Title

D. Zack Garza

Contents

1 | Lecture 13

Recall that we previously looked at the regular function fields: we took a function field in one variable and considered the class of function fields for which we could take any extension of the constant field that we wanted. As long as the ground field is perfect, being regular is equivalent to the constant subfield being k itself. However, we haven't done anything with them yet!

If you take an algebraic closure of the finite ground field $\mathbb{F}_q$, there is a unique subextension of degree r for every r, so we call that $\mathbb{F}_{q^r}$. The extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is cyclic galois, with a geometric Frobenius $x \to x^q$. Note that $\mathbb{F}_{q^r}$ is the fixed field of F^r, the rth power of the Frobenius map. We set $K_r := K\mathbb{F}_{q^r}$, which is a regular function field over $\mathbb{F}_{q^r}$. Note that we could view this as a function field just over $\mathbb{F}_q$, but it would not be regular. Then K_r/K is a degree r arithmetic extension of function fields.

Question 1.0.1: What happens to places when making this scalar extension? I.e., how to places in K decompose in K_r?

Remark 1.0.2: This is related to an Algebraic Number Theory I problem: for $v \in \Sigma(K_{/\mathbb{F}_q})$ above an affine Dedekind domain R such that $v \in \Sigma(K/R)$, let S be the integral closure of K in K_r. Then we want to factor $p_v S$?

> Not quite sure.

1.1 How Places Split

> **Lemma 1.1.1** *(Key lemma about how places split.).*
> Suppose $d := \deg(v)$. Then K_r/K is galois, so we have $efg = r$. In fact, $c = 1$, so $f = \dfrac{r}{\gcd(d,r)}$
> and $g = \gcd(d, r)$ and each place $w \in \Sigma(K_r/\mathbb{F}_{q^r})$ has degree $\dfrac{d}{\gcd(d,r)}$.

Remark 1.1.2: We have the following cases:

- The extension is *inert* iff $\gcd(d, r) = 1$,

- The extension *splits completely* iff $r \mid d$,

- All w dividing v have degree 1 iff $d \mid r$.

The last thing we proved was that the degree zero divisor class group is finite when we're over a finite ground field. Why is this true? Whenever there is a divisor of degree n, then the set of degree n divisors is a coset of the degree zero divisors, all of which have the same cardinality. We proved

finiteness using the Riemann-Roch theorem, using the fact that the set of *effective* degree n divisors is finite for all n.

The next main topic will be the **zeta function**, which keeps track of three equivalent packets of information: A_n, the number of effective divisors of degree n, the number of places of degree d (since an effective divisor is a linear combination of these), and N_r the number of degree 1 points in the degree r extension, i.e. the number of $\mathbb{F}_{q^r}$ rational points.

1.2 Counting Effective Divisors

Lemma 1.2.1*(?).*
Suppose $C \in \mathrm{Cl}(K)$, then

- The number of effective divisors $D \in [C]$ is given by

$$\frac{q^{\ell(C)} - 1}{q - 1},$$

  where $\ell(C)$ is the dimension of the linear system associated to the divisor class C, and this is the dimension of a projective space over $\mathbb{F}_q$.

- For all $n > 2g - 2$ with $\delta \mid n$, we have

$$A_n = h\left(\frac{q^{n+1-g} - 1}{q - 1}\right).$$

Proof (?).
Proof of (a): The set of effective divisors linearly equivalent to D is naturally viewed as the projectivization $\mathbb{P}\mathcal{L}(D)$ of the one-dimensional subspaces of the linear system of that divisor class. It is then a fact that the number of elements in a d-dimensional vector space over $\mathbb{F}_q$ has dimension precisely $\dfrac{q^d - 1}{q - 1}$ elements. The projectivization comes in because two different functions have the same divisor if one of them is a constant multiple of the other. Note that the number of elements is computed as the number of nonzero elements divided by the number of nonzero scalars.

Proof of (b): This will come out of the Riemann-Roch theorem. In order to compute the number of divisors in a divisor class, you need to know the dimension of the linear system, which is not easy in general. However, if the divisor class has sufficiently large degree, the Riemann-Roch theorem tells you exactly what it is. As long as $n > 2g - 2$, there is no correction term, and the dimension of the linear system is equal to its degree minus the genus plus one. So by Riemann-Roch, since $\deg(D) > 2g - 2$, D is non-special and $\ell([D]) = n - g + 1$, which yields the desired formula for A_n. $\blacksquare$

Remark 1.2.2: This is the sharpest result possible: the canonical divisor has degree $2g - 2$ and is special, so this fails for the canonical class.

The upshot: there are three piece of information:

- N_r, the number of $\mathbb{F}_{q^r}$ rational points,

- $\left| \Sigma_d(K_{/\mathbb{F}_q}) \right|$ the number of closed points / places of degree d,

- A_n the number of effective divisors of degree n,

and there are simple formulas relating these. Moreover, it is enough to know only finitely many of these quantities, where the number depends on g.

1.3 Hasse-Weil Zeta Functions

There is a general theory that will unify

- The Riemann zeta function, thought of as the zeta function of $\mathbb{Z}$,

- The Dedekind zeta function, attached to the ring of integers over a number field,

- The Hasse-Weil zeta function of a one variable function field over a finite field,

all of which will be special cases of a *Serre zeta function* which can be attached to a finite type scheme over $\mathbb{Z}$.

Note that we aren't specifically discussing schemes in this course, but you don't need to know much about what a scheme is to define the Hasse-Weil zeta function. Just note that an affine finite-type $\mathbb{Z}$-scheme corresponds to a finitely generated $\mathbb{Z}$-algebra, and a general finite-type $\mathbb{Z}$-scheme will be covered by finitely many affine ones, the zeta function will be determined by these finitely many $\mathbb{Z}$-algebras and some kind of inclusion-exclusion principle (since the scheme is a not necessarily disjoint union of affine schemes).

Recall that $A_n = A_n(K)$ is the number of effective divisors of degree n, which we've proved is finite. We have a formula when $n > 2g - 2$, namely

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n = \sum_{D \in \mathrm{Div}^+(K)} t^{\deg(D)} \in \mathbb{Z}[[t]],$$

where Div^+ are the effective divisors and we've collected terms based on their degree. This is analogous to the Dedekind zeta function of a number field K, a formal Dirichlet series which is

given by

$$\zeta_K(s) = \sum_{I \in \mathcal{I}(\mathbb{Z}_K^\bullet)} |\mathbb{Z}_K/I|^{-s}.$$

where the sum is now over all of the nonzero ideals of the ring of integers, where we measure the size using the *norm*, i.e. the size of the residue field. There's an analogy between integral ideals (vs fractional ideals) and effective divisors. We could get an Euler product decomposition for the Dedekind zeta function by only considering prime ideals, since in a Dedekind domain all ideals factor uniquely into prime ideals. In fact, any nonzero ideal is a linear combination of prime ideals. Similarly, the effective divisors are linear combinations of effective divisors, so an Euler product expansion is possible here too. If we take a prime ideal, since we're in a discrete valuation ring, we can consider the local ring at that point. We can take the residue field, which in general won't be finite, but will be a finite extension. So a reasonable measure of the size of a prime divisor would be the dimension of its residue field as a vector space over K.

Note that if we wanted to make these look even more similar to each other, we could define a_n (depending on $\mathbb{Z}_K$) as

$$a_n = \left| \left\{ I \trianglelefteq \mathbb{Z}_K \mid |\mathbb{Z}_K/I| = n \right\} \right|,$$

which allows us to write

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

Question 1.3.1: Where we're going: how does $Z(t)$ depend on K?

Answer 1.3.2: It turns out that it only depends on $A_0, A_1, \cdots, A_{2g-2}$, and thus $Z(t)$ depends on only finitely much information. We will

1. Show that $Z(t) \in \mathbb{Z}(t)$, i.e. it is a rational function and can be written $Z(t) = P(t)/Q(t)$.

   > Note: the denominator will always be the same, $(1-t)(1-qt)$, and we'll always have $\deg P = 2g$. This is essentially coming from ℓ-adic cohomology. We'll also determine the leading coefficient.

2. Understand $\deg P$ and $\deg Q$ in terms of the genus g.

3. Ask about the roots of $P(t)$, and establish a Riemann hypothesis for Dedekind zeta functions (and in particular, the Riemann zeta function).

   > In particular, what are their magnitudes? This is what Weil did, this is the big theorem in this area. Note that we'll need to consider reciprocal roots, which will end up having magnitude $\sqrt{q}$. We'll see why this happens, and it turns out to be analogous to fact that the nontrivial zeros of the Riemann zeta function have real part $1/2$.

These are approximately in order of difficulty. The first two will follow from Riemann-Roch, but the third will be much deeper. This is essentially a positive characteristic analogue of the usual Riemann

hypothesis. Note that we're in a global field, the positive characteristic analog of a number field, and for number fields the Riemann hypothesis is the single outstanding problem. In the function field case, it is a theorem!

> **Proposition 1.3.3***(Formula for the zeta function exhibiting rationality).*
> Let $K_{/\mathbb{F}_q}$ have genus g and $\delta = I(K)$ the index, the least positive degree of a divisor.[a]
>
> a. If $g = 0$, then
>
> $$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-q^\delta t^\delta} - \frac{1}{1-t^\delta}\right).$$
>
> b. If $g \geq 1$, then $Z(t) + F(t) + G(t)$ where
>
> $$F(t) = \frac{1}{q-1}\sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)}t^{\deg(C)}$$
>
> $$G(t) = \frac{h}{g-1}\left(\frac{q^{1-g}(qt)^{2g-2+\delta}}{1-(qt)^\delta} - \frac{1}{1-t^\delta}\right),$$
>
> so F involves summing over all divisor classes of degree at most $2g-2$, and G is a term coming from Riemann-Roch involving the class number h.
>
> ――――――――――――――――――――
> [a]It will turn out (by a theorem of Schmidt) that $\delta = 1$ in the case of a finite ground field.

Note that as a consequence, it will definitely be rational in q, and will have a simple pole at $t = 1$.

There's no major idea for the proof: when the degree of the divisor class is sufficiently large, we just have an exact formula. If it is smaller, than the formula involves the dimension of the linear system.

1.4 Proof of Rationality

> *Proof (of rationality of $Z(t)$).*
> Recall that $\ell(C)$ is the dimension of the associated Riemann-Roch space.
> When $g = 0$, by Riemann-Roch we have $\mathrm{Cl}^0(K) = 0$ over any ground field $\Bbbk$ (see exercises), and so $h = 1$. Since every $n \geq 0$ satisfies $n \geq 2g - 2$ when $g = 0$, if $\delta \mid n$ we have
>
> $$A_n = h\left(\frac{q^{n+1-g}-1}{q-1}\right) = \frac{q^{n+1}-1}{q-1},$$
>
> and since $A_n = 0$ unless n is divisible by δ, we have
>
> $$Z(t) = \sum_{n=0}^\infty A_n t^n = \sum_{n=0}^\infty A_{\delta n} t^{\delta n} = \sum_{n=0}^\infty \frac{q^{\delta n+1}-1}{q-1}t^{\delta n}.$$

This can now be split into two terms, each of which will have a geometric series to sum. Now let $g \geq 1$, and write

$$\sum_{n=0}^{\infty} A_n t^n = \sum_{\deg(C) \geq 0} \left| \left\{ A \in C \mid A \geq 0 \right\} \right| t^{\deg(C)},$$

where we instead count the number of divisors in each divisor class (a consequence of the previous lemma). Continuing this computation, we separate out the part where $\deg(C) \leq 2g-2$ and pull out the -1 in the numerator:

$$\cdots = \sum_{\deg(C) \geq 0} \frac{q^{\ell(C)} - 1}{q - 1} t^{\deg(C)}$$

$$= \left(\frac{1}{q-1} \right) \left(\sum_{0 \leq \deg(C) \leq 2g-2} q^{\ell(C)} t^{\deg(C)} + \sum_{\deg(C) > 2g-2} q^{\deg(C)-g+1} t^{\deg(C)} - \sum_{\deg(C) \geq 0} t^{\deg(C)} \right)$$

$$:= F(t) + G(t),$$

so we can write

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg(C) \leq 2g-2} q^{\ell(C)} t^{\deg(C)}$$

$$(q-1)G(t) = \sum_{n=\frac{2g-2}{\delta}+1}^{\infty} h q^{n\delta+1-g} t^{n\delta} - \sum_{n=0}^{\infty} h t^{n\delta}.$$

Note that $\delta \mid 2g-2$ since the canonical divisor has degree $2g-2$ and δ is a gcd. Note that for $g = 1$, the index divides zero, which tells you nothing about it! This now reduces to some geometric series that can be summed, which shows these are rational functions in t. ∎

Exercise 1.4.1 *(?)*: Let $K = \mathbb{F}_q(t)$, then $g = 0, \delta = 1$, and

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

We will see in general that the numerator is of the form $L(t)$ where $L \in \mathbb{Z}[t]$ has degree $2g$.

Note that this all generalized to higher dimensional projective varieties $X_{/\mathbb{F}_q}$, for which these properties were proved by the work of Deligne. In general, $Z(t)$ will be of the form

$$Z_X(t) = \frac{L_1(t) \cdots L_{2d-1}(t)}{L_0(t) \cdots L_{2d}(t)},$$

where $d = \dim(X)$ and $\deg L_i$ will be the dimension of the ith ℓ-adic cohomology. Moreover, if $X_{/\mathbb{F}_q}$ is a reduction mod q of a variety in characteristic zero, these will be the Betti numbers of $X_{/\mathbb{C}}$. If we take a compact Riemann surface, which has a honest topological genus of g, the Betti numbers are $1, 2g, 1$, and this recovers the formula above for $L(t)$ and its degree.

The next result will be the following theorem:

> **Theorem 1.4.2***(Schmidt, 1910ish).*
> For all $K_{/\mathbb{F}_q}$,
>
> $$\delta = I(K) = 1.$$

This will greatly simplify the previous formulas. A useful application is if you have a genus zero curve of index 1, applying Riemann-Roch to a divisor of degree 1 shows that the function field is rational. Thus the only genus zero function field over $\mathbb{F}_q$ is the rational function field. Useful aside: the Riemann hypothesis here gives an estimate of the number of $\mathbb{F}_{q^r}$ rational points.