


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

Last updated: 2020-11-27

Contents

1	Lecture 1	4
1.1	Field Theory	4
1.1.1	Notion 1	4
1.1.2	Notion 2	4
1.1.3	Notion 3	4
1.2	Case Study: The Luroth Problem.	6
1.3	Onto Business	7
1.4	Lecture 1, A Review	8
2	Lecture 1: Discussion	8
3	Lecture 2	10
3.1	Base Extension	10
3.2	Example of a Non-Regular Family of Function Fields	14
4	Lecture 3	16
4.1	Polynomials Defining Regular Function Fields	16
5	Lecture 4	18
5.1	One Variable Function Fields (Ch. 1)	18
5.1.1	Valuation Rings and Krull Valuations	19
6	Monday, November 23	26
7	Lecture 11A: Weil's Proof of Riemann-Roch	26
8	Lecture 11B: Weil's Proof of Riemann-Roch	31
9	Lecture 11C: Weil's Proof of Riemann-Roch	31
10	Lecture 12 (Chapter 3: Curves Over a Finite Field)	31
10.1	Base Extension	31
10.1.1	Splitting of Places	32
10.2	Degree 1 Places and Rational Points on a Curve	34
10.3	Finiteness of Places and Rational Points	35
10.4	Finiteness of Class Group	36
11	Lecture 13	37
11.1	Hasse-Weil Zeta Functions	39
11.2	Proof of Rationality	41
12	Lecture 14	43
12.1	The Functional Equation	47
12.2	The L Polynomial	49
13	Indices	49

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 $x_1, \dots, x_n \in \ell$ such that $\ell = k(x_1, \dots, x_n)$ and ℓ is the smallest field extension of k .

Concretely, every element of ℓ is a quotient of the form $\frac{p(x_1, \dots, x_n)}{q(x_1, \dots, x_n)}$ with $p, q \in k[x_1, \dots, x_n]$.

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, \dots, x_n , with coefficients in R , i.e. $S = R[x_1, \dots, x_n]$.

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 $k(t_1, \dots, t_n) := \text{frac}(k[t_1, \dots, t_n])$.

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 1.1.4:

- 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 1.1.5 (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 1.1.6 (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 1.1.7 (?).

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 1.1.8 (Transcendence Degree)

The *transcendence degree* of ℓ/k is the cardinality of any transcendence basis.

Analogy: dimension in linear algebra.

Theorem 1.1.9 (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 1.1.10 (Bounds on Transcendence Degree).

Let K/k be finitely degenerated, so $K = k(x_1, \dots, x_n)$. 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 $\text{trdeg}(F(x)/F) = 1$ [x/F 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 $k \hookrightarrow k(x_1) \hookrightarrow k(x_1, x_2) \hookrightarrow \dots \hookrightarrow k(x_1, \dots, x_n) = K$ to obtain a chain of length n . The transcendence degree is thus the number of indices i such that x_i is transcendental over $k(x_1, \dots, x_{i-1})$.

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

Definition 1.1.11 (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 be 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 $k \subset \ell \subset k(t_1, \dots, t_d)$ with $k(t_1, \dots, t_d)/\ell$ 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 1.2.5: 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 $k(t_1, \dots, t_n)$, thus so does G . Set $\ell := k(t_1, \dots, t_n)^G$ 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 $\text{Aut}(k(t_1, \dots, t_n)/\ell) = G.A$

- 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. ℓ/\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

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

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 1: Discussion

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 $\mathbb{Z}_{(p)} := \mathbb{Z}[\{\frac{1}{\ell} \mid \ell \neq p\}]$ for all primes p .

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

Exercise 2.0.2: Show that a valuation ring is a local ring, i.e. it has a unique maximal ideal.

Example 2.0.3: Where does the log come from?

There is a p -adic valuation:

$$v : \mathbb{Q} \rightarrow \mathbb{Z}_{(p)}$$

$$\frac{a}{b} = p^n \frac{u}{v} \mapsto n.$$

Then we recover

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q}^\times \mid v_p(x) \geq 0\} \cup \{0\}$$

$$\mathfrak{m}_{(p)} = \{x \in \mathbb{Q}^\times \mid v_p(x) > 0\} \cup \{0\}$$

There is a p -adic norm

$$|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}$$

$$0 \mapsto 0$$

$$x \mapsto p^{-n} = p^{-v_p(x)}.$$

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

$$d_p : \mathbb{Q}^2 \rightarrow \mathbb{R}$$

$$(x, y) \mapsto |x - y|_p.$$

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 $\tilde{\Sigma} = \{\text{Valuation rings } R_v \text{ of } K\} \mid A \subset R_v \subsetneq K$. 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*

$$\Sigma(K/k) := \left\{ \text{Nontrivial valuations } v \in K \mid v(x) \geq 0 \forall x \in k^\times \right\},$$

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 2.0.4 (?)

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

$$\deg : \text{Div}(K) \rightarrow \mathbb{Z}$$

which need not be surjective.

We can consider principle divisors with the map

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

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

3 | Lecture 2

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 $p_i \in k[t_1, \dots, t_n]$, and base extension comes from the map $k[t_1, \dots, t_n] \hookrightarrow \ell[t_1, \dots, t_n]$.

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

In general we have a map

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

Note that this will be an exact functor on the category $k\text{-Vect}$, i.e. ℓ is a flat module. Here everything is free, and $\text{free} \implies \text{flat}$, 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 3.1.2: If ℓ/k is algebraic and $\ell \otimes_k \ell$ is a domain, then $\ell = k$.

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 3.1.3: 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 3.1.4: For ℓ/k a field extension,

- Show $k(t) \otimes_k \ell$ is a domain with fraction field $\ell(t)$.
- Show it is a field $\iff \ell/k$ is algebraic.

Proposition 3.1.5 (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 3.1.6: 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 3.1.7.

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

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

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 3.1.8: 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 $k^{\frac{1}{p}} := k(\{x^{\frac{1}{p}} \mid x \in k\})$ is obtained by adjoining all p th 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 $k^{\frac{1}{p}} \rightarrow k$, 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 won't 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 3.1.9 :** This is pretty technical, yo. 

Example 3.1.10: Set $k = \mathbb{F}_p(a, b)$ a rational function field in two variables as the ground field. Set

$$A := k[x, y] / \langle ax^p + b - y^b \rangle.$$

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

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 $\alpha^p = a, \beta^p = b$, so

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

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 p th 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 3.1.11: 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 3.1.12 (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 3.1.13: 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 3.1.14:

- 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 $\tilde{K}_N := \mathbb{Q}(t)(E[N])$ 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

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

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

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

$\det \rho_N = \chi_N \bmod N$, 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:

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

We obtain a field theory diagram

$$\begin{array}{c} \bar{K}_N \\ \downarrow \scriptstyle \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \quad \searrow \scriptstyle \{\pm I\} \\ K_N \\ \downarrow \scriptstyle \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) / \{\pm I\} \\ \mathbb{Q}(t) \end{array}$$

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 $\mathbb{Q}(H) := H_N^H$. 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 3

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.¹

Definition 4.1.2 (Geometrically Irreducible)

A polynomial of positive degree $f \in k[t_1, \dots, t_n]$ is **geometrically irreducible** if $f \in \bar{k}[t_1, \dots, t_n]$ 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 $k[t_1, \dots, t_n]/\langle f \rangle$ is a domain. Let K_f be the fraction field.

Exercise 4.1.3 (an easy one):

- Above for $1 \leq i \leq n$ let x_i be the image of t_i in K_f . Show that $K_f = k(x_1, \dots, x_n)$.
- Show that if K/k is generated by x_1, \dots, x_n , then it is the fraction field of $k[t_1, \dots, t_n]/\mathfrak{p}$ for some prime ideal \mathfrak{p} (equivalently, a height 1 ideal).

Proposition 4.1.4 (?).

Suppose that f is geometrically irreducible.

- The function field K/k is regular.
- For all ℓ/k , $f \in \ell[t_1, \dots, t_n]$ is irreducible.

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

Proof.

By definition of geometric irreducibility, $\bar{k}[t_1, \dots, t_n]/\langle f \rangle = k[t_1, \dots, t_n]/\langle f \rangle \otimes_k \bar{k}$ 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 $\ell[t_1, \dots, t_n]/\langle f \rangle$ is a domain. ■

¹Hint: use a denominator clearing argument.

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

Exercise 4.1.5: 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 $K_f := k[x, y] / \langle y^d - p(x) \rangle$ is a regular one-variable function field over k , and thus elliptic curves yield regular function fields.²

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

Exercise 4.1.6 (Nice, Recommended): Assume k is a field, if necessary assuming $\text{ch}(k) \neq 2$.

a. Let $f(x, y) = x^2 - y^2 - 1$ and show K_f 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?³

Question 4.1.7: Can we always construct regular function fields using geometrically irreducible polynomials?

Answer 4.1.8: In several variables, no, since not every variety is birational to a hypersurface. In one variable, yes, as the following theorem shows:

Theorem 4.1.9 (Regular Function Fields in One Variable are Geometrically Irreducible).

Let K/k be a one variable function field (finitely generated, transcendence degree one). Then

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

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 $K = k(x, y)$. ■

²Referred to as *hyperelliptic* or *superelliptic* function fields. Hint: use FT 9.21 or Lang's Algebra.

³This is an example of a non-rational genus zero function field.

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 .

Remark 4.1.10: 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 4.1.11: Can every one variable function field be 2-generated?

Answer 4.1.12: 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 4.1.13: Example from earlier lecture:

$$ax^p + b - y^b$$

Remark 4.1.14: We can find 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 4

5.1 One Variable Function Fields (Ch. 1)

Since we have the field-theoretic preliminaries out of the way, we now start studying one-variable function fields in earnest. The main technique that we use to extract the geometry will be the theory of valuations. These may be familiar from NTII, but we will cover them in more generality here.

5.1.1 Valuation Rings and Krull Valuations

Recall that NTII approach to valuations:

Definition 5.1.1 (Valuation)


A **valuation** on a field K is a map $v : K \rightarrow \mathbb{R} \cup \{\infty\}$ such that $v(K^\times) \subset \mathbb{R}$, $v(0) = \infty$, and v is of the form $-\log(|\cdot|)$ where $|\cdot| : K \rightarrow [0, \infty)$ is an *ultrametric norm*.^a Recall that an *ultrametric norm* satisfies not only the triangle inequality but the ultrametric triangle inequality, i.e. $d(x, z) \leq \max(x, z)$.

^aIn other words, $e^{-v(\cdot)}$ is an ultrametric norm.

We now take an algebraic approach to this definition, where we'll end up replacing \mathbb{R} with something more general.

Definition 5.1.2 (Valuation Ring)

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

Remark 5.1.3: This is a “largeness” property. It also implies that $K = \text{ff}(R)$. 

Definition 5.1.4 (Group of Divisibility)


Given any integral domain R with fraction field K , the **group of divisibility** $G(R)$ is defined as the *partially ordered commutative group*^a

$$G(R) := K^\times / R^\times.$$

We will write the group law here additively. The ordering is given by $x \leq y \iff y/x \in R$.

^aThis means that the two structures are compatible.

Remark 5.1.5: Note that the way the partial order is written, it's a relation on K^\times , but it is not quite a partial ordering there. It is reflexive and transitive, but need not be antireflexive: if $x/y, y/x \in R$ then x, y differ by an element of $u \in R^\times$ so that $x = uy$. In particular, they need not be equal. This gives a structure of a *quasiordering*, and if you set $x \sim y \iff x \leq y$ and $y \leq x$, this leads to an equivalence relation, and modding out by it yields a partial order. Here this is accomplished by essentially trivializing units.

Another way to think of $G(R)$ is as the nonzero principal fractional ideals of K , since any two generators of an ideal will differ by a unit. 

Remark 5.1.6: Inside this group there is a *positive cone* $G(R)^+$ of elements that are “nonnegative”: since we're in a commutative setting, the zero element is equal to 1, and the positive cone is given by $\{y \geq 0\} = \{y \in R\}$, and is thus given by the group $G(R)^+ = (R, \cdot)$.

This is very general: if you're studying factorization in integral domains, many properties are reflected in $G(R)$. E.g. being a UFD (the most important factorization property!) implies that $G(R)$ is a free commutative group.

Remark 5.1.7: In general this is only a *partially* ordered group and not totally ordered. For example, take $R = \mathbb{Z}$ and $x = 2, y = 3$, then neither of $2/3, 3/2$ are in \mathbb{Z} , so $x \not\leq y$ and $y \not\leq x$. On the other hand, if we do have a total order, then either x or x^{-1} is in the ring, which are exactly valuation subring of a field.

Claim: R is a valuation ring $\iff G(R)$ is totally ordered.

Remark 5.1.8: Note that \mathbb{R} is a totally ordered group.

This makes $G(R)$ the “target group” of a generalized analytic valuation. Whenever we have a valuation ring, we have a totally ordered commutative group, and the valuation $v : K^\times \rightarrow G(R)$ is a quotient map which we can extend to K by $v(0) := \infty$. This has some familiar properties:

- (VRK1) For all $x, y \in K^\times$,⁴

$$v(xy) = v(x) + v(y).$$

- (VRK2) For all $x, y \in K^\times$ such that $x + y \neq 0$,

$$v(x + y) \geq \min(v(x), v(y)).$$

For ultrametric norms, all triangles are isosceles: is that true for this type of function? The answer is yes, by the following exercise:

Exercise 5.1.9(?): If $v(x) \neq v(y)$, then $v(x + y) = \min(v(x), v(y))$.

So the properties here are formally identical to the NTII notion of valuation, with $(\mathbb{R}, +, \leq)$ replaced by $(G(R), +, \leq)$.

Exercise 5.1.10(?): Conversely, if $v : K^\times \rightarrow G$ is a map into a totally ordered commutative group satisfying VRK1 and VRK2⁵, then

$$R_v := \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$$

is a valuation ring.⁶ We can thus extract valuation rings in this situation.

Exercise 5.1.11(?): A valuation ring is **local**, i.e. there is a unique maximal ideal

$$\mathfrak{m}_v := \{x \in K^\times \mid v(x) > 0\} \cup \{0\}.$$

⁴This follows from the fact that the quotient map is a group morphism. Note that the additive notation makes this more suggestive of what an original valuation satisfied.

⁵Any such map satisfying these two properties is a **Krull valuation**, Krull's generalization of classical valuations.

⁶Note that in a totally ordered group, either $v(x) \geq 0$ or $-v(x) \geq 0$, so we get the property that either $x, x^{-1} \in R_v$.

Remark 5.1.12: These two constructions are morally mutually inverse. This doesn't hold on the nose, since there is extraneous data in the new analytic valuation. Recall that in NTII we have a notion of equivalence of norms, and two distinct norms that are equivalent can give rise to the same valuation. For example, given a valuation, one can scale it by $\alpha \in \mathbb{R}$, and it's easy to check that this gives the same valuation. It is possible for the valuation not to surject onto \mathbb{R} , but this doesn't happen in practice. The image is usually infinite cyclic, what we call a *discrete valuation*, and so one is led to the definition of the *value group* of the valuation as its image. If you have a notion of equivalence of Krull valuations, you want to allow for isomorphisms of the value group. The cleanest notion of equivalence is thus the following:

Definition 5.1.13 (Equivalence of Krull valuations)

Two Krull valuations on a field K are **equivalent** iff their valuation rings are *equal*.

Remark 5.1.14: Going back to NTII, if you have two nonarchimedean norms on a field, then there are many equivalent conditions for equivalence, and this is one of them.

Some general valuation theory:

- Every totally ordered commutative group is a group of divisibility.⁷
- A totally ordered group has **rank 1** if it is nontrivial and embeds into \mathbb{R}
 - If the value group is trivial, $R = K$
- A Krull valuation of rank at most 1 is the NTII notion of a valuation.

Exercise 5.1.15(?): For $n \geq 2$, put the lexicographic order on \mathbb{Z}^n , and show this has rank strictly larger than 1. Thus $\mathbb{Z}^n \hookrightarrow \mathbb{R}$ as a commutative group, but not as a totally ordered commutative group.

Remark 5.1.16: In fact, for any ordered group G , one can attach a rank: a cardinal number $r(G)$. Here, $r((\mathbb{Z}^n, \text{lex})) = n$. This is useful when studying $\text{Spec}(R)$ for R a DVR.

A valuation of rank bigger than 1 does not induce a norm on K in the metric sense, although this is not so important. A closer notion is expanding the notion of a metric space by allowing the metric to be defined on X as $d : X \times X \rightarrow R$ for some R more general than \mathbb{R} , like a totally ordered group or a nonarchimedean field. This would yield a class of topological spaces that are reminiscent of metric spaces.

Definition 5.1.17 (Important: Regular and Centered)

Let $v : K^\times \rightarrow (G, +)$ be a Krull valuation and let $A \subset K$ be a subring of K . Then v is **A -regular** or **centered in A** if A is a subset of some valuation ring R_v . In this case, $\mathfrak{p} := \mathfrak{m}_v \cap A \in \text{Spec}(A)$ is denoted the **center of v in A** .^a

^aHere \mathfrak{m}_v denotes pulling back the maximal ideal along this morphism of rings.

⁷Pete's Commutative Algebra Notes, Ch. 17.10

Remark 5.1.18: The term regularity here arises because we'll want to think of elements of A as functions and the valuation as a type of point, then the notion of being a regular function at a point will carry over. The center is the subset of A with strictly positive valuation. Also recall that pulling back prime ideals yields prime ideals, and maximal ideals are a special kind of prime ideal, but in general pulling back a maximal ideal may not result in another maximal ideal. So somehow the valuation affects every subring on which it is regular.

Definition 5.1.19 (Key: Zariski-Riemann Space)

For $A \subset K$, define

$$\Sigma(K/A) := \left\{ \text{valuation rings } A \subset R \subsetneq K \mid K = \text{ff}(R) \right\}$$

$$\tilde{\Sigma}(K/A) := \left\{ \text{valuation rings } A \subset R \subseteq K \mid K = \text{ff}(R) \right\}.$$

The set $\tilde{\Sigma}(K/A)$ is the **Zariski-Riemann space**.

Remark 5.1.20: Note that in this definition, we're taking all A -regular valuation rings R in K . If someone says R is a valuation ring of K , they likely mean that $K = \text{ff}(R)$. Note that fields are valuation rings, so otherwise, any subfield of K would also be a valuation ring of K . Here, K itself plays the role of a generic point. (?) The only difference in these two definitions is that in the first, the trivial valuation ring is being excluded.

Definition 5.1.21 (Key: Places, Points of a Curve)

If K/k is a one variable function field^a, then $\Sigma(K/k)$ will be the **points of the associated algebraic curve** or **places**. These can be thought of as valuation rings, or equivalence classes of Krull valuations, where two valuations are equivalent if they have the same valuation ring.

^aFinitely generated field extension of transcendence degree one.

Remark 5.1.22: In terms of scheme theory, these will be the closed points of our algebraic curve. We will view elements $f \in K$ as meromorphic functions on $\Sigma(K/k)$.

Definition 5.1.23 (Zariski Topology)

The **Zariski topology** on $\Sigma(K/A)$ has a sub-base

$$\left\{ U(f) \mid f \in K \right\} \quad U(f) := \left\{ v \in \tilde{\Sigma}(K/A) \mid v(f) \geq 0 \right\} = \tilde{\Sigma}(K/A[f]).$$

and we thus take the minimal topology such that all of these sets are open. In other words, every open set is a finite intersection and/or arbitrary unions, including empty intersections/unions. The last term is precisely the subring generated by A and f . Thus a base is $U(f_1, \dots, f_n) = \tilde{\Sigma}(K/A[f_1, \dots, f_n])$. The Zariski topology on $\Sigma(K/A)$ is defined the same way and/or via the subspace topology, since this removes a single point.

Remark 5.1.24: We thus get the subrings of K that contain A and are finitely generated as A -algebras. We'll be specifically looking at the case where A is a field and K is a one variable function field.


Theorem 5.1.25 (Zariski). $\tilde{\Sigma}(K/A)$ is quasi-compact.*Proof* (?).See Mazamara (?) in the chapter discussing valuation rings. ■

Note that by definition, $v_n \notin \Sigma(K/A)$. In $\tilde{\Sigma}(K/A)$, we have a trivial valuation v_n whose value group is trivial and valuation ring is K itself, and v_n is a generic point of $\Sigma(K/A)$: its closure is the entire space. In other words, it is in every nonempty open subset. Since we have at least one generic point, and in general there may be many, if $|\tilde{\Sigma}(K/A)| > 1$ then this is not a separated (T_1) space since the point is not closed.⁸ Another example of such a space would be $\text{Spec}(R)$ for R a commutative ring with positive Krull dimension, which will be Kolmogorov (T_0) but not separated. Such a spectrum is the underlying topological space of some affine scheme, and in general, schemes will have these kinds of properties that are bad (but not *too* bad).

In our case of interest, when K/k is finitely generated of transcendence degree one, we'll see that this is the cofinite topology on an infinite space: the proper closed subsets are precisely the finite subsets, or equivalently every nonempty open subset has finite complement. This is far from Hausdorff: the intersection of two open subsets will still have finite complement, so any two nonempty open subsets must intersect.

It's not generally true that just removing the generic point v_n will make the space separated, but in our case, it will be. So if we restrict to nontrivial valuation rings, then the underlying set will be infinite and we'll get the cofinite topology. This will be the coarsest separated topology, i.e. if you want singletons to be closed, finite subsets must be closed. If $k \subset A \subset K$ where A is a Dedekind domain with fraction field K , we will see that if we consider not the k -regular elements but the A -regular ones, we'll get $\Sigma(K/A) = \text{maxSpec}(A)$ and both Zariski topologies are cofinite. Note that in a Dedekind domain, trading in a prime spectrum for a max spectrum is removing a generic point, so this matches up. The moral: the topology of $\Sigma(K/k)$ is not doing anything interesting and we won't need it much.

When K/k instead has transcendence degree *bigger* than 1, then $\tilde{\Sigma}(K/k)$ is much more interesting. If we were doing things scheme-theoretically, we could try to define a structure sheaf: attaching a sheaf whose stalks are local commutative rings to make it a locally ringed space.⁹ Here, the choice of a ring is straightforward: literally $\tilde{\Sigma}(A, A[f_1, \dots, f_n])$. There's an exercise that shows that although defining a sheaf on the entire space is somewhat annoying, defining it on a basis suffices.

Exercise 5.1.26 (?): Endow $\tilde{\Sigma}(K/k)$ with the structure of a locally ringed space. 

Remark 5.1.27: In dimension 1 (the case we're studying), the corresponding Zariski-Riemann space will be the scheme associated to the complete nonsingular model of the curve. So this

⁸Note that in French, separated may be interpreted as Hausdorff, but here we mean points are closed or equivalently any two distinct points admit open neighborhoods that do not meet the other point.

⁹Schemes are a full subcategory of the much larger category of locally ringed spaces.

valuation-theoretic approach will take you from the function field back to a nice model of the scheme itself. But note that in larger dimensions, there is no unique complete nonsingular model – for example, you can blow any one up to get another – so this pattern can't possibly continue to hold. In fact, it's not clear if we even know if there's *one* such model!

Remark 5.1.28: Thus in dimension > 1 , you get something that is decidedly not a scheme, but is still relevant to the study of resolution of singularities for your function field. Where do these come up? Zariski used $\Sigma(K/A)$ to prove resolution of singularities¹⁰ in characteristic zero and dimensions 2 and 3 in 1944, although dimension 2 was classical by the Italian school. Later, Hironaka (1984) got the Fields medal for proving resolution of singularities for all dimensions in characteristic zero using an ingenious inductive argument that avoided Zariski-Riemann spaces entirely. It remarkably doesn't use any new objects/tools, just uses existing ones in a clever way. So why talk about Zariski-Riemann spaces at all? In the last 10 years or so, work of Ternkin and Conrad has revived and generalized them. They study *relative* such spaces.

Problem. (Open)

In positive characteristic, resolution of singularities is only known up to dimension ≤ 3 .

The following is an extremely important result from commutative algebra:

Theorem 5.1.29 (CA 17.17).

Let $A \subset K$ be a subring of a field, then

$$\bigcap_{v \in \tilde{\Sigma}(K/A)} R_v,$$

the intersection of all valuation subrings of the field, is the integral closure of A in K .

The proof is mostly a Zorn's lemma type of argument. Note that each R_v is generally big, contains A , and $\text{ff}(R_v) = K$. Moreover, each valuation ring is integrally closed, although we haven't proved this yet.

Corollary 5.1.30 (?).

For K/k function field, $\bigcap_{v \in \Sigma(K/k)} R_v = \kappa(K)$, the constant subfield of K .

Proof (?).

Note that $\kappa(K)$ is the integral (algebraic) closure of k in K . Applying the theorem directly almost works, except the theorem involves $\tilde{\Sigma}$. Can we remove the tilde? Suppose not, this can only happen if $\Sigma(K/k) = \emptyset$ and the intersection is just K itself, the largest thing in the intersection. But can the integral closure of k in K be K itself? No, since the transcendence degree of the function field is positive. So K/k is transcendental, while $\kappa(K)/k$ is an algebraic extension, a contradiction. ■

¹⁰Resolving means given K/k , we want to find a complete nonsingular affine variety whose function field is K .

Remark 5.1.31: Note that $\Sigma(K/k)$ is nonempty: there is a nontrivial valuation ring between k and K in great generality, and there are often many.

Claim Key: If $\text{trdeg}(K/k) = 1$, then every $v \in \Sigma(K/k)$ is discrete and thus has value group isomorphic to \mathbb{Z} .

So despite the fact that we've introduced a more general notion of higher rank valuations, in dimension 1, every single valuation is discrete.

Proof (?).

Let $v \in \Sigma(K/k)$ be a place, so its a valuation ring with fraction field K that is not K , then R_v is not a field. So its maximal ideal \mathfrak{m}_v is nonzero, so choose a nonzero element $t \in \mathfrak{m}_v$. Then $t \in R_v$ and R_v contains k , so $k[t] \subset R_v$. Note that $k[t]$ is a PID sitting inside a valuation ring. So restrict this maximal ideal down: $\mathfrak{m}_v \cap k[t]$ is a prime ideal of $k[t]$ containing t , and thus the center $\mathfrak{m}_v \cap k[t] = \langle t \rangle$. This follows because a prime ideal in the polynomial ring $k[t]$ which contains t is necessarily generated by t , since there's exactly one such ideal.

Now restricting the valuation on K to $k(t) \subset K$, $K/k(t)$ will be a finite extension (from the first lecture). We know $k(t) \subset K$, and we can now check that $v|_{k(t)}$ is the t -adic valuation v_t . Note that \mathfrak{m}_v can not contain any other monic irreducible polynomials, since distinct such polynomials are coprime. Since we're in a PID, this ideal would contain any linear combination of them and thus contain 1. So consider the map

$$k[t] \hookrightarrow R_v \rightarrow G(R_v) = K^\times / R_v^\times.$$

Note that the units of $k[t]$ map trivially, using the fact that any element in $k[t]$ can be written as $u \prod p_i^{a_i}$ with the p_i monic irreducible polynomials. The unit maps to zero, along with all of the other monic irreducibles, and thus the image is determined entirely by the image of powers of t . This whole term goes to zero unless some $p_i \mapsto t$, in which case it maps to some power of t .

So suppose $t \mapsto \gamma \neq 0 \in G(R)$, which is nonzero because t was not a unit (since it was in the maximal ideal). Then the image is exactly $\gamma^{\mathbb{N}}$, the non-negative integer powers of the image of t . But if we know goes on this domain, taking denominators shows where it goes on the fraction field (of a UFD), so the image is the cyclic group generated by γ , i.e. the powers of t are literally the only valuations we get. So the image of $k(t)^\times$ in $G(R_v)$ is $\gamma^{\mathbb{Z}}$, yielding a discrete valuation. This proves that the restriction to the rational function field $k(t)$ is discrete, and we want to use this to deduce that the original valuation is discrete.

We can now use NTII:^a since $K/k(t)$ is finite, it follows that v is discrete iff $v|_{k(t)}$ is discrete, and thus v is discrete. ■

^aSee NTII, Corollary 1.60: a valuation on a field whose restriction to a finite index subfield is discrete is itself discrete.

So every place of K/k is a discrete valuation as long as the transcendence degree is one, but this is far from the case for degree ≥ 2 ! In the following example, we'll have a rational function field, which

makes things easier. You need a theory of extending Krull valuations, since we'll define a non-rank 1 valuation on the rational function field. But an arbitrary finitely generated field extension of degree d over k is a finite degree extension of the rational function field, and valuation theory will tell you that every valuation downstairs can be extended in full generality to a finite degree field extension, and the rank will not change.

Exercise 5.1.32(?): If K/k is finitely generated of $\text{trdeg} \geq 2$, then $\Sigma(K/k)$ has valuations of rank d .

Note that the Zariski-Riemann space only consists of discrete valuations, which is a characteristic property of one variable function fields. So these higher rank valuations may look weird, but when studying a function field of higher transcendence degree (e.g. for an algebraic surface), these occur.

Exercise 5.1.33 (Constructing valuations of arbitrary rank and value group): Let k be a field and $K = k(t_1, \dots, t_n)$. Set $G = \mathbb{Z}^n$ with the lex order, so $G^{\geq 0} = \mathbb{N}^n$.

- Show that $k[t_1, \dots, t_n] = k[G^{\geq 0}]$, where the RHS is the associated semigroup ring.
- Define $v : k[G^{\geq 0}]^\bullet \rightarrow G^{\geq 0}$ by mapping each polynomial the minimal index of a monomial in its support. For example,

$$v(a_1 t_1^3 t_2 + a_2 t_1^2 t_2^{10}) = (2, 10),$$

which has support $(3, 1)$ and $(2, 10)$, and we take the min in the lex order.

- Extend v to $v : K^\bullet \rightarrow G$ satisfying VRK1 and VRK2. Show that $R_v := v^{-1}(G^{\geq 0}) \cup \{0\}$ is a valuation ring with value group G , and in particular, the rank is n .

Note that doing this for $n = 1$ reduces to the t -adic valuation, which just keeps track of the smallest power of t appearing. Here you can extend to fraction fields by defining $v(x/y) = v(x) - v(y)$. The semigroup ring can't be the valuation ring, since polynomial rings are not local rings, so it's much bigger. Note also that \mathbb{Z} can be replaced with any group G , since it's never used in anything but a psychological fashion.

Slogan 5.1.34: There is a huge difference between $\text{trdeg} = 1$ and $\text{trdeg} > 1$, and so we'll only be working with the former case in this course.

6 | Monday, November 23

7 | Lecture 11A: Weil's Proof of Riemann-Roch

Let K/k be a one variable function field, finitely generated of transcendence degree one, with $\kappa(K) = k$, so k is algebraically closed in K . Define the *small Adele ring* associated to K , as the

restricted direct product with respect to $\{R_v \mid v \in \Sigma(K/k)\}$:

$$A_k := \prod_{v \in \Sigma(K/k)}^{\text{res}} K = \left\{ (x_v) \in K^{\Sigma(K/k)} \mid x_v \in R_v \text{ for a.e. } v \right\},$$

where each factor is a copy of K . Note that a *restricted* direct product is when you have a family of sets, and for each set you also attach a subset. Then if you have a tuple in the entire direct product, it's in the restricted direct product iff for all but finitely many coordinates lie in a given subset. Here the subset is the valuation ring R_v . So these are tuples of elements of K , indexed by places, where each element has a p -adic valuation and the only restriction is that (except for finitely many cases) we want this valuation to be nonnegative.

Remark 7.0.1: To get the *big* Adele ring, you'd replace K with its completion with respect to the p -adic valuation. If k is finite, then this is equal to the positive characteristic Adele ring from NTII. If you complete, then you get a complete discretely valued field whose residue field equals the residue field at the place v . So for finite extensions of k , the residue will be finite iff k is finite, and from the structure theory of discretely valued fields, this field has a natural topology: the adic topology, coming from the inverse limit. This will be locally compact iff the residue field is finite. Here, since the ground field is infinite, even passing to the completion wouldn't yield anything locally compact. So there's no advantage to passing to the completion, although there's no harm either.

Note that A_k is a ring, and in fact a K -algebra, but we will only need its structure as a K -vector space. This structure comes from embedding $K \hookrightarrow A_k$ diagonally, so $x \mapsto [x, x, \dots]$, and pull back $v \in \Sigma(K/k)$, remembering that every element of K (a rational function) is regular except for finitely many v .

If we have a valuation on K , we can consider a place p and projecting onto the k th factor:

$$A_j \xrightarrow{\pi_p} K \xrightarrow{v_p} \mathbb{Z} \cup \{\infty\}.$$

So we now attach an adelic version of the Riemann-Roch space: for $D \in \text{Div } K$, we set

$$\mathcal{A}_k(D) := \left\{ \alpha \in \mathcal{A}_K \mid v_p(\alpha) \geq -v_p(D) \forall p \in \Sigma(K/k) \right\}.$$

The only difference here is that the usual space is over K , and here we're over \mathcal{A}_K , which is a much larger space. This makes things easier, however, in the same sense that studying a large collection of local fields is easier than studying the corresponding global field. Note that the p -adic valuation v_p is just the coefficient of p in the divisor, and $\mathcal{A}_K \cap K$ yields the usual Riemann-Roch space.

Exercise 7.0.2(?):

- Show that $\mathcal{A}_K(D)$ is an k -subspace of \mathcal{A}_K .¹¹
- Show that (just as for the Riemann-Roch space) $D_1 \leq D_2 \implies \mathcal{A}_K(D_1) \subseteq \mathcal{A}_K(D_2)$.

¹¹Consider scaling by nonzero constants, where the valuation of constants are zero.

Lemma 7.0.3(?).

$$D_1 \leq D_2 \implies \dim_k \mathcal{A}_K(D_2)/\mathcal{A}_K(D_1) = \deg D_2 - \deg D_1.$$

Note that this is the adelic analogue of our first lemma on Riemann-Roch spaces, now with an equality instead of being bounded above.

Proof (?).

As we did before, by induction we can assume $D_2 = D_1 + p$ for some $p \in \Sigma(K/k)$, i.e. we can go from the smaller divisor to the bigger one by repeatedly adding closed points. Then choose an element $t \in k^\times$ such that $v_p(t) = v_p(D_2)$, and define a similar map

$$\begin{aligned} \varphi \mathcal{A}_K(D_2) &\rightarrow k_p \\ \alpha &\mapsto (t\alpha p) \pmod{\mathfrak{m}_p}. \end{aligned}$$

Why? Once you multiply by t , note that we're looking in the p th component. The condition before was that the valuation at the p th component was at least $-v_p(D_2)$, but now we're adding $v_p(D_2)$. This yields a nonnegative valuation, making the image lie inside the corresponding local ring, so it makes sense to consider it modulo the maximal ideal to get an element of the residue field. As before, it should be clear that this is k -linear, $\ker \varphi = \mathcal{A}_K(D_1)$, and is surjective. The kernel are exactly those elements such that multiplying by t makes the p -adic valuation at least 1, since that's what the maximal ideal is. This is indeed $\mathcal{A}_K(D_1)$, since D_1 and D_2 are the same except for the added condition $D_2 = D_1 + p$ at p .


So the main difference is that the map is now *surjective*, which was not true for the original Riemann-Roch space. Why? This is a purely local situation. Take an element which is zero away from the p component, which is easy to do since zero is in R_v for any v . So can you find an element of k such that multiplying by t and reducing modulo the maximal ideal yields every element of the residue field? ■

Theorem 7.0.4(2.13).

For all D ,

$$\dim_k \mathcal{A}_K / (\mathcal{A}_K(D) + K) = \iota(D) := \ell(D) - \deg(D) + g - 1,$$

where $\iota(D)$ is the index of speciality of the divisor, which measures the discrepancy between the degree and the dimension.

Remark 7.0.5: This says that adding K into the adelic Riemann-Roch space results in a big k -vector space, having high dimension in the infinite dimensional k -vector space \mathcal{A}_K . 

Proof (Step 1).

For divisors $A_1 \leq A_2$, we have a short exact sequence of k -vector spaces

$$0 \rightarrow \mathcal{L}(A_2)/\mathcal{L}(A_1) \xrightarrow{\sigma_1} \mathcal{A}_K(A_2)/\mathcal{A}_K(A_1) \xrightarrow{\sigma_2} (\mathcal{A}_K(A_2) + K) / (\mathcal{A}_K(A_1) + K) \rightarrow 0.$$

The first thing we did was compute the dimension of the middle quotient space, which was $\deg D_2 - \deg D_1$. Note that σ_2 is a quotient map, but σ_1 just comes from embedding $K \hookrightarrow \mathcal{A}_K$. To show exactness, the only nontrivial part is that $\ker(\sigma_2) \subset \text{im}(\sigma_1)$. So take an element $\alpha \in \mathcal{A}_K(A_1) \bmod \mathcal{A}_K(A_1)$ such that $\sigma_2(\alpha) = 0$, so there exists an $x \in K$ such that $\alpha - x \in \mathcal{A}_K(A_1)$ by definition of being zero in the last quotient. Since $\mathcal{A}_K(A_1) \subseteq \mathcal{A}_K(A_2)$, we have that $x \in \mathcal{A}_K(A_2) \cap K := \mathcal{L}(A_2)$. This follows because $\alpha, \alpha - x$ are both in $\mathcal{A}_K(A_2)$. Thus we have

$$\alpha + \mathcal{A}_K(A_1) = x + \mathcal{A}_K(A_1) = \sigma(x + \alpha(A_1)).$$

■

Proof (Step 2).

We can now compute the dimension of this quotient. Using step 1 and Lemma 2.12, we get

$$\begin{aligned} \dim_k (\mathcal{A}_K(A_2) + K) / (\mathcal{A}_K(A_1) + K) &= \dim_k \mathcal{A}_K(A_2)/\mathcal{A}_K(A_1) - \dim_k \mathcal{L}(A_2)/\mathcal{L}(A_1) \\ &= (\deg A_1 - \ell(A_2)) - (\deg A_1 - \ell(A_1)) \\ &= \iota(A_1) - \iota(A_2), \end{aligned}$$

where the last step follows from adding and subtracting $g - 1$.

■

Proof (Step 3).

By step 2, it is enough to show that for all $A_1 \in \text{Div } K$, there exists a bigger divisor $A_2 \geq A_1$ such that $\iota(A_2) = 0$ (by just adding closed points) and $\mathcal{A}_K(A_2) + K = \mathcal{A}_K$. By Riemann's inequality, we have $\iota(A_2) = 0$ if $\deg A_2 \gg 0$, so choose such an $A_2 \geq A_1$. Thus we're reduced to showing that if $\iota(B) = 0$ for all $B \in \text{Div } K$, then $\mathcal{A}_K = \mathcal{A}_K(B) + K$. We'll do this by choosing another large effective divisor.^a

Let $B_1 \geq B$, then we have

$$\begin{aligned} \ell(B_1) &\leq \deg(B_1) + \ell(B) - \deg(B) \\ &= \deg(B_1) - g + 1. \end{aligned}$$

Also, Riemann's inequality gives $\ell(B_1) \geq \deg(B_1) - g + 1$, so we have equality. Thus any divisor greater than or equal to a non-special divisor is again non-special.

We want to take an arbitrary element of the Adele ring and show that it differs from an element of the adelic Riemann-Roch space associated to B by an element of K , so we'll cleverly choose a divisor in order to do this. So take an arbitrary element $\alpha \in \mathcal{A}_K$ of the Adele ring, then we may choose $B_1 \geq B$ such that $\alpha \in \mathcal{A}_K(B_1)$. I.e., choosing B_1 large enough is allowing the poles to be however bad you want them to be, and α is a fixed element, all but finitely many elements have valuation ≥ 0 .

We understand the relative situation well, based on what we proved. By step 2, since B, B_1

are non-special, the dimension of the quotient is zero:

$$\begin{aligned}\dim_k(\mathcal{A}_K(B_1) + K)/(\mathcal{A}_K(B) + K) &= \deg(B_1 - \ell(B_1)) - (\deg B - \ell(B)) \\ &= (g - 1) - (g - 1) \\ &= 0.\end{aligned}$$

But then these spaces are equal to each other, so $\mathcal{A}_K(B_1) + K = \mathcal{A}_K + K$. But we chose B_1 arbitrarily large so it contained α , and we found that the resulting space is no bigger than the original. Note that B_1 was chosen so that $\alpha \in \mathcal{A}_K(B_1)$ before adding K , which remains true when adding K . But this says α is in the LHS, which equals the RHS. Then $\alpha \in \mathcal{A}_K(B)$, where α was arbitrary, so $\alpha \in \mathcal{A}_K(B) + K$. ■

^aThis “cone structure” on divisors is very useful!

Corollary 7.0.6(2.14).

This can be applied to the zero divisor:

$$\dim_k \mathcal{A}_K(\mathcal{A}_K(0) + K)\iota(0) = g.$$

Exercise 7.0.7(?): Corollary 2.14 shows that if $K = k(t)$ is the rational function field, then we have $\mathcal{A}_K(0) + K = \mathcal{A}_K$.¹² Show this directly. ✍

Remark 7.0.8: Note that analogy to consider $\mathcal{A}(\mathbb{Q})$, where you get $\mathcal{A}_{\mathbb{Q}} = \widehat{\mathbb{Z}} + \mathbb{Q}$, where $\widehat{\mathbb{Z}}$ denotes the profinite completion. Recall that $\mathbb{A}_{\mathbb{Q}} = \prod_p' \mathbb{Q}_p \times \mathbb{R}$, and inside of this we have $\mathbb{A}(0) := \prod_p \mathbb{Z}_p \times \mathbb{R}$. Not too crazy of a fact: given an Adele, it has finitely many places where its p -adic valuation is negative, so it shouldn't be hard to find a rational number as a correction term which doesn't change the valuation. The fact that this works for \mathbb{Q} is related to \mathbb{Z} being a PID. ✍

¹²So every Adele differs from a rational function by an effective Adele.

8 | Lecture 11B: Weil's Proof of Riemann-Roch

9 | Lecture 11C: Weil's Proof of Riemann-Roch

10 | Lecture 12 (Chapter 3: Curves Over a Finite Field)

We consider $k = \mathbb{F}_q$ a finite field, which by definition is a one variable global function field. Idea: we've defined some affine dedekind domains (the holomorphy rings) had a finite nonempty set of places of the function field. These are analogous to the ring of integers of a number field, or more generally S -integer rings. Recall some basic results from NT1: the finiteness of the class group, and the finite generation of the unit group. Here we have a class groups of affine Dedekind domain, and by Rosen's theorem, there are infinitely many as you vary over nonempty subsets of places of the function field, and they're all closely connected to a geometric class group: the degree zero divisor class group. Thus by this analogy, when the field is finite, we'd expect that $\text{Cl}^0(K)$ is finite as well, which is the main result we'll prove today.

10.1 Base Extension

Let K/\mathbb{F}_q be a one variable function field with constant field \mathbb{F}_q , so that the only elements of K that are algebraic over \mathbb{F}_q are already in \mathbb{F}_q . Since \mathbb{F}_q is a perfect field ($x \mapsto x^p$ is a surjection), every such function field is regular.

Let $\bar{\mathbb{F}}_q$ be an algebraic closure, then for all $r \in \mathbb{Z}^+$ there exists a unique degree r extension, which we'll denote \mathbb{F}_{q^r} . The extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is a cyclic galois extension (i.e. it's galois group is cyclic) with a canonical generator: the Frobenius map.

The galois theory of the constant field comes in when trying to study constant extensions of the function field. There is a general theory of constant extensions, but in our case, every such extension will be cyclic or procyclic, so we don't need the entire theory.

For any positive integer r , define the extension $K_r := K\mathbb{F}_{q^r}$ given by extending scalars, which is a regular function field over \mathbb{F}_{q^r} . There are two ways to obtain this: either take an algebraic closure of K and take the compositum, or take $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$, which we proved was again a field. This K_r is what we get by extending constants, and the way regular function fields work is that if you make an arbitrary extension of the ground field, then you retain a regular function field over this new extension. On the other hand, note that K_r/K is a degree r arithmetic extension of function field,

whose galois group is also generated by Frobenius. If we take any regular function field over k and then take a finite galois extension l/k , then extending scalars in this way would give an extension of the upstairs fields which is galois and has the same galois group as the constant extension. This is *arithmetic* because the only thing that changes going from K to K_r is the field of constants.

In the analogy of function fields as the meromorphic functions on a Riemann surface, this type of extension has no analog: since \mathbb{C} is algebraically closed, there are no constant extensions. So arithmetic extensions are just extending scalars, and *geometric* extensions don't change the constant field at all and instead have the property that if you extended scalars to the algebraic closure, you'd have an extension of the same degree. Note that the étale fundamental group also has a similar decomposition into an arithmetic part and a geometric part (see Daniel Litt's course).

10.1.1 Splitting of Places

Question 10.1.1: Given a place in K , how does it split (or not) in K_r ?

Remark 10.1.2: We can ask this question in whenever we have an extension of function fields. This reduces to the usual ATI type of question: for $v \in \Sigma(K/\mathbb{F}_q)$, choose an affine Dedekind domain R such that $v \in \Sigma(K/R)$, i.e. the place is regular. Let S be the integral closure of K in K_r ; this place corresponds to a maximal ideal \mathfrak{p} , we then want to factor its pushforward $\mathfrak{p}_v S$. So this question is a special case of how a prime ideal factors in an extension of Dedekind domains.

We'll temporarily black-box the following lemma:

Lemma 10.1.3(?).

Suppose v is the downstairs place, r is the degree of the extension, and $d := \deg(v)$. Then

- K_r/K is galois and we have $efg = r$.^a
- This extension will be unramified: we in fact have $e = 1$, so $g = \gcd(d, r)$ and $f = r/\gcd(d, r)$, and
- Each place $w \in \Sigma(K_r/\mathbb{F}_{q^r})$ lying over v has degree $d/\gcd(d, r)$.

^a e is the prime ramification index, f is the prime residual degree, and g is the number of distinct primes. This result essentially comes from ANTI, replacing $\sum e_i f_i = r$.

Remark 10.1.4: Note that having an extension of Dedekind domains coming from a galois extension of fields simplifies things: this makes the inertial degree and ramification indices coincide.

Example 10.1.5(?):

- The extension is inert $\iff \gcd(d, r) = 1$
 - I.e. d, r are coprime and $g = e = 1, f = r$.
- The extension splits completely $\iff r \mid d$.

- If $r = d$, i.e. we take a degree d place and extend scalars to K_d , it splits completely into d degree 1 places.

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

Remark 10.1.6: Suppose we have w over v with $w \in \Sigma(\mathbb{F}_{q^r})$ and $v \in \Sigma(K/\mathbb{F}_q)$. If v has degree d , this means that the residue field satisfies $k(v) \cong \mathbb{F}_{q^d}$, since we have unique extensions in each degree. If f is the f from ANTI, it is also the degree of the residual extension, so we know $[k(w) : k(v)] = f$ and thus $k(w) \cong \mathbb{F}_q^{fd}$.

On the other hand, $k(w)$ is an extension of \mathbb{F}_{q^r} of degree $\deg(w)$, so $k(w) \cong \mathbb{F}_{(q^r)^{\deg(w)}} = \mathbb{F}_{q^{r \deg(w)}}$. Thus $r = fg$ and

$$q^{f \deg(v)} = q^{r \deg(w)} \implies \deg(w) = \left(\frac{f}{r}\right) \deg(v) = \frac{\deg(v)}{g}.$$

The residue field, if it changes at all, can only increase in size, since any extension of Dedekind domains induces an extension of residue fields. So the size of the residue field of w is at least as big as the size of the residue field of v . But the degree of w is measured relative to the extended field \mathbb{F}_{q^r} , since it's the degree of the residue field as an extension of \mathbb{F}_{q^r} . So consider $\deg(w) = \deg(v)/g$, we see that even as the residue field is increasing by a factor of f , the degree of the point is decreasing by a factor of g .

Upshot: The residue field grows, but its degree can only shrink. Thus making an extension forces the degrees of the upstairs places to *decrease*.

We're trying to find out in how many ways a discrete valuation extends to a finite degree field extension. From ANTII, we have a result that describes this: if v is a rank 1 valuation on k and L/K is a finite degree extension, then the extensions of v to L correspond with $\text{mSpec}(\widehat{K_v} \otimes_K L)$, where the hat denotes completing K with respect to the valuation. The e, f, g can all be computed as well.¹³

This is some finite degree $\widehat{K_v}$ algebra, and if L/K is separable then this decomposes as a finite product of finite degree field extensions of K and $\widehat{K_v}$, the number of which will be g . The e and f can be read off because each extension will have a ramified and unramified part.

Exercise 10.1.7(?):

- Show that $\mathbb{F}_{q^d} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r} \cong \mathbb{F}_{q^l}^{d'}$ where $l = \text{lcm}(d, r)$ and $d' = \text{gcd}(d, r)$.
- Generalize this to the case when k_p/k and ℓ/k are both cyclic galois extensions.

10.2 Degree 1 Places and Rational Points on a Curve

¹³See Pete's NTII notes, Theorem 1.64.

Taking the lemma as a black box, for $r \in \mathbb{Z}^+$ let $N_r := |\Sigma_1(K_r/\mathbb{F}_{q^r})|$, i.e. the number of degree 1 places of the function field after making a degree r extension. Equivalently, $N_r = |C(\mathbb{F}_{q^r})|$ where C is a unique complete nonsingular curve over \mathbb{F}_q corresponding to K , and this denotes the number of \mathbb{F}_{q^r} rational points. We'll eventually see these are finite.

Remark 10.2.1: Important way of thinking about these: degree one places of a function field over k correspond to k -rational points of a curve.

Corollary 10.2.2 (Equivalence of data: places and rational points).

$$N_r = \sum_{d \mid r} d \cdot |\Sigma_d(K/\mathbb{F}_q)|,$$

so knowing the number of closed points of each degree is equivalent to knowing the \mathbb{F}_{q^r} -points for all r .

Proof (?).

Let $w \in \Sigma_1(K_r/\mathbb{F}_{q^r})$ be a degree 1 point and set $v := w \cap K$ so w lies over v . What is the degree of v ? Setting $d := \deg(v)$, the lemma gives

$$1 = \deg(w) = \frac{d}{\gcd(d, r)},$$

which implies that $\gcd(d, r) = d$ and thus $d \mid r$. So for each d dividing r , every degree d place $v \in \Sigma(K/\mathbb{F}_q)$ contributes $\gcd(d, r) = d$ degree 1 points on K_r , i.e. every downstairs degree d place splits into d degree one places. So for every such d , every degree d closed point contributes d degree 1 closed points lying above it, and conversely if d does not divide r then the upstairs point would not have degree 1, so this accounts for all of the degree 1 points. ■

Remark 10.2.3: We saw that the degree 1 places and the rational points are the same information, and there is a third equivalently quantity: A_n , defined to be the number of effective divisors of degree n .

10.3 Finiteness of Places and Rational Points

Lemma 10.3.1(?).

- a. For all d , the number of degree d closed points $\Sigma_d(K/\mathbb{F}_q)$ is finite (and therefore N_r is finite), and
- b. For all n , A_n is finite.

Proof (of a).

Let L/K be a degree n extension of regular function fields over \mathbb{F}_q . We then have a restriction map

$$r : \Sigma(L/\mathbb{F}_q) \twoheadrightarrow \Sigma(K/\mathbb{F}_q)$$

which we showed is surjective with finite fibers. We can say a little bit more: for all places $w \in \Sigma(L/\mathbb{F}_q)$, we have an inequality

$$\left(\frac{1}{n}\right) \deg(w) \leq \deg(r(w)) \leq \deg(w),$$

noting that we're now measuring all degrees over a common ground field \mathbb{F}_q . So things are now what you'd expect: the degree of the upstairs point is a multiple of the degree of the downstairs point. The upper bound comes from the fact that the residue of the upstairs point is a finite extension of the residue field of the downstairs points. The opposite inequality comes from ANTI: the degree of the residual extension is at most the degree of the entire extension. So r doesn't preserve degrees exactly, but preserves them up to a bounded factor, and thus $\Sigma_{\leq d}(L/\mathbb{F}_q)$ is finite for all $d \iff \Sigma_{\leq d}(K/\mathbb{F}_q)$ is finite for all d . Because of this, we can reduce the situation by exchanging the function field L/\mathbb{F}_q with any other function field for which L is a finite extension, and in particular we can take the rational function field $K = \mathbb{F}_q(t)$. What are the degree d places of a rational function field? There is exactly one place at infinity, and the remaining ones correspond to monic irreducible polynomials. Since \mathbb{F}_q is finite, there are only finitely many such polynomials of any fixed degree.^a ■

^aThere is an exact formula for this quantity.

Proof (of b).

Left as an exercise.

Some remarks: how do you build an effective divisor of degree n ? Take closed points (places) and start adding them up with positive coefficients, then the degree of the divisor is the sum of the degrees of the places. But if you only have finitely many places, each of which can only be used a bounded number of times (certainly no more than n times!), thus one can only build finitely many effective divisors of each degree. ■

10.4 Finiteness of Class Group

Proposition 10.4.1 (*Finiteness of class group*).

The degree 0 divisor class group $\text{Cl}^0(K)$ is finite.

This is a geometric analog of the finiteness of the class group of the ring of integers of a number field. By Rosen's theorem, as an immediate corollary, the class group of any affine dedekind domain over a finite ground field is finite. This follows from looking at the exact sequence: a finite index subgroup of the class group of any dedekind domain is a quotient of $\text{Cl}^0(K)$, and a finite index subgroup of a finite group is finite.

Proof (?).

Set $\delta := I(K)$ to be the index, i.e. the least possible degree of a divisor.^a

In any case, for all $n \in \mathbb{Z}$, we have

$$\text{Cl}^n K = \left\{ \begin{array}{ll} 0 & \delta \nmid n \\ |\text{Cl}^0 K| & \delta \mid n \end{array} \right.$$

If you have any degree n divisors, then $\text{Cl}^n K$ will be a coset of $\text{Cl}^0 K$. Here we just look at the degree map, which is a group morphism onto its image, of which all nonempty fibers have the same size. Thus we may work with $\text{Cl}^n K$ for $n \gg 0$.

In particular, choose $n \geq g$ the genus such that $\delta \mid n$, and let $D \in \text{Div}^n K$. A Riemann-Roch computation shows that $\ell(D)$, the dimension of the linear system, is at least $n - g + 1$, and so we have $\ell(D) \geq 1$ and D is linearly equivalent to an effective divisor. This shows that the map taking effective degree n divisors to $\text{Cl}^n K$ taking a divisor to its divisor class (restricted to effective divisors) is surjective. But we just saw that the set of effective degree n divisors is finite – it was built out of finitely many closed points of bounded degrees – forcing $\text{Cl}^n K$ to be finite. The result follows because $\text{Cl}^n K$ is a coset of $\text{Cl}^0 K$, all of which have the same size, and the index is finite. ■

^aBy a theorem of Schmidt, we'll later prove that $\delta = 1$.

Definition 10.4.2 (Class Number of K)

The **class number** of K is defined as

$$h := |\text{Cl}^0 K|.$$

Remark 10.4.3: There is a much fancier proof: there exists a g -dimensional abelian variety A/\mathbb{F}_q , the *Jacobian variety* of C/\mathbb{F}_q , such that $\text{Cl}^0 K \cong A(\mathbb{F}_q)$. It is built out of the degree 0 divisor class group in some functorial way. In particular, A is a projective variety, and thus embeds into some $\mathbb{P}_{/\mathbb{F}_q}^N$, and so $|A(\mathbb{F}_q)| \leq |\mathbb{P}_{/\mathbb{F}_q}^N| < \aleph_0$.

As one varies over all function fields over all finite fields, there will only be finitely many whose class number is bounded by some fixed h_0 . E.g. there are only finitely many function fields of class number 1, and these can be explicitly listed. So $h \rightarrow \infty$ in some sense, which is not proved by showing that $|A(\mathbb{F}_q)| \rightarrow \infty$, and we'll instead prove it using methods closer to what we're seeing in this course.

Up next: setting up the zeta function.

11 | 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 $x \rightarrow x^q$. Note that \mathbb{F}_{q^r} is the fixed field of F^r , the r th 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 do places in K decompose in K_r ?

Remark 11.0.1: 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 R in K_r . Then we want to factor $p_v S$?

Not quite sure.

Lemma 11.0.2 (Key lemma about how places split.).

Suppose $d := \deg(v)$. Then K_r/K is galois, so we have $efg = r$. In fact, $e = 1$, so $f = \frac{r}{\gcd(d, r)}$ and $g = \gcd(d, r)$ and each place $w \in \Sigma(K_r/\mathbb{F}_{q^r})$ has degree $\frac{d}{\gcd(d, r)}$.

Remark 11.0.3: 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 11.0.4(?).

Suppose $C \in \text{Cl}(K)$, 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 11.0.5: 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 .

11.1 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

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

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

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

Where we're going: How does $Z(t)$ depend on K ? It turns out that it only depends on $A_0, A_1, \dots, A_{2g-2}$, 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 11.1.1 (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 .

^aIt 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, then the formula involves the dimension of the linear system.

11.2 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 $\text{Cl}^0(K) = 0$ over any ground field \mathbb{k} (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:

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

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 11.2.1(?): 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 i th 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 11.2.2 (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.

12 | Lecture 14

Recall that the *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

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

which is a formal power series with integer coefficients.

Remark 12.0.1: Recall that we have proved that it is a rational function of t , and in particular when $g = 0, \delta = 1$ ¹⁴ 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 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

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

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, how many are in each degree, and what is the dimension of the Riemann-Roch space?

Remark 12.0.2: This is analogous to the Dedekind zeta function of a number field K , in which case

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

¹⁴The *index* of the function field, least positive degree of a divisor.

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

Theorem 12.0.3 (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 12.0.4: 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 n th roots of unity in \mathbb{C} .

Lemma 12.0.5 (?).

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/d th roots of unity, then raising to the d th power gives them multiplicity d . On the RHS, this is an exercise in cyclic groups: consider the n th power map on $\mathbb{Z}/r\mathbb{Z}$ and compute its image and kernel. As ξ ranges over r th roots of unity, ξ^m ranges over all r/d th 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 12.0.6 (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 12.0.7(?): 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 $d := \gcd(m, r)$ 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^r into ones that have the same fiber. We then can range over all p first, then over all p^r in the fiber above p , yielding

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

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

$$\prod_{p^r/p} \frac{1}{1 - t^{r \deg(p^r)}} = (1 - t^{rm/d})^{-d} = \prod_{\xi \in \mu_r} (1 - (\xi t)^m)^{-1},$$

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 12.0.8: 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 δ th 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 $\text{Ord}_{t=1}(t^\delta) = 0$, we get

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

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 δ th 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 12.0.9: 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 is 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 12.0.10(?): 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 understanding 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.

12.1 The Functional Equation

Theorem 12.1.1 (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 $\frac{1}{qt}$ 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: it gives the dimension in terms of the dimension of a complementary divisor.

Take a canonical divisor $\mathcal{K} \in \text{Div}(K)$, 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

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

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

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,

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

$$= q^{g-1} t^{2g-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\deg(C)-(2g-2)+\ell(\mathcal{K}-C)} t^{\deg(C)-(2g-2)} \quad \text{by Riemann-Roch}$$

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

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

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

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

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

$$= (q-1)G(t),$$

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

12.2 The L Polynomial

Definition 12.2.1 (The L Polynomial)

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

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

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)} = \frac{a_{2g}t^{2g} + \cdots + a_1t + a_0}{(1-t)(1-qt)}.$$

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, \dots, 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, \dots, 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 $\mathbb{F}_q, \mathbb{F}_{q^2}, \dots, \mathbb{F}_{q^g}$ 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.

13 | Indices

List of Todos

What's a global field?	7
Look up uniformizing elements and valuations.	13
Not quite sure.	37

Definitions

1.1.1	Definition – Finitely Generated Field Extension	4
1.1.2	Definition – Finitely Generated Algebras	4
1.1.3	Definition – Rational Function Field	4
1.1.6	Definition – Algebraically Independent	5
1.1.8	Definition – Transcendence Degree	5
1.1.11	Definition – Function Fields	6
1.3.1	Definition – ?	7
2.0.4	Definition – ?	9
4.1.2	Definition – Geometrically Irreducible	16
5.1.1	Definition – Valuation	19
5.1.2	Definition – Valuation Ring	19
5.1.4	Definition – Group of Divisibility	19
5.1.13	Definition – Equivalence of Krull valuations	21
5.1.17	Definition – Important: Regular and Centered	21
5.1.19	Definition – Key: Zariski-Riemann Space	22
5.1.21	Definition – Key: Places, Points of a Curve	22
5.1.23	Definition – Zariski Topology	22
10.4.2	Definition – Class Number of K	36
12.2.1	Definition – The L Polynomial	49

Theorems

1.1.5	Theorem – Field Theory Notes 11.19	5
1.1.7	Theorem – ?	5
1.1.9	Theorem – Transcendence Degree is Additive in Towers	6
1.1.10	Theorem – Bounds on Transcendence Degree	6
1.2.1	Theorem – Luroth	6
1.2.2	Theorem – Castelnuovo	6
1.2.3	Theorem – Zariski	7
1.2.4	Theorem – Clemens-Griffiths	7
1.4.1	Theorem – Finitely Generated in Towers	8
3.1.5	Proposition – FT 12.7, 12.8	11
3.1.12	Theorem – FT 12.20	13
3.2.1	Proposition – Some Facts	14
4.1.4	Proposition – ?	16
4.1.9	Theorem – Regular Function Fields in One Variable are Geometrically Irreducible	17
5.1.25	Theorem – Zariski	23
5.1.29	Theorem – CA 17.17	24
7.0.4	Theorem – 2.13	28
10.4.1	Proposition – Finiteness of class group	36
11.1.1	Proposition – Formula for the zeta function exhibiting rationality	41
11.2.2	Theorem – Schmidt, 1910ish	42

12.0.3	Theorem – F.K. Schmidt	44
12.0.6	Proposition – Factorization identity for the zeta function	44
12.1.1	Theorem – Functional Equation	47

Exercises

1.1.4	Exercise	5
1.2.5	Exercise	7
2.0.2	Exercise	8
3.1.2	Exercise	10
3.1.4	Exercise	11
3.1.6	Exercise	11
3.1.8	Exercise	12
3.1.14	Exercise	14
4.1.1	Exercise	16
4.1.3	Exercise – an easy one	16
4.1.5	Exercise	17
4.1.6	Exercise – Nice, Recommended	17
5.1.9	Exercise – ?	20
5.1.10	Exercise – ?	20
5.1.11	Exercise – ?	20
5.1.15	Exercise – ?	21
5.1.26	Exercise – ?	23
5.1.32	Exercise – ?	26
5.1.33	Exercise – Constructing valuations of arbitrary rank and value group	26
7.0.2	Exercise – ?	27
7.0.7	Exercise – ?	30
10.1.7	Exercise – ?	33
11.2.1	Exercise – ?	42
12.0.7	Exercise – ?	45
12.0.10	Exercise – ?	46

List of Figures