in particular if $C : F(x, y) = 0$ this is the fraction field of
$$\mathbb{F}_q[x, y]/(F(x, y)).$$

E.g. $C : y^2 = x^3 - x$ over $\mathbb{F}_5 \Rightarrow \mathbb{F}_5(C) = \mathbb{F}_5(x, \sqrt{x^3 - x})$

$C : \{y^2 = x^3 - x,\ w^2 = 2\}$ over $\mathbb{F}_5 \Rightarrow \mathbb{F}_5(C) = \mathbb{F}_{25}(x, \sqrt{x^3 - x})$

Goal

What is the *ring of integers* of K, $\mathcal{O}_K$? What are the *primes* in $\mathcal{O}_K$?

Valuations on $\mathbb{F}_q(x)$

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

$$\mathbb{F}_q(x) = \mathbb{F}_q(\mathbb{P}^1) \hookleftarrow \mathbb{F}_q[x]$$

Question

Is $\mathbb{F}_q[x]$ cut out by valuation bounds in the same way as $\mathbb{Z}$?

Let $f \in \mathbb{F}_q(x)$ be a rational function on $\mathbb{P}^1$. Fix $P \in \mathbb{P}^1(\mathbb{F}_{q^n})$ for some $n \geq 1$, define

$$\mathrm{ord}_P(f) := \text{the order of vanishing of } f \text{ at } P.$$

Definition

The *absolute value of* f *at* P is $|f|_P = (q^n)^{-\mathrm{ord}_P(f)}$.

Absolute values on $\mathbb{F}_q(x)$

Let $f \in \mathbb{F}_q(x) = \mathbb{F}_q(\mathbb{P}^1)$ and fix $P \in \mathbb{P}^1(\mathbb{F}_{q^n})$ for some $n \geq 1$.

Definition

The *absolute value of f at P* is $|f|_P = (q^n)^{-\mathrm{ord}_P(f)}$.

For example, if $f = x/(x^2 - 2)$ and $q = 5$ then

$$|f|_0 = 5^{-1}, \qquad |f|_{\pm\sqrt{2}} = 25^1, \qquad |f|_\infty = 5^{-1},$$

and $|f|_P = 1$ for all other P.

Remarks

- This is a non-archimedean
- Varying P gives all absolute values on $\mathbb{F}_q(x)$
- $|f|_P \leq 1$ precisely when f does not have a pole at P
- $\{f \in \mathbb{F}_q(x) : |f|_P \leq 1\}$ is a discrete valuation ring

The analogue of $\mathbb{Z} \hookrightarrow \mathbb{Q}$ for $\mathbb{F}_q(\mathbb{P}^1)$

Mirroring the case of number fields:

$$\bigcap_{P \in \mathbb{P}^1(\overline{\mathbb{F}}_q)} \{f \in \mathbb{F}_q(x) : |f|_P \leq 1\} = \{f \in \mathbb{F}_q(x) : f \text{ has no poles}\}$$

but all we've constructed is $\mathbb{F}_q \hookrightarrow \mathbb{F}_q(x)$. To get a more exciting ring, we repeat but excluding a point P_0.

- $P_0 = \infty$, we get $\{f \in \mathbb{F}_q(x) : f \text{ has no poles except possibly at } \infty\}$. If $f = f_1/f_2$ then f_2 must be constant so this subring is $\mathbb{F}_q[x]$.
- $P_0 = \sqrt{\alpha}$ for $\square \neq \alpha \in \mathbb{F}_q$, we get $\{f \in \mathbb{F}_q(x) : f \text{ has no poles except possibly at } \sqrt{\alpha}\}$. If $f = f_1/f_2$ then we need $f_2 = c(x^2 - \alpha)^i$, but this also has a zero at $-\sqrt{\alpha}$! Instead we look at the subring $\{f \text{ has no poles except possibly at } \pm\sqrt{\alpha}\} = \mathbb{F}_q[1/(x^2 - \alpha), x/(x^2 - \alpha)]$.

Definition

A *closed point* on $C/\mathbb{F}_q$ is a Galois orbit of points in $C(\overline{\mathbb{F}}_q)$.

The ring of integers of $\mathbb{F}_q(C)$

Definition

Let $K = \mathbb{F}_q(C)$ and fix a finite set S of closed points on C. The *ring of integers of K with respect to S* is

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

Suppose $C : y^2 = x^3 - x$, $p \neq 2$. Then $\mathbb{F}_q[x,y]/(y^2 - x^3 + x) = \{a(x) + yb(x) : a, b \in \mathbb{F}_q[x]\}$.

- Letting $S = \{\infty\}$

$$\mathcal{O}_{K,S} = \{f \in K : f \text{ has no poles except possibly at } \infty\} = \mathbb{F}_q[x,y]/(y^2 - x^3 + x).$$

- Letting $S = \{(0,0)\}$, we change variables: $s = 1/x$, $t = y/x^2$ so that $C : t^2 = s - s^3$.

$$\mathcal{O}_{K,S} = \{f \in K : f \text{ has no poles except possibly at } (x,y) = (0,0)\} = \mathbb{F}_q[s,t]/(t^2 - s + s^3).$$

- Letting $S = \{(-1,0), (0,0), (1,0), \infty\}$

$$\mathcal{O}_{K,S} = \{f \in K : f \text{ has no poles except possibly at } (-1,0), (0,0), (1,0) \text{ or } \infty\}$$
$$= \mathbb{F}_q[x,y,1/y]/(y^2 - x^3 + x).$$

Properties of $\mathcal{O}_{K,S}$

More generally, for *smooth* $C : F(x, y) = 0$ over $\mathbb{F}_q$, taking $S = \{\text{points at } \infty\}$ gives

$$\mathcal{O}_{K,S} = \{f \in K : f \text{ has no poles at affine points on } C\} = \mathbb{F}_q[x, y]/(F(x, y)).$$

A non-constant morphism $\phi : C \to \mathbb{P}^1$ induces an inclusion $\mathbb{F}_q[x] \hookrightarrow \mathbb{F}_q(C)$. Letting $S = \phi^{-1}(\infty)$, it can be shown that

$$\mathcal{O}_{K,S} \text{ is the integral closure of } \mathbb{F}_q[x] \text{ in } K.$$

The field of fractions of $\mathcal{O}_{K,S}$ is K

$\mathcal{O}_{K,S}$ is a Dedekind domain, i.e.

- it's integrally closed in K: discrete valuation rings are integrally closed
- it's Noetherian
- every non-zero prime ideal is maximal: we'll see this soon

This structure allows us to factorize the ideals of $\mathcal{O}_{K,S}$ uniquely into primes.

The primes of $\mathcal{O}_{K,S}$

Recall that for $K = \mathbb{F}_q(C)$ and S a finite set of closed points

$$\mathcal{O}_{K,S} = \{f \in K : f \text{ has no poles outside of } S\} = \bigcap_{\text{closed } P \notin S} \{f \in K : |f|_P \leq 1\}.$$

The unique maximal ideal of $\{f \in K : |f|_P \leq 1\}$ is

$$\{f \in K : |f|_P < 1\} = \{f \in K : f \text{ has a zero at } P\}.$$

From this we can construct a prime ideal of $\mathcal{O}_{K,S}$.

Definition

For a closed point $P \notin S$, the *prime ideal of* $\mathcal{O}_{K,S}$ *at* P is

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

Sanity check: $\mathfrak{p}_{P,S}$ is prime as it's the kernel of the homomorphism

$$\mathcal{O}_{K,S} \ni f \mapsto f(P) \in \overline{\mathbb{F}}_q.$$

The primes of $\mathcal{O}_{K,S}$

Definition

For a closed point $P \notin S$, the *prime ideal of* $\mathcal{O}_{K,S}$ *at* P is

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

Proposition

Every prime ideal of $\mathcal{O}_{K,S}$ is of the form $\mathfrak{p}_{P,S}$ for a closed point $P \notin S$. There's a correspondence between the primes of $\mathcal{O}_{K,S}$ and the Galois orbits of points in $C(\overline{\mathbb{F}}_q)$ not in S.

When $C = \mathbb{P}^1$ and $S = \{\infty\}$ we saw that $\mathcal{O}_{K,S} = \mathbb{F}_q[x]$. Here the prime ideals are generated by irreducible elements. Let $q = 5$, some irreducibles are

$$\begin{array}{ccc} x - \lambda \quad (\lambda \in \mathbb{F}_5) & x^2 - 2 & x^6 - 2 \\ \lambda \in \mathbb{P}^1(\mathbb{F}_5) & \{\pm\sqrt{2}\} \subset \mathbb{P}^1(\mathbb{F}_{25}) & \{\zeta\sqrt[6]{2} : \zeta^6 = 1\} \subset \mathbb{P}^1(\mathbb{F}_{15625}) \end{array}$$

From this description, we deduce that every prime ideal of $\mathcal{O}_{K,S}$ is maximal!

Example

Let $C : y^2 = x^3 - x$, $K = \mathbb{F}_q(C)$ and $S = \{\infty\}$. We saw previously that

$$\mathcal{O}_{K,S} = \mathbb{F}_q[x,y]/(y^2 - x^3 + x), \qquad \mathfrak{p}_{P,S} = \{f \in \mathcal{O}_{K,S} : f \text{ has a zero at } P\}$$

for closed $P \neq \infty$. Let $q = 7$: $\mathfrak{p}_{(0,0),S} = (x,y)$ and $\mathfrak{p}_{\{(2,\pm\sqrt{-1})\},S} = (x-2, x^3 - x + 1)$.

More generally,

- The primes in $\mathcal{O}_{K,S}$ correspond to primes $\mathfrak{p}$ of $\mathbb{F}_q[x,y]$ containing $(y^2 - x^3 + x)$.
- Since $(0) \subset (y^2 - x^3 + x) \subseteq \mathfrak{p} \subseteq \mathfrak{m} \subset \mathbb{F}_q[x,y]$, we just determine the maximal ideals $\mathfrak{m}$.
- A generalisation of Hilbert's Nullstellensatz says: the maximal ideals of $\mathbb{F}_q[x,y]$ arise from points $P = (p_x, p_y) \in \overline{\mathbb{F}}_q^2$. They are $(x - p_x, y - p_y) \cap \mathbb{F}_q[x,y]$.
- The maximal ideals for $P, P' \in \overline{\mathbb{F}}_q^2$ are equal precisely when $\sigma(p_x) = p'_x$ and $\sigma(p_y) = p'_y$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.
- The prime ideals in $\mathcal{O}_{K,S}$ correspond to closed points $\neq \infty$ on C.

The Chinese Remainder Theorem

Fix $K = \mathbb{F}_q(C)$, S a finite set of closed points. We have a ring $\mathcal{O}_{K,S}$ with prime ideals $\mathfrak{p}_{P,S}$.

The Chinese Remainder Theorem

Let $P, Q \notin S$ be distinct closed points. There's an isomorphism

$$\mathcal{O}_{K,S}/(\mathfrak{p}_{P,S} \cap \mathfrak{p}_{Q,S}) \longrightarrow \mathcal{O}_{K,S}/\mathfrak{p}_{P,S} \times \mathcal{O}_{K,S}/\mathfrak{p}_{Q,S}.$$

In particular, 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 $f(Q) = t$.

For example, let $C : y^2 = x^3 - x$ over $\mathbb{F}_7$, $S = \{\infty\}$, $P = (0,0)$ and $Q = \{(2, \pm\sqrt{-1})\}$.

Let's find $f = a(x) + yb(x) \in \mathcal{O}_{K,S}$ $(a, b \in \mathbb{F}_7[x])$ with $f(P) = 3$ and $f(Q) = 2\sqrt{-1}$.

$$f(P) = 3 \;\Rightarrow\; a(0) = 3, \qquad f(Q) = 2\sqrt{-1} \;\Rightarrow\; a(2) + \sqrt{-1}b(2) = 2\sqrt{-1}.$$

Can take $b(x) = x$ and $a(x) = 2x + 3$ giving $f(x) = 2x + 3 + xy$.

Thank you for listening!

Any questions?