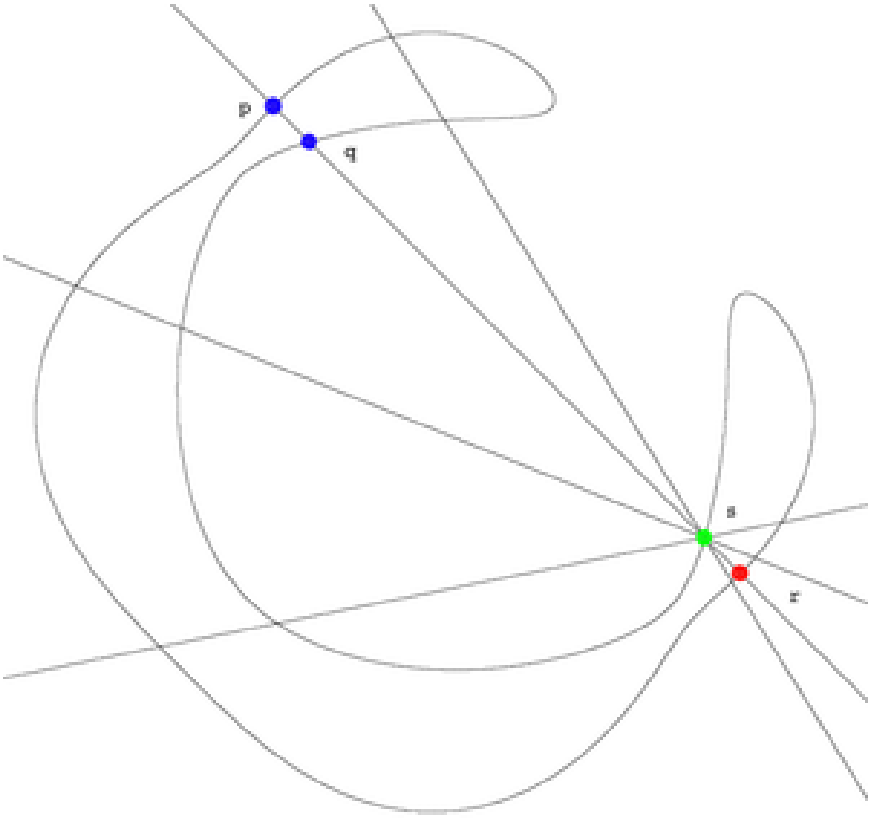


Notes: These are notes live-tex'd from a graduate course in Algebraic Curves taught by Pete Clark at the University of Georgia in Fall 2020. As such, any errors or inaccuracies are almost certainly my own.

Algebraic Curves

University of Georgia, Fall 2020

D. Zack Garza

D. Zack Garza
University of Georgia
dzackgarza@gmail.com

Contents

1 | Lecture 1?

1.1 Field Theory

See Chapter 11 of Field Theory notes.

1.1.1 Notion 1

Definition 1.1.1 (Finitely Generated Field Extension)
A field extension ℓ/k is *finitely generated* if there exists a finite set $x_1, \cdots, x_n \in \ell$ such that $\ell = k(x_1, \cdots, x_n)$ and ℓ is the smallest field extension of k.
Concretely, every element of ℓ is a quotient of the form $\dfrac{p(x_1, \cdots, x_n)}{q(x_1, \cdots, x_n)}$ with $p, q \in k[x_1, \cdots, x_n]$.

There are three different notions of finite generation for fields, the above is the weakest.

1.1.2 Notion 2

The second is being finitely generated as an algebra:

Definition 1.1.2 (Finitely Generated Algebras)
For $R \subset S$ finitely generated algebras, S is finitely generated over R if every element of S is a polynomial in $x_1, \cdots, x_n$, with coefficients in R, i.e. $S = R[x_1, \cdots, x_n]$.

Note that this implies the previous definition, since anything that is a polynomial is also a quotient of polynomials.

1.1.3 Notion 3

The final notion: ℓ/k is finite (finite degree) if ℓ is finitely generated as a k-module, i.e. a finite-dimensional k-vector space.

Definition 1.1.3 (Rational Function Field)
A *rational function field* is $k(t_1, \cdots, t_n) \coloneqq ff\left(k[t_1, \cdots, t_n]\right)$.

Note that we can make a similar definition for infinitely many generators by taking a direct limit (here: union), and in fact every element will only involve finitely many generators.

Exercise 1.1.1:

a. Show $k(t)/k$ is finitely generated by notion (3) but not by (2).

b. Show that $k[t]/k$ is (2) but not (1).

Note $k[t]$ is not a field.

c. Show that it is not possible for a **field** extension to satisfy (2) but not (1).

Hint: Zariski's lemma.

d. Show that if ℓ/k is finitely generated by (3) and algebraic, then it satisfies (1).

Theorem 1.1.1 ***(Field Theory Notes 11.19).***
If $L/K/F$ are field extensions, then L/F is finitely generated $\iff$ K/F and L/K are finitely generated.

See Artin-Tate Lemma, this doesn't necessarily hold for general rings.

Definition 1.1.4 (Algebraically Independent)
For ℓ/k, a subset $\{x_i\} \subset \ell$ is *algebraically independent* over k if no finite subset satisfies a nonzero polynomial with k coefficients.
In this case, $k[\{x_i\}]/k$ is *purely transcendental* as a rational function field.

Theorem 1.1.2 ***(?).***
For ℓ/k a field extension,

a. There exists a subset $\{x_i\} \subset \ell$ algebraically independent over k such that $\ell/k(\{x_i\})$ is algebraic.

b. If $\{y_t\}$ is another set of algebraically independent elements such that $\ell/k(\{y_t\})$ is algebraic, then $|\{x_i\}| = |\{y_t\}|$.

Thus every field extension is algebraic over a purely transcendental extension. A subset as above is called a *transcendence basis*, and every 2 such bases have the same cardinality.

We have a notion of generation (similar to "spanning"), independence, and bases, so there are analogies to linear algebra (e.g. every vector space has a basis, any two have the same cardinality). There is a common generalization: matroids.

Definition 1.1.5 (Transcendence Degree)
The *transcendence degree* of ℓ/k is the cardinality of any transcendence basis.
Analogy: dimension in linear algebra.

Theorem 1.1.3 ***(Transcendence Degree is Additive in Towers).***
If $L/K/F$ are fields then $\text{trdeg}(L/F) = \text{trdeg}(K/F) + \text{trdeg}(L/K)$.

Theorem 1.1.4 ***(Bounds on Transcendence Degree).***
Let K/k be finitely degenerated, so $K = k(x_1, \cdots, x_n)$. Then $\text{trdeg}(K/k) \leq n$, with equality iff K/k is purely transcendental.

Proof .
Suppose K is monogenic, i.e. generated by one element. Then $\text{trdeg}(F(x)/F) = \mathbb{1}[x/F \text{ is transcendental}]$.
So the degree increases when a transcendental element is added, and doesn't change when x is algebraic.
By additivity in towers, we take $k \hookrightarrow k(x_1) \hookrightarrow k(x_1, x_2) \hookrightarrow \cdots \hookrightarrow k(x_1, \cdots, x)n) = K$ to obtain a chain of length n. The transcendence degree is thus the number of indices i such that x_i is transcendental over $k(x_1, \cdots, x_{i-1})$.

Similar to checking if a vector is in the span of a collection of previous vectors.

■

Definition 1.1.6 (Function Fields)
For $d \in \mathbb{Z}^{\geq 0}$, an extension K/k is *a function field in d variables* (i.e. of dimension d) if K/k is finitely generated of transcendence degree d.

The study of such fields is birational geometry over the ground field k. $k = \mathbb{C}$ is of modern interest, things get more difficult in other fields.

The case of $d = 1$ is much easier: the function field will itself be the geometric object and everything will built from that.

Main tool: valuation theory, which will correspond to points on the curve.

1.2 Case Study: The Luroth Problem.

For which fields k and $d \in \mathbb{Z}^{\geq 0}$ is it true that if $k \subset \ell \subset k(t_1, \cdots, t_d)$ with $k(t_1, \cdots, t_d)/\ell$ finite then ℓ is purely transcendental?

Theorem 1.2.1 ***(Luroth).***
True for $d = 1$: For any $k \subset \ell \subset k(t)$, $\ell = k(x)$.

Theorem 1.2.2 ***(Castelnuovo).***
Also true for $d = 2, k = \mathbb{C}$.

Theorem 1.2.3 ***(Zariski).***
No if $d = 2$, $k = \bar{k}$, and k is positive characteristic. Also no if $d = 2, k \neq \bar{k}$ in characteristic zero.

Theorem 1.2.4 ***(Clemens-Griffiths).***
No if $d \geq 3$ and $k = \mathbb{C}$.

Unirational need not imply rational for varieties.

Exercise 1.2.1: Let k be a field, G a finite group with $G \hookrightarrow S_n$ the Cayley embedding. Then S_n acts by permutation of variables on $k(t_1, \cdots, t_n)$, thus so does G. Set $\ell \coloneqq k(t_1, \cdots, t_n)^G$ the fixed field, then by Artin's observation in Galois theory: if you have a finite field acting effectively by automorphisms on a field then taking the fixed field yields a galois extension with automorphism group G.

So $\mathrm{Aut}(k(t_1, \cdots, t_n)/\ell) = G$.A

a. Suppose $k = \mathbb{Q}$, and show that an affirmative answer to the Luroth problem implies an affirmative answer to the inverse galois problem for $\mathbb{Q}$.

Hint: works for any field for which Hilbert's Irreducibility Theorem holds.

b. $\ell/\mathbb{Q}$ need not be a rational function field, explore the literature on this: first example due to Swan with $|G| = 47$.

c. Can still give many positive examples using the Shepherd-Todd Theorem.

What's a global field?

1.3 Onto Business

Definition 1.3.1 (?)
For K/k a field extension, set $\kappa(K)$ to be the algebraic closure of k in K, i.e. special case of *integral closure*. If K/k is finitely generated, then $\kappa(K)/k$ is finite degree.
Here $\kappa(k)$ is called the *field of constants*, and K is also a function field over $\kappa(k)$.

In practice, we don't want $\kappa(k)$ to be a proper extension of k.

If this isn't the case, we replace considering K/k by $K/\kappa(k)$. If K/k is finitely generated, then

$$k \xhookrightarrow{\text{finite}} \kappa(k) \xhookrightarrow{\text{finitely generated}} K$$

Where we use the fact that from above, $\kappa(k)/k$ is finitely generated and algebraic and thus finite, and by a previous theorem, if K/k is transcendental then $K/\kappa(k)$ is as well, and thus finitely generated. Thus if you have a function field over k, you can replace k by $\kappa(k)$ and regard K as a function field over $\kappa(k)$ instead.

1.4 Lecture 1, A Review

Review of lecture one:

Theorem 1.4.1 ***(Finitely Generated in Towers).***
See video

- Transcendence bases
- Lüroth problem

2 | Lecture 2?

For K/k a one variable function field, if we want a curve C/k, what are the points? We'll use *valuations*, see NT 2.1.

See also completions, residue fields.

If $R \subset K$ a field, R is a *valuation ring* of K if for all $x \in K^\times$, at least one of $x, x^{-1} \in R$.

Example 2.0.1: The valuation rings of $\mathbb{Q}$ are $\mathbb{Z}_{(p)} \coloneqq \mathbb{Z}[\left\{ \frac{1}{\ell} \;\middle|\; \ell \neq p \right\}]$ for all primes p.

See also Krull valuation, takes values in some totally ordered commutative group.

Exercise 2.0.1: Show that a valuation ring is a local ring, i.e. it has a unique maximal ideal.

Example 2.0.2: Where does the log come from?

There is a p-adic valuation:

$$\begin{aligned} v : \mathbb{Q} &\to \mathbb{Z}_{(p)} \\ \frac{a}{b} = p^n \frac{u}{v} &\mapsto n. \end{aligned}$$

Then we recover

$$\mathbb{Z}_{(p)} = \left\{ x \in \mathbb{Q}^\times \;\middle|\; v_p(x) \geq 0 \right\} \cup \{0\}$$
$$\mathfrak{m}_{(p)} = \left\{ x \in \mathbb{Q}^\times \;\middle|\; v_p(x) > 0 \right\} \cup \{0\}$$

.

There is a p-adic norm

$$\begin{aligned} |\cdot|_p : \mathbb{Q} &\to \mathbb{R} \\ 0 &\mapsto 0 \\ x &\mapsto p^{-n} = p^{-v_p(x)}. \end{aligned}$$

Then we get an ultrametric function, a non-archimedean function

$$\begin{aligned} d_p : \mathbb{Q}^2 &\to \mathbb{R} \\ (x, y) &\mapsto |x - y|_p. \end{aligned}$$

We then recover $v_p(x) = -\log_p |x|_p$.

See NT 1 notes.

For $A \subset K$ a subring of a field, we'll be interested in the place $\tilde{\Sigma} = \{\text{Valuation rings } R_v \text{ of } K\} \;\middle|\; A \subset R_v \subsetneq K$. Thus the valuation takes non-negative values on all elements of K. Can equip this with a topology (the "Zariski" topology, not the usual one). This is always quasicompact, and called the *Zariski-Riemann space*. Can determine a sheaf of rings to make this a locally ringed space.

We can define an equivalence of valuations and define the set of *places*

$$\Sigma(K/k) \coloneqq \left\{ \text{Nontrivial valuations } v \in K \;\middle|\; v(x) \geq 0 \, \forall x \in k^\times \right\},$$

which will be the points on the curve. Here the Zariski topology will be the cofinite topology (which is not Hausdorff). Scheme-theoretically, this is exactly the set of closed points on the curve.

Definition 2.0.1 (?)
Generic point: closure is entire space.

Note we will have unique models for curves, but this won't be the case for surfaces: blowing up a point will yield a birational but inequivalent surface.

From this we can also define *divisor group* as the free $\mathbb{Z}$-module on $\Sigma(K/k)$, which comes with a degree map

$$\deg : \mathrm{Div}(K) \to \mathbb{Z}$$

which need not be surjective.

We can consider principle divisors with the map

$$\begin{aligned} K^\times &\to \mathrm{Div}(K) \\ f &\mapsto (f). \end{aligned}$$

We can define the class group as divisors modulo principle divisors $\mathrm{cl}(K) = \mathrm{Div}(K)/\operatorname{im}(K^\times)$ and the Riemann-Roch space $\mathcal{L}(D)$. The Riemann-Roch theorem will then be a statement about $\dim \mathcal{L}(D)$.

3 | Lecture 3

3.1 Base Extension

Given some object A/k and $k \hookrightarrow \ell$ is a field extension, we would like some extended object A/ℓ.

Example 3.1.1: An *affine variety* V/k is given by finitely many polynomials in $p_i \in k[t_1, \cdots, t_n]$, and base extension comes from the map $k[t_1, \cdots, t_n] \hookrightarrow \ell[t_1, \cdots, t_n]$.

More algebraically, we have the affine coordinate ring over k given by $k[V] = k[t_1, \cdots, t_n]/\langle p_i \rangle$, the ring of polynomial functions on the zero locus corresponding to this variety. We can similarly replace k be ℓ in this definition. Here we can observe that $\ell[V] \cong k[V] \otimes_k \ell$.

In general we have a map

$$\begin{aligned} \cdot \otimes_k \ell& \\ \{k\text{-vector spaces}\} &\to \{\ell\text{-vector spaces}\} \\ \{k\text{-algebras}\} &\to \{\ell\text{-algebras}\}. \end{aligned}$$

Note that this will be an exact functor on the category k-Vect, i.e. ℓ is a flat module. Here everything is free, and free $\implies$ flat, so things work out nicely.

What about for function fields?

Since k is a k-algebra, we can consider $k \otimes_k \ell$, however this need not be a field.

> Note: tensor products of fields come up very often, but don't seem to be explicitly covered in classes! We'll broach this subject here.

Exercise 3.1.1: If ℓ/k is algebraic and $\ell \otimes_k \ell$ is a domain, the $\ell = k$.

I.e. this is rarely a domain. Hint: start with the monogenic case, and also reduce to the case where the extension is not just algebraic but finite.

Tensor products of field extensions are still interesting: if ℓ/k is finite, it is galois $\iff \ell \otimes_k \ell \cong \ell^{[\ell:k]}$. So its dimension as an ℓ-algebra is equal to the degree of ℓ/k, so it splits as a product of copies of ℓ.

Remark 3.1.1: We'd like the tensor product of a field to be a field, or at least a domain where we can take the fraction field and get a field. This hints that we should not be tensoring algebraic extensions, but rather transcendental ones.

Exercise 3.1.2: For ℓ/k a field extension,

a. Show $k(t) \otimes_k \ell$ is a domain with fraction field $\ell(t)$.

b. Show it is a field $\iff \ell/k$ is algebraic.

Proposition 3.1.1 ***(FT 12.7, 12.8).***
Let $k_1, k_2/k$ are field extensions, and suppose $k_1 \otimes_k k_2$ is a domain. Then this is a field $\iff$ at least one of k_1/k or k_2/k is algebraic.

Reminder: for ℓ/k and $\alpha \in \ell$ algebraic over k, then $k(\alpha) = k[\alpha]$.

So we'll concentrate on when $K \otimes_k \ell$ is a domain. What's the condition on a function field K/k that guarantees this, i.e. when extending scalars from k to ℓ still yields a domain? If this remains a domain, we'll take the fraction field and call it the *base change*.

Exercise 3.1.3: If K/k is finitely generated (i.e. a function field) and $K \otimes_k \ell$ is a domain, then $ff(K \otimes_k \ell)/\ell$ is finitely generated.

The point: if taking a function field and extending scalars still results in a domain, we'll call the result a function field as well.

Most of all, we want to base change to the algebraic closure. We'll have issues if the constant field is not just k itself:

Lemma 3.1.
If $K \otimes_k \bar{k}$ is a domain, then the constant field $\kappa(k) = k$.

Proof .
Use the fact that $\cdot \otimes_k V$ is exact. We then get an injection

$$\begin{array}{ccc} \kappa(k) \otimes_k \kappa(k) & \hookrightarrow & K \otimes_k \bar{k} \\ & \searrow \quad \nearrow & \\ & \kappa(k) \otimes_k \bar{k} & \end{array}$$

Here we use the injections $\kappa(k) \hookrightarrow \bar{k}$ and $\kappa(k) \hookrightarrow K$.
We now have an injection of k-algebras, and subrings of domains are domains. So apply the first exercise: the only way this can happen is if $\kappa(k) = k$.

■

Exercise 3.1.4: The simplest possible case: describe $\mathbb{C}(t) \otimes_{\mathbb{R}} \mathbb{C}$, tensored as $\mathbb{R}$-algebras.

Won't be a domain by the lemma, some $\mathbb{C}(t)$-algebra of dimension 2.

In order to have a good base change for our function fields, we want to constant extension to be trivial, i.e. $\kappa(k) = k$. This requires that the ground field be algebraically closed.

In this case, you might expect that extending scalars to the algebraic closure would yield a field again. This is true in characteristic zero, but false in positive characteristic.

A more precise question: if $\kappa(k) = k$, must $K \otimes_K \bar{k}$ be a field? If that's true and we're in positive characteristic, recalling the for an algebraic extension this being a field is equivalent to it being a domain. But if that's a domain, the tensor product of every algebraic extension must be a domain, which is why this is an important case.

If so, then $K \otimes_k k^{\frac{1}{p}}$ is a field, where $k^{\frac{1}{p}} \coloneqq k(\left\{x^{\frac{1}{p}} \;\middle|\; x \in k\right\})$ is obtained by adjoining all pth roots of all elements. This is a purely inseparable extension. The latter condition (this tensor product being a field) is one of several equivalent conditions for a field to be separable.

Note that frobenius maps $k^{\frac{1}{p}} \twoheadrightarrow k$, so this is sort of like inverting this map.

Remember that K/k is transcendental, and there is an extended notion of separability for non-algebraic extensions. Another equivalent condition is that every finitely generated subextension is separably generated, i.e. it admits a transcendence basis $\{x_i\}$ such that $k \hookrightarrow k(\{x_i\}) \hookrightarrow F$ where $F/k(\{x_i\})$ is algebraic and separable. Such a transcendence basis is called a *separating transcendence basis*. Since we're only looking at finitely generated extensions, we wont' have to worry much about the difference between separable and separably generated.

What's the point? There's an extra technical condition to ensure the base change is a field: the function field being separable over the ground field.

Is this necessarily the case if $\kappa(k) = k$? No, for a technical reason:

⚠ **Warning 3.1.1:** This is pretty technical, yo.

Example 3.1.2: Set $k = \mathbb{F}_p(a, b)$ a rational function field in two variables sa the ground field. Set

$$A \coloneqq k[x, y] / \left\langle ax^p + b - y^b \right\rangle.$$

Then A is a domain, so set $k = ff(A)$.

Claim: $\kappa(k) = k$, so k is algebraically closed in this extension, but K/k is *not* separable. How to show: extending scalars to $k^{\frac{1}{p}}$ does not yield a domain.

Let $\alpha, \beta \in \bar{k}$ such that $\alpha^p = a, \beta^b = b$, so

$$ax^p + b - y^b = (\alpha x + \beta - y)^p,$$

which implies $K \otimes_k k^{\frac{1}{p}}$ is not a domain: $k[x, y]$ is a UFD, so the quotient of a polynomial is a domain iff the polynomial is irreducible. However, the pth power map is a homomorphism, and this exhibits the image of the defining polynomial as something non-irreducible.

Note that $f(x, y) = ax^p + b - y^p$ is the curve in this situation. The one variable function field is defined by quotienting out a function in two variables and taking the function field. Every 1-variable function field can be obtained in this way. Therefore this polynomial is irreducible, but becomes reducible over the algebraic closure. So we'd like the polynomial to be irreducible over both.

Remark 3.1.2: This is pretty technical, but we won't have to worry if $k = k^{\frac{1}{p}}$. Equivalently, frobenius is surjective on k, i.e. k is a perfect field.

If k is not perfect, it can happen (famous paper of Tate) making an inseparable base extension can decrease the genus of the curve.

Reminder: the perfect fields:

- Anything characteristic zero, every reducible polynomial is separable.
- Any algebraically closed field
- Finite fields (frobenius is always injective)

Imperfect fields include:

- Function fields in characteristic p
- Complete discretely valued fields $k((t))$ in characteristic p

Look up uniformizing elements and valuations.

Theorem 3.1.1 ***(FT 12.20).***
For field extensions K/k, TFAE

1. $\kappa(k) = k$ and K/k is separable
2. $K \otimes_k \bar{k}$ is a domain, or equivalently a field
3. For all field extensions ℓ/k, $K \otimes_k \ell$ is a domain.

Allows making not just an algebraic base change, but a totally arbitrary one.

A field extension satisfying these conditions is called **regular**.

Regular corresponds to nonsingularity in this neck of the woods.

Remark 3.1.3: The implication 2 $\implies$ 3 is the interesting one. To prove it, reduces to showing that if $k = \bar{k}$ and R_i are domains that are finitely generated as k-algebras, then $R_1 \otimes_k R_2$ is also a domain.

This doesn't always happen, e.g. $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ is not a domain. Really need algebraically closed.

This is a result in affine algebraic geometry. An algebra that is a domain and finitely generated over a field is an *affine algebraic variety*, more precisely it is integral. The tensor product on the coordinate ring side corresponds to taking the product of varieties.

Thus the fact here is that a product of integral varieties remains integral, as long as you're over an algebraically closed field. Proof uses Hilbert's Nullstellensatz.

Exercise 3.1.5:

a. Show that $k(t)/k$ is regular.

I.e. $k(t) \otimes_k \bar{k}$ is a domain.

b. Show every purely transcendental extension is regular.

c. Show that for a field k, every extension is regular $\iff$ $k = \bar{k}$.

d. Show K/k is regular $\iff$ every finitely generated subextension is regular.

3.2 Example of a Non-Regular Family of Function Fields

Choose an elliptic curve $E/\mathbb{Q}(t)$ with j-invariant t. For $N \in \mathbb{Z}^+$, define $\tilde{K}_N \coloneqq \mathbb{Q}(t)(E[N])$ the N-torsion field of E.

Then $\tilde{K}_N/\mathbb{Q}(t)$ is a finite galois extension with galois group isomorphic to the image of the modular galois representation

$$\rho_N : g(\mathbb{Q}(t)) \to \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \mod N.$$

See Cornell-Silverman-Stevens covering the proof of FLT, modular curves from the function field perspective.

Proposition 3.2.1 ***(Some Facts).***
ρ_N is surjective, and

$$\mathrm{Aut}(\tilde{K}_N/\mathbb{Q}(t)) \cong \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}).$$

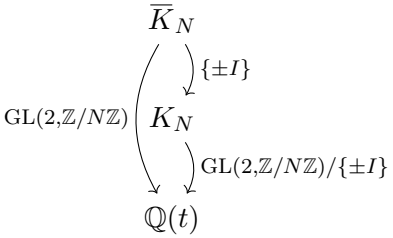
$\det \rho_N = \chi_N \mod N$, the cyclotomic character, and therefore χ_N restricted to $g(\tilde{K}_N)$ is trivial, so $\tilde{K}_N \supset \mathbb{Q}(\zeta_N)$. For $N \geq 3$, $\mathbb{Q}(\zeta_N) \supsetneq \mathbb{Q}$, so $\tilde{K}_N/\mathbb{Q}(t)$ is a non-regular function field.

Actually $\tilde{K}_N$ depends on the choice of E: difference choices of nonisomorphic curves with the same j-invariant differ by a quadratic twist and the ρ_N differ by a quadratic character on $g(\mathbb{Q}(t))$. Importantly, this changes the kernel, and thus the field.

To fix this, we look at the *reduced galois representation*, the following composition:

$$\bar{\rho}_N : g(\mathbb{Q}(t)) \to \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \twoheadrightarrow \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

We obtain a field theory diagram



So if you just take the field fixed by $\pm I$, you get K_N. In this case, the reduced galois representation depends only on the j-invariant, and not on the model chosen. So the function field $K_N/\mathbb{Q}(t)$ is the "canonical" choice.

Question: Does this make $K_N/\mathbb{Q}(t)$ regular?

Answer: No, $\rho_N(g(K_N)) = \{\pm I\}$ and $\det(\pm I) = 1$, so we still have $K_N \supset \mathbb{Q}(\zeta_N)$.

In this course, we'll identify algebraic curves over k and one-variable function fields K/k. The function field K_N corresponds to an algebraic curve $X(N)/\mathbb{Q}$ that is "nicer" over $\mathbb{Q}(\zeta_N)$. In fact, see Rohrlich: $\kappa(K_N) = \mathbb{Q}(\zeta_N)$.

Our curves will have points (equal to valuations) which will have degrees. If the constant subfield is not just k, this prevents degree 1 points on the curve.

By Galois theory, for every subgroup $H \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm I\}$, we'll get a function field $\mathbb{Q}(H) \coloneqq K_N^H$. In this case, $\mathbb{Q}(H)/\mathbb{Q}$ is regular $\iff \det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$.

Later we'll understand the residues at points as the residue fields of some DVRs, then the residue field will always contain the field of constants.

4 | Lecture 4

Last of preliminaries. Upcoming: one-variable function fields and their valuation rings.

4.1 Polynomials Defining Regular Function Fields

Where's the curve: $f(x,y)=0$.

Exercise 4.1.1: Let R_1, R_2 be k-algebras that are also domains with fraction fields K_i. Show $R_1 \otimes_k R_2$ is a domain $\iff$ $K_1 \otimes_k K_2$ is a domain.

Denominator-clearing argument.

Definition 4.1.1 (Geometrically Irreducible)
A polynomial of positive degree $f \in k[t_1, \cdots, t_n]$ is *geometrically irreducible* if $f \in \bar{k}[t_1, \cdots, t_n]$ is irreducible as a polynomial.

If $n=1$ then f is geometrically irreducible $\iff$ it's linear, i.e. of degree 1.

Let f be irreducible, then since polynomial rings are UFDs then $\langle f \rangle$ is a prime ideal (irreducibles generate principal ideals) and $k[t_1, \cdots, t_n]/\langle f \rangle$ is a domain. Let K_f be the fraction field.

Exercise 4.1.2: Easy:

a. Above for $1 \leq i \leq n$ let x_i be the image of t_i in K_f. Show that $K_f = k(x_1, \cdots, x_n)$.

b. Show that if K/k is generated by $x_1, \cdots, x_n$, then it is the fraction field of $k[t_1, \cdots, t_n]/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ (equivalently, a height 1 ideal).

Proposition 4.1.1*(?).*
Suppose that f is geometrically irreducible.

a. The function field K/k is regular.

b. For all ℓ/k, $f \in \ell[t_1, \cdots, t_n]$ is irreducible.

In this case we say f is *absolutely irreducible* as a synonym for geometrically irreducible.

Proof .
By definition of geometric irreducibility, $\bar{k}[t_1, \cdots, t_n]/\langle f \rangle = k[t_1, \cdots, t_n]/\langle f \rangle \otimes_k \bar{k}$ is a domain. The exercise shows that $K_f \otimes_k k$ is a domain, so K_f is regular.

It follows that for all ℓ/k, $K_f \otimes_k \ell$ is a domain, so $\ell[t_1, \cdots, t_n]/\langle f \rangle$ is a domain. ■

Moral: geometrically irreducible polynomials are good sources of regular function fields.

Exercise 4.1.3: Let k be a field, $d \in \mathbb{Z}^+$ such that $4 \nmid d$ and $p(x) \in k[x]$ be positive degree. Factor $p(x) = \prod_{i=1}^{r} (x - a_i)^{\ell_i}$ in $\bar{k}[x]$.

a. Suppose that for some i, $d \nmid \ell_i$. Show that $f(x, y) := y^d - p(x) \in k[x, y]$ is geometrically irreducible. Conclude that $K_f := ff\left(k[x, y]/\left\langle y^d - p(x) \right\rangle\right)$ is a regular one-variable function field over k, and thus elliptic curves yield regular function fields.

Referred to as *hyperelliptic* or *superelliptic* function fields. Hint: use FT 9.21 or Lang's Algebra.

b. What happens when $4 \mid d$?

Exercise 4.1.4(Nice, Recommended): Assume k is a field, if necessary assuming $\mathrm{ch}(k) \neq 2$.

a. Let $f(x, y) = x^2 - y^2 - 1$ and show K_f is is rational: $K_f = k(z)$.

b. Let $f(x, y) = x^2 + y^2 - 1$. Show that K_f is again rational.

c. Let $k = \mathbb{C}$ and $f(x, y) = x^2 + y^2 + 1$, K_f is rational.

d. Let $k = \mathbb{R}$. For $f(x, y) = x^2 + y^2 + 1$, is K_f rational?

Example of a non-rational genus zero function field.

Question (converse): Can we always construct regular function fields using geometrically irreducible polynomials?

Answer: In several variables, no, since not every variety is birational to a hypersurface.

In one variable, yes:

Theorem 4.1.1 ***(Regular Function Fields in One Variable are Geometrically Irreducible).***
Let K/k be a one variable function fields (finitely generated, transcendence degree one). Then

a. If K/k is separable, then $K = k(x, y)$ for some $x, y \in K$.

b. If K/k is regular (separable + constant subfield is k, so stronger) then $K \cong K_f$ for a geometrically irreducible $f \in k[x, y]$.

Proof .
Recall separable implies there exists a separating transcendence basis.
Proof of (a):
This means there exists a primitive element $x \in K$ such that $K/k(x)$ is finite and separable.
By the Primitive Element Corollary (FT 7.2), there exist a $y \in K$ such that $K = k(x, y)$.
Proof of (b):
Omitted for now, slightly technical.
■

Importance of last result: a regular function field on one variable corresponds to a nice geometrically irreducible polynomial f.

> Note: the plane curve module may not be smooth, and in fact usually is not possible. I.e. $k[x, y]/\langle f \rangle$ is a one-dimensional noetherian domain, which need not be integrally closed.

Question: Can every one variable function field be 2-generated?

Answer: Yes, as long as the ground field is perfect. In positive characteristic, the suspicion is no: there exists finite inseparable extensions ℓ/k that need arbitrarily many generators.

However, what if K/k has constant field k but is not separable? Riemann-Roch may have something to say about this.

Example 4.1.1: Example from earlier lecture:

$ax^p + b - y^b$

Moral: look for examples of nice function fields by taking irreducible polynomials in two variables. This will define a one-variable function field. If the polynomial is geometrical reducible, this produces regular function fields.

Next: One variable function fields and their valuations.

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

Remark 5.0.1: 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.

Lemma 5.1 ***(Key lemma about how places split.).***
Suppose $d \coloneqq \deg(v)$. 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 5.0.2: 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.

Lemma 5.2 ***(?).***
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 $\frac{q^d-1}{q-1}$ 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.

■

Remark 5.0.3: This is the sharpest result possible: the canonical divisor has degree $2g-2$ and is special, so this fails for the canonical class.

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.

5.1 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

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

which allows us to write

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

Where we're going: How does $Z(t)$ depend on K? 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 5.1.1 ***(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.

5.2 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

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

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:

$$\begin{aligned}
\cdots &= \sum_{\deg(C) \geq 0} \frac{q^{\ell(C)} - 1}{q - 1} t^{\deg(C)} \\
&= \left(\frac{1}{q-1}\right)\left(\sum_{0 \leq \deg(C) \leq 2g-2} q^{\ell(C)} t^{\deg(C)} + \sum_{\deg(C) > 2g-2} q^{\deg(C)-g+1} t^{\deg(C)} - \sum_{\deg(C) \geq 0} t^{\deg(C)}\right) \\
&:= F(t) + G(t),
\end{aligned}$$

so we can write

$$\begin{aligned}
F(t) &= \frac{1}{q-1} \sum_{0 \leq \deg(C) \leq 2g-2} q^{\ell(C)} t^{\deg(C)} \\
(q-1)G(t) &= \sum_{n=\frac{2g-2}{\delta}+1}^{\infty} h q^{n\delta+1-g} t^{n\delta} - \sum_{n=0}^{\infty} h t^{n\delta}.
\end{aligned}$$

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 5.2.1(?): 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 5.2.1 ***(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.

6 | Lecture 14

Recall the that *Hasse-Weil zeta function* of a one-variable function field $K/\mathbb{F}_q$ over a finite ground field is defined in the following way: let $A_n = A_n(K)$ be the number of effective divisors of degree n. We have proved that A_n is finite, and for $n > 2g - 2$ we have a formula

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

which is a formal power series with integer coefficients.

Remark 6.0.1: Recall that we have proved that it is a rational function of t, and in particular when $g = 0, \delta = 1$ [1] we get

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

We got another expression which isn't fantastic: it involves this δ, which we'll work toward proving is equal to 1. When $g > 1$, we broke the zeta function into two pieces $Z(t) = F(t) + G(t)$. For divisors of sufficiently high degree, Riemann-Roch tells you what the dimension of the Riemann-Roch space is, and $G(t)$ explains the part coming from divisors of large degree. We obtained a

[1] The *index* of the function field, least positive degree of a divisor.

formula previously for $F(t)$ and $G(t)$, and once we show $\delta = 1$ the formula for G will simplify. For $F(t)$, we specifically had

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

where the sum is over divisor classes and ℓ is the dimension of linear system corresponding to a divisor. But this isn't a great formula: what are these classes, dhow many are in each degree, and what is the dimension of the Riemann-Roch space?

Remark 6.0.2: This is analogous to the Dedekind zeta function of a number field K, in which case

$$\zeta_K(s) = \sum_{T \in \ell(\mathbb{Z}_k)}^{\bullet} |\mathbb{Z}_k / I|^{-s},$$

which will be covered in a separate lecture on *Serre zeta functions*.

Theorem 6.0.1 ***(F.K. Schmidt).***
For all $K/\mathbb{F}_q$, we have $\delta = I(K) = 1$ where I is the index.

This will follow from the associated, but it much weaker. However, this is one of the facts we'd like to establish to use to *prove* the Riemann hypothesis.

Remark 6.0.3: Pete studied this in 2004 and found that every $I \in \mathbb{Z}^+$ arises as the index of a genus one function field $K/\mathbb{Q}$.

Notation: for $n \in \mathbb{Z}^+$, let μ_n denote the nth roots of unity in $\mathbb{C}$.

Lemma 6.1 ***(?).***
For $m, r \in \mathbb{Z}^+$, set $d := \gcd(m, r)$. Then

$$\left(1 - t^{mr/d}\right)^d = \prod_{\xi \in \mu_r} 1 - (\xi t)^m.$$

Proof (?).
In $\mathbb{C}[x]$, we have

$$(X^{r/1} - 1)^d = \prod_{\xi \in \mu_r} (X - \xi^m),$$

where both sides are monic polynomials whose roots include the (r/d)th roots of unity, each with multiplicity d. On the LHS, the distinct roots are the r/dth roots of unity, then raising to the dth power gives them multiplicity d. On the RHS, this is an exercise in cyclic groups: consider the nth power map on $\mathbb{Z}/r\mathbb{Z}$ and compute its image and kernel. As ξ ranges over rth roots of unity, ξ^m ranges over all r/dth roots of unity, each occurring with multiplicity d. Substituting $X = t^{-m}$ and multiplying both sides by t^r yields the original result.

Special case: set $m = r$, so $d = r$, then the RHS is r copies of 1.

■

Next up, we want to compare the zeta function $Z(t)$ for a function field over $\mathbb{F}_q$ to the zeta function obtained when extending scalars to $\mathbb{Q}^r$.

Proposition 6.0.1 ***(Factorization identity for the zeta function).***
Let $K/\mathbb{F}_q$ be a function field, $r \in \mathbb{Z}^+$, and take the compositum K_r of K and $\mathbb{F}_q^r$ viewed as a function field over $\mathbb{F}_q^r$. Let $Z(t)$ be the zeta function of $K/\mathbb{F}_q$ and $Z_r(t)$ the zeta function of $K_r/\mathbb{F}_q^r$. Then

$$Z_r(t^r) = \prod_{\xi \in \mu_r} Z(\xi t).$$

Proof (?).
We have an Euler product formula

$$Z(t) = \prod_{p \in \Sigma(K/\mathbb{F}_q)} (1 - t^{\deg(p)})^{-1}.$$

where the sum is over places of the function field.

> Proving this Euler product formula might show up in a separate lecture, but it is not any more difficult than proving it for the Riemann zeta function.

Exercise 6.0.1(?): Why is this product expansion true? Write as a geometric series with ratio $t^{\deg(p)}$. Here just expand each summand to get

$$Z(t) = \prod_p \sum_{j=1}^{\infty} t^{j \deg(p)}.$$

Multiplying this out and collecting terms is in effect multiplying out the prime divisors to get effective divisors.
We now use the result about splitting that was stated (but not proved):

Claim: If $p \in \Sigma_m(K/\mathbb{F}_q)$ is a degree n place and $r \in \mathbb{Z}^+$, then there exist precisely $d \coloneqq \gcd(m, r)$places p^r of K_r lying over p. Moreover, each place p^r has degree m/d.

In order to compare $Z_r(t)$ to $Z(t)$, we collect the p' into ones that have the same fiber. We then can range over all p first, then over all p' in the fiber above p, yielding

$$Z_r(t^r) = \prod_{p \in \Sigma(K_{/\mathbb{F}_q})} \prod_{p'/p} \frac{1}{1 - t^{r \deg(p')}}.$$

Using the Euler product identity, we have for $p \in \Sigma_m(K_{/\mathbb{F}_q})$ and $d \coloneqq \gcd(m, r)$ we can express the innermost product as

$$\prod_{p'/p} \frac{1}{1 - t^{r \deg(p')}} = (1 - t^{rm/d})^{-d} = \prod_{\xi \in \mu_r} (1 - (\xi t)^m)^{-1},$$

where we've used the fact that we know there are exactly d places and each contributes the same degree in the first expression. By using $-d$ in the previous lemma, we get the last term. Combining all of this yields

$$Z_r(t^r) = \prod_{\xi \in \mu_r} \prod_{p \in \Sigma(K_{/\mathbb{F}_q})} (1 - (\xi t)^{\deg p})^{-1} = \prod_{\xi \in \mu_r} Z(\xi t).$$

■

Remark 6.0.4: Similar to taking an abelian extension of number fields and noting that the Dedekind zeta function factors into a finite product: the original zeta function, and in general, Hecke L functions. If you do this for an abelian number field over $\mathbb{Q}$, then the Dedekind zeta function of the upstairs number field will be a finite product where one of the terms in the Riemann zeta function and the others are Dirichlet L functions associated to certain Dirichlet characters. So this is some (perhaps simpler) version of that.

We can finally prove Schmidt's theorem that $\delta = 1$.

Proof ($\delta = 1$).
Take a δth root of unity $\xi \in \mu_\delta$. Then for all places $p \in \Sigma(K_{/\mathbb{F}_q})$, δ divides $\deg p$ by definition since it is a gcd, and so we have

$$Z(\xi t) = \prod_{p \in \Sigma(K_{/\mathbb{F}_q})} (q - (\xi t)^{\deg p})^{-1} = \prod_{p \in \Sigma_{K_{\mathbb{F}_q}}} \frac{1}{1 - t^{\deg p}} = Z(t),$$

using the fact that $\xi^{\deg p} = 1$.
We're now in a situation where we can apply the previous proposition, which gives the following identity for the zeta function over the degree δ extension:

$$Z_\delta(t^\delta) = \prod_{\xi \in \mu_\delta} Z(\xi t) = Z(t)^\delta.$$

Our previous formulas show that any zeta function for a 1-variable function field over a finite field has a simple pole at $t = 1$, and since $\mathrm{Ord}_{t-1}(t^\delta) = 0$, we get

$$-1 = \mathrm{Ord}_{t-1} Z_\delta(t^\delta) = \mathrm{Ord}_{t-1} Z(t)^\delta) = -\delta,$$

where for the first equality we're using the fact that the $(t-1)$-adic valuation of $Z_\delta(t^\delta)$ is one, and for the RHS, the ordinary zeta function has a simple pole at $t = 1$ and since we have a valuation, raising something to the δth power is just δ times the original valuation.

■

There is some modest representation theory (character theory) that shows up when looking at zeta functions of abelian extensions.

Remark 6.0.5: We can also conclude that every genus zero function field $K_{/\mathbb{F}_q}$ is isomorphic to $\mathbb{F}_q(t)$ and thus rational, since such a function field rational iff it has index one. Why? By Riemann-Roch, index one implies existence of a divisor of degree one, and taking a genus zero curve says that every divisor of nonnegative degree is linearly equivalent to an effective divisor. Thus if you have a divisor of degree one, you have an effective divisor of degree one, which makes the function field a degree one extension of a rational function field.

Exercise 6.0.2(?): Let $K = \mathbb{F}_q(t)$, then show that $g = 0, \delta = 1$, and

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

Hint: go back to complicated formulas and substitute $\delta = 1$ to simplify things.

Thus for rationality of the zeta function, we can get rid of the δ cluttering up formulas. Going back to the plan, we wanted to show

1.Rationality: $Z(t) \in \mathbb{Q}(t)$ and thus $Z(t) = P(t)/Q(t)$,

2. Understand the degrees of P and Q in terms of the genus, and

3. Ask about the roots of $P(t)$ to understand the analog of the Riemann Hypothesis for Dedekind zeta functions

We'll want to establish a functional equation, as is the usual yoga for zeta functions, since it helps establish a meromorphic continuation to $\mathbb{C}$.

The algebraic significance of the functional equation is that it aids in understand several equivalent packets of data:

- The number of effective divisors of a given degree,
- The number of places of a given degree,
- The number of rational points over each finite degree extension of the base field.

6.1 The Functional Equation

Theorem 6.1.1 ***(Functional Equation).***
Let $K_{/\mathbb{F}_q}$ be a function field of genus g, then

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

Proof (?).
For $g = 0$, we know that

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

and plugging in $\dfrac{1}{qt}$ is a straightforward calculation. So assume $g \geq 1$.
The idea was that we wrote $Z(t) = F(t) + G(t)$. The $F(t)$ piece came from summing over divisor classes of degree between 0 and $2g-2$ and recording the dimension of the associated linear system. The tricky piece $G(t)$ came from summing an infinite geometric series to get a more innocuous closed-form expression of a rational function. So the strategy here is to separately establish the functional equation for each of F and G separately. How to do this:

for $g = 0$, there was no $F(t)$ piece. If we have a closed form it's just a computational check. For $F(t)$, we'll use our greatest weapon and dearest ally, the Riemann-Roch theorem. This will provide the extra symmetry we need.
We essentially already applied Riemann-Roch to $G(t)$ to get the closed-form expression, but we haven't applied it to the small degree divisors. This doesn't tell you what the dimension is, but rather gives you a duality result: ti gives the dimension in terms of the dimension of a complementary divisor.
Take a canonical divisor $\mathcal{K} \in \mathrm{Div}(K)$, so $\deg \mathcal{K} = 2g - 2$. As C runs through all divisor classes of $\mathcal{K}$ of degree d with $0 \leq d \leq 2g - 2$, so does the complementary divisor $\mathcal{K} - C$.
We can thus write

$$(q-1)F(t) = \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} t^{\deg(C)}$$
$$(q-1)G(t) = h\left(\frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t}\right).$$

We can thus compute

$$\begin{aligned}(q-1)F\left(\frac{1}{qt}\right) &= \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} \left(\frac{1}{qt}\right)^{\deg C} \\ &= \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(\mathcal{K}-C)} \left(\frac{1}{qt}\right)^{2g-2-\deg C},\end{aligned}$$

where in the second step we've exchanged C for $\mathcal{K} - C$ and noted that $\deg(\mathcal{K} - C) = 2g - 2 - \deg(C)$. We now do the calculation another way,

$$\begin{aligned}(q-1)F(t) &= \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} t^{\deg C} \\ &= q^{g-1} t^{2g-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\deg(C)-(2g-2)+\ell(\mathcal{K}-C)} t^{\deg(C)-(2g-2)} \quad \text{by Riemann-Roch} \\ &= q^{g-1} t^{2g-2} \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(\mathcal{K}-C)} \left(\frac{1}{qt}\right)^{\deg(\mathcal{K}-C)} \\ &= q^{g-1} t^{2g-2} (q-1) F\left(\frac{1}{qt}\right).\end{aligned}$$

where we've used Riemann-Roch to find that $\ell(C) = \ell(\mathcal{K} - C) + \deg(C) - g + 1$. Cancelling the common factor of $(q - 1)$ establishes the functional equation for $F(T)$.
Now using the fact that $\delta = 1$, we have

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

and thus

$$\begin{aligned}(q-1)q^{g-1}t^{2g-2}G\left(\frac{1}{qt}\right) &= hq^{g-1}t^{2g-2}\left(q^g\left(\frac{1}{qt}\right)^{2g-1} - \frac{1}{1-q\left(\frac{1}{qt}\right)} - \frac{1}{1-\frac{1}{qt}}\right)\\ &= h\left(\frac{-1}{1-t} + \frac{q^g t^{2g-1}}{1-qt}\right)\\ &= (q-1)G(t),\end{aligned}$$

which establishes the functional equation for $G(t)$.

■

6.2 The L Polynomial

Definition 6.2.1 (The L Polynomial)

$$L(t) \coloneqq (1-t)(1-qt)Z(t) \in \mathbb{Z}[t].$$

This clears the denominators in $Z(t)$, so this is now a polynomial of degree at most $2g$. We can thus rewrite

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)} = \frac{a_{2g}t^{2g} + \cdots + a_1 t + a_0}{(1-t)(1-qt)}.$$

Note that if we know $L(t)$, then we know $Z(t)$, and in particular we would like to know what the coefficients a_j are. We'll be able to determine $a_0 = 1$ in all cases, as well as a_{2g} in all cases pretty easily. So it looks like it only remains to compute $a_1, \cdots, a_{2g-1}$, but the functional equation will give a "mirror" relation between pairs of coefficients. The upshot is that the functional equation shows that we only need to know $a_1, \cdots, a_g$ to completely determine $Z(t)$. If $g = 1$, just one coefficient suffices. It turns out that a_1 will be $q+1$ minus the number of degree one places.

Questions: what are the constraints on these quantities? Can we write the zeta function in a nice way? Exactly what do we need to compute to determine it?

It will turn out that computing the number of rational points over $\mathbb{F}_q, \mathbb{F}_{q^2}, \cdots, \mathbb{F}_{q^g}$ will be possible. For example, for a hyperelliptic curve, we'll have an explicit defining equation and can make an explicit point count, and you only need g of them.

7 | Indices

List of Todos

Definitions

Theorems

Exercises

List of Figures