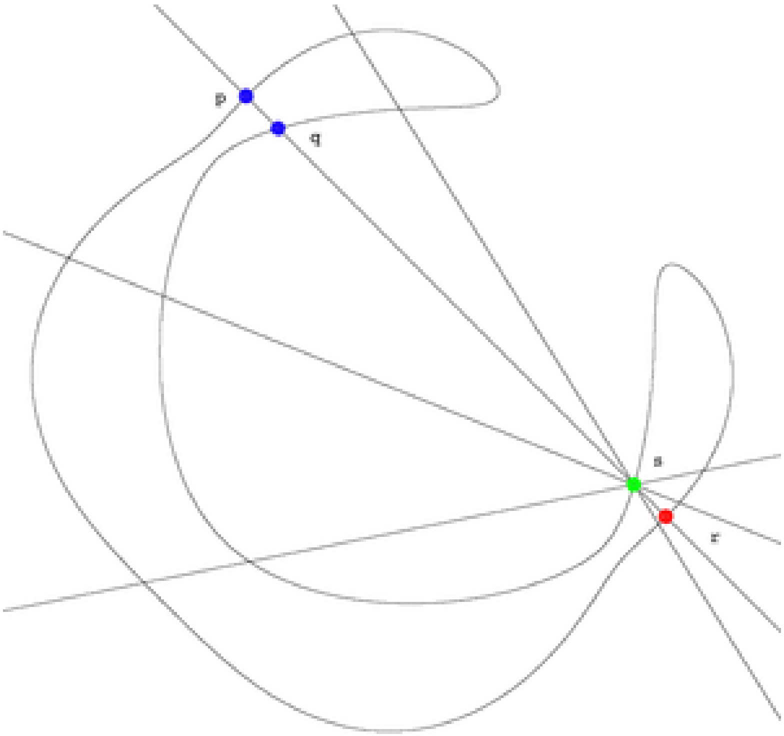

Notes: These are notes live-tex'd from a graduate course in Algebraic Curves taught by Pete Clark at the University of Georgia in Fall 2020. As such, any errors or inaccuracies are almost certainly my own.

Algebraic Curves

University of Georgia, Fall 2020

D. Zack Garza

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

Last updated: 2020-12-18

Contents

1 References

1.1 References

- Stichtenoth[1].

2 Lecture 1: Field Theory Preliminaries

The main theorems in this course, in order of importance:

- The Riemann-Roch Theorem
- The Riemann-Hurwitz Formula

2.1 Finite Generation of Fields

See Chapter 11 of Field Theory notes.

2.1.1 Notion 1

Definition 2.1.1 (Finitely Generated Field Extension)
A field extension ℓ/k is *finitely generated* if there exists a finite set $x_1, \cdots, x_n \in \ell$ such that $\ell = k(x_1, \cdots, x_n)$ and ℓ is the smallest field extension of k.
Concretely, every element of ℓ is a quotient of the form $\dfrac{p(x_1, \cdots, x_n)}{q(x_1, \cdots, x_n)}$ with $p, q \in k[x_1, \cdots, x_n]$.

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

2.1.2 Notion 2

The second is being finitely generated as an algebra:

Definition 2.1.2 (Finitely Generated Algebras)
For $R \subset S$ finitely generated algebras, S is finitely generated over R if every element of S is a polynomial in $x_1, \cdots, x_n$, with coefficients in R, i.e. $S = R[x_1, \cdots, x_n]$.

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

2.1.3 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 2.1.3 (Rational Function Field)
A *rational function field* is $k(t_1, \cdots, t_n) := ff\,(k[t_1, \cdots, t_n])$.

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 2.1.4:

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).[1]

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

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

Theorem 2.1.5 ***(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.[a]

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

Definition 2.1.6 (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 2.1.7 ***(Existence of transcendence bases).***
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.

[1] Note $k[t]$ is not a field.
[2] Hint: Zariski's lemma.

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).[3]

The following notion will be analagous to that of dimension in linear algebra:

Definition 2.1.8 (Transcendence Degree)
The *transcendence degree* of ℓ/k is the cardinality of any transcendence basis.

Theorem 2.1.9 ***(Transcendence Degree is Additive in Towers).***
If $L/K/F$ are fields then $\operatorname{trdeg}(L/F) = \operatorname{trdeg}(K/F) + \operatorname{trdeg}(L/K)$.

Theorem 2.1.10 ***(Bounds on Transcendence Degree).***
Let K/k be finitely degenerated, so $K = k(x_1, \cdots, x_n)$. Then $\operatorname{trdeg}(K/k) \leq n$, with equality iff K/k is purely transcendental.

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

[a]This is similar to checking if a vector is in the span of a collection of previous vectors.

Definition 2.1.11 (Function fields in d variables)
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.

Remark 2.1.12: The study of such fields is birational geometry over the ground field k. $k = \mathbb{C}$ is of modern interest, things get more difficult in other fields. The case of $d = 1$ is much easier: the function field will itself be the geometric object and everything will built from that. Our main tool will be **valuation theory**, where valuations will correspond to points on the curve.

2.2 Case Study: The Lüroth Problem.

Question 2.2.1: For which fields k and $d \in \mathbb{Z}^{\geq 0}$ is it true that if $k \subset \ell \subset k(t_1, \cdots, t_d)$ with $k(t_1, \cdots, t_d)/\ell$ finite then ℓ is purely transcendental?

Answer 2.2.2: It's complicated, and depends on d and k. We have the following partial results.

[3]There is a common generalization: matroids.

Theorem 2.2.3 ***(Lüroth).***
True for $d = 1$: For any $k \subset \ell \subset k(t)$, $\ell = k(x)$.

Theorem 2.2.4 ***(Castelnuovo).***
Also true for $d = 2, k = \mathbb{C}$.

Theorem 2.2.5 ***(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 2.2.6 ***(Clemens-Griffiths).***
No if $d \geq 3$ and $k = \mathbb{C}$.

Remark 2.2.7: Note that unirational need not imply rational for varieties.

Exercise 2.2.8: Let k be a field, G a finite group with $G \hookrightarrow S_n$ the Cayley embedding. Then S_n acts by permutation of variables on $k(t_1, \cdots, t_n)$, thus so does G. Set $\ell := k(t_1, \cdots, t_n)^G$ the fixed field, then by Artin's observation in Galois theory: if you have a finite field acting effectively by automorphisms on a field then taking the fixed field yields a galois extension with automorphism group G.

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

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

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

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

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

What's a global field?

2.3 Integrals Closures and Constant Fields

Definition 2.3.1 (Integral Closure and Field of Constants)
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 $\kappa(K)$.

Remark 2.3.2: In practice, we don't want $\kappa(K)$ to be a proper extension of k. If this isn't the case, we replace considering K/k by $K/\kappa(K)$. If K/k is finitely generated, then

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

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

3 | Lecture 1: Discussion and Review

3.1 Valuations

- Transcendence bases
- Lüroth problem

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

See also *Krull valuations*, which take values in some totally ordered commutative group.

Exercise 3.1.2: Show that a valuation ring is a local ring, i.e. it has a unique maximal ideal.

Example 3.1.3: Where does the log come from?

There is a p-adic valuation:

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

Then we recover

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

.

There is a p-adic norm

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

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

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

We then recover $v_p(x) = -\log_p |x|_p$.[4]

3.2 Places

For $A \subset K$ a subring of a field, we'll be interested in the place $\tilde{\Sigma} = \{\text{Valuation rings } R_v \text{ of } K\} \;\Big|\; A \subset R_v \subsetneq K$. 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*

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

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

Definition 3.2.1 (Generic Points)
A point $p \in X$ a topological space is a **generic point** iff its closure in X is all of X.

Remark 3.2.2: 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.

3.3 Divisors

Definition 3.3.1 (Divisor Group)
The *divisor group* of K is the free $\mathbb{Z}$-module on $\Sigma(K/k)$

[4] See NT 1 notes for more details on valuations.

Remark 3.3.2: This comes with a degree map

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

which need not be surjective.

Definition 3.3.3 (Principal Divisors)
Consider the map

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

Then we define $\operatorname{im}\varphi_d$ as the subgroup of **principal divisors**.

Definition 3.3.4 (Class Group)
Define the **class group** of K as

$$\mathrm{cl}(K) := \{\text{Divisors}\} / \{\text{Principal divisors}\} := \mathrm{Div}(K)/\operatorname{im}\varphi_d.$$

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

4 | Lecture 2: Field Theory Preliminaries

4.1 Base Extension

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

Example 4.1.1: An *affine variety* V/k is given by finitely many polynomials in $p_i \in k[t_1, \cdots, t_n]$, and base extension comes from the map $k[t_1, \cdots, t_n] \hookrightarrow \ell[t_1, \cdots, t_n]$. More algebraically, we have the affine coordinate ring over k given by $k[V] = k[t_1, \cdots, t_n]/\langle p_i \rangle$, the ring of polynomial functions on the zero locus corresponding to this variety. We can similarly replace k be ℓ in this definition. Here we can observe that $\ell[V] \cong k[V] \otimes_k \ell$.

In general we have a map

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

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

What about for function fields? Since k is a k-algebra, we can consider $k \otimes_k \ell$, however this need not be a field. Note that tensor products of fields come up very often, but don't seem to be explicitly covered in classes! We will broach this subject here.

Exercise 4.1.2: If ℓ/k is algebraic and $\ell \otimes_k \ell$ is a domain, the $\ell = k$.

Remark 4.1.3: In other words, this is rarely a domain. A hint: start with the monogenic case, and also reduce to the case where the extension is not just algebraic but finite.

Remark 4.1.4: 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.

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 4.1.5: For ℓ/k a field extension,

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

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

Proposition 4.1.6 ***(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.[a]

[a] 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.

4.2 When Extensions Preserve Being a Domain

Question 4.2.1: 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?

Definition 4.2.2 (Base Change)
If this remains a domain, we'll take the fraction field and call it the **base change**.

Exercise 4.2.3: If K/k is finitely generated (i.e. a function field) and $K \otimes_k \ell$ is a domain, then $ff(K \otimes_k \ell)/\ell$ is finitely generated.

Remark 4.2.4: The point here is that 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 4.2.5.
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

$$\begin{tikzcd} \kappa(K) \otimes_k \kappa(K) \arrow[rr, hook] \arrow[dr, hook] & & K \otimes_k \bar{k} \\ & \kappa(K) \otimes_k \bar{k} \arrow[ur, hook] & \end{tikzcd}$$

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 4.2.6 ***(the simplest possible case):*** Describe $\mathbb{C}(t) \otimes_{\mathbb{R}} \mathbb{C}$, tensored as $\mathbb{R}$-algebras.

Remark 4.2.7: Won't be a domain by the lemma, and will instead be some $\mathbb{C}(t)$-algebra of dimension 2.

4.3 Good Base Change For Function Fields

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.

Question 4.3.1 ***(a more precise one):*** 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 $k^{\frac{1}{p}} := k\left(\left\{x^{\frac{1}{p}} \;\middle|\; x \in k\right\}\right)$ is obtained by adjoining all pth roots of all elements. This is a purely inseparable extension. The latter condition (this tensor product being a field) is one of several equivalent conditions for a field to be separable.[5]

Remark 4.3.2: Recall 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*

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

transcendence basis. Since we're only looking at finitely generated extensions, we wont' have to worry much about the difference between separable and separably generated.

Question 4.3.3: 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 $\kappa(K) = k$?

⚠ **Answer 4.3.4:** No, for fairly technical reasons.

Example 4.3.5: Set $k = \mathbb{F}_p(a, b)$ a rational function field in two variables as the ground field. Set

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

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

Claim: $\kappa(K) = k$, so k is algebraically closed in this extension, but K/k is *not* separable.

How to show: extending scalars to $k^{\frac{1}{p}}$ does not yield a domain.

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

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

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

Remark 4.3.6: 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 4.3.7: 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.

Recall that the perfect fields are given by:

- 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 [6]

Theorem 4.3.8 ***(FT 12.20: Regular Field Extensions).***
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.

Remark 4.3.9: Note that this allows making not just an algebraic base change, but a totally arbitrary one.

Definition 4.3.10 (?)
A field extension satisfying these conditions is called **regular**.

Remark 4.3.11: Regular corresponds to "nonsingular" in this neck of the woods. 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 4.3.12:

a. Show that $k(t)/k$ is regular. [7]

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.

4.4 Example of a Non-Regular Family of Function Fields

Choose an elliptic curve $E/\mathbb{Q}(t)$ with j-invariant t. For $N \in \mathbb{Z}^+$, define $\tilde{K}_N \coloneqq \mathbb{Q}(t)(E[N])$ the N-torsion field of E. Then $\tilde{K}_N/\mathbb{Q}(t)$ is a finite galois extension with galois group isomorphic to the image of the modular galois representation [8]

[6] This is a good time to review valuations and uniformizing elements from NTII.
[7] I.e. $k(t) \otimes_k \bar{k}$ is a domain.
[8] See Cornell-Silverman-Stevens covering the proof of FLT, modular curves from the function field perspective.

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

Proposition 4.4.1 ***(Some Facts).***
ρ_N is surjective, and

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

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

Remark 4.4.2: Actually $\tilde{K}_N$ depends on the choice of E: difference choices of nonisomorphic curves with the same j-invariant differ by a quadratic twist and the ρ_N differ by a quadratic character on $g(\mathbb{Q}(t))$. Importantly, this changes the kernel, and thus the field.

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

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

We obtain a field theory diagram

$$\begin{tikzcd}
\overline{K}_N \arrow[d, bend left, "\{\pm I\}"] \arrow[dd, bend right=60, "\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})"'] \\
K_N \arrow[d, bend left, "\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})/\{\pm I\}"] \\
\mathbb{Q}(t)
\end{tikzcd}$$

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

Answer 4.4.4: 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 $H \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\left\{\pm I\right\}$, we'll get a function field $\mathbb{Q}(H) := H_N^H$.gg 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.

5 Lecture 3: Last of Preliminaries

Today we'll be wrapping up the last of the preliminaries. Upcoming: one-variable function fields and their valuation rings.

5.1 Polynomials Defining Regular Function Fields

Question 5.1.1: Where's the curve in all of this?

Answer 5.1.2: This will come from an equation like $f(x, y) = 0$.

Exercise 5.1.3: 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.[9]

5.2 Geometric Irreducibility

Definition 5.2.1 (Geometrically Irreducible Polynomial)
A polynomial of positive degree $f \in k[t_1, \cdots, t_n]$ is **geometrically irreducible** if $f \in \bar{k}[t_1, \cdots, t_n]$ is irreducible as a polynomial.

Remark 5.2.2: If $n = 1$ then f is geometrically irreducible $\iff$ f is linear, i.e. of degree 1. Let f be irreducible, then since polynomial rings are UFDs then $\langle f \rangle$ is a prime ideal (irreducibles generate principal ideals) and $k[t_1, \cdots, t_n]/\langle f \rangle$ is a domain. Let K_f be the fraction field.

Exercise 5.2.3 ***(an easy one):***

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

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

Proposition 5.2.4 ***(?).***
Suppose that f is geometrically irreducible.

a. The function field K/k is regular.

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

Definition 5.2.5 (Absolutely Irreducible Polynomial)
In this case we say f is **absolutely irreducible** as a synonym for geometrically irreducible.

[9] Hint: use a denominator clearing argument.

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

Slogan 5.2.6: Geometrically irreducible polynomials are good sources of regular function fields.

Exercise 5.2.7: Let k be a field, $d \in \mathbb{Z}^+$ such that $4 \nmid d$ and $p(x) \in k[x]$ be positive degree. Factor $p(x) = \prod_{i=1}^{r} (x - a_i)^{\ell_i}$ in $\bar{k}[x]$.

a. Suppose that for some i, $d \nmid \ell_i$. Show that $f(x, y) := y^d - p(x) \in k[x, y]$ is geometrically irreducible. Conclude that $K_f := ff\left(k[x, y]/\left\langle y^d - p(x)\right\rangle\right)$ is a regular one-variable function field over k, and thus elliptic curves yield regular function fields.[10]

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

Exercise 5.2.8 ***(Nice, Recommended):*** Assume k is a field, if necessary assuming $\mathrm{ch}(k) \neq 2$.

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

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

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

d. Let $k = \mathbb{R}$. For $f(x, y) = x^2 + y^2 + 1$, is K_f rational?[11]

Question 5.2.9: Can we always construct regular function fields using geometrically irreducible polynomials?

Answer 5.2.10: In several variables, no, since not every variety is birational to a hypersurface. In one variable, yes, as the following theorem shows:

5.3 Our Function Fields are Geometrically Irreducible

Theorem 5.3.1 ***(Regular Function Fields in One Variable are Geometrically Irreducible).***
Let K/k be a one variable function field (finitely generated, transcendence degree one). Then

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

[10] Referred to as *hyperelliptic* or *superelliptic* function fields. Hint: use FT 9.21 or Lang's Algebra.
[11] This is an example of a non-rational genus zero function field.

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

Recall separable implies there exists a separating transcendence basis.

Proof (of a).
This means there exists a primitive element $x \in K$ such that $K/k(x)$ is finite and separable. By the Primitive Element Corollary (FT 7.2), there exist a $y \in K$ such that $K = k(x, y)$. ■

Proof (of b).
Omitted for now, slightly technical. ■

Remark 5.3.2: Importance of last result: a regular function field on one variable corresponds to a nice geometrically irreducible polynomial f.

Remark 5.3.3: Note that 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 5.3.4: Can every one variable function field be 2-generated?

Answer 5.3.5: 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 5.3.6: Example from earlier lecture:

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

Remark 5.3.7: 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.

6 Lecture 4: Chapter 1, One Variable Function Fields and Their Valuations

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.

6.1 Valuation Rings and Krull Valuations

Recall that NTII approach to valuations:

Definition 6.1.1 (Valuation)
A **valuation** on a field K is a map $v : K \to \mathbb{R} \cup \{\infty\}$ such that $v(K^\times) \subset \mathbb{R}$, $v(0) = \infty$, and v is of the form $-\log(|\cdot|)$ where $|\cdot| : K \to [0, \infty)$ is an *ultrametric norm.*[a] Recall that an *ultrametric norm* satisfies not only the triangle inequality but the ultrametric triangle inequality, i.e. $d(x, z) \leq \max(x, z)$.

[a] In 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 6.1.2 (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 6.1.3: This is a "largeness" property. It also implies that $K = \mathrm{ff}(R)$.

6.2 Group of Divisibility

Definition 6.2.1 (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 $x \leq y \iff y/x \in R$.

[a] This means that the two structures are compatible.

Remark 6.2.2: 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 6.2.3: 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 6.2.4: 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 6.2.5: Note that $\mathbb{R}$ is a totally ordered group.

6.3 Generalized Valuations

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 $v : K^\times \to G(R)$ is a quotient map which we can extend to K by $v(0) \coloneqq \infty$. This has some familiar properties:

- (VRK1) For all $x, y \in K^\times$,[12]

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

- (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 6.3.1 ***(?):*** 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 $(G(R), +, \leq)$.

[12] This 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.

Exercise 6.3.2*(?)*: Conversely, if $v : K^\times \to G$ is a map into a totally ordered commutative group satisfying VRK1 and VRK2[13], then

$$R_v \coloneqq \left\{ x \in K^\times \;\middle|\; v(x) \geq 0 \right\} \cup \{0\}$$

is a valuation ring.[14] We can thus extract valuation rings in this situation.

Exercise 6.3.3*(?)*: A valuation ring is **local**, i.e. there is a unique maximal ideal

$$\mathfrak{m}_v \coloneqq \left\{ x \in K^\times \;\middle|\; v(x) > 0 \right\} \cup \{0\}\,.$$

Remark 6.3.4: 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 6.3.5** (Equivalence of Krull valuations)
> Two Krull valuations on a field K are **equivalent** iff their valuation rings are *equal*.

Remark 6.3.6: 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.[15]
- 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 6.3.7*(?)*: 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 6.3.8: 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 $\operatorname{Spec}(R)$ for R a DVR.

---

[13] Any such map satisfying these two properties is a **Krull valuation**, Krull's generalization of classical valuations.
[14] Note that in a totally ordered group, either $v(x) \geq 0$ or $-v(x) \geq 0$, so we get the property that either $x, x^{-1} \in R_v$.
[15] Pete's Commutative Algebra Notes, Ch. 17.10

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 $d : X \times X \to R$ 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.

6.4 Regular or Centered Valuations

Definition 6.4.1 (Important: Regular and Centered)
Let $v : K^\times \to (G, +)$ 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, $\mathfrak{p} := \mathfrak{m}_v \cap A \in \operatorname{Spec}(A)$ is denoted the **center of** v **in** A.[a]

[a] Here $\mathfrak{m}_v$ denotes pulling back the maximal ideal along this morphism of rings.

Remark 6.4.2: 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 6.4.3 (Key: Zariski-Riemann Space)
For $A \subset K$, define

$$\Sigma(K/A) := \left\{ \text{valuation rings } A \subset R \subsetneq K \,\middle|\, K = \operatorname{ff}(R) \right\}$$
$$\tilde{\Sigma}(K/A) := \left\{ \text{valuation rings } A \subset R \subseteq K \,\middle|\, K = \operatorname{ff}(R) \right\}.$$

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

Remark 6.4.4: 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 $K = \operatorname{ff}(R)$. 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 6.4.5 (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.

[a] Finitely generated field extension of transcendence degree one.

Remark 6.4.6: 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 $\Sigma(K/k)$.

6.5 Topological Considerations

Definition 6.5.1 (Zariski Topology)
The **Zariski topology** on $\Sigma(K/A)$ has a sub-base

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

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 $U(f_1, \cdots, f_n) = \tilde{\Sigma}(K/A[f_1, \cdots, f_n])$. 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 6.5.2: 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 6.5.3 ***(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 $\left|\tilde{\Sigma}(K/A) > 1\right|$ then this is not a separated (T_1) space since the point is not closed.[16] Another example of such a space would be $\operatorname{Spec}(R)$ 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

[16]Note 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.

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.

6.6 Scheme Theory, Resolution of Singularities

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.[17] Here, the choice of a ring is straightforward: literally $\tilde{\Sigma}(A, A[f_1, \cdots, f_n])$. 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 6.6.1 ***(?):*** Endow $\tilde{\Sigma}(K/k)$ with the structure of a locally ringed space.

Remark 6.6.2: 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 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 6.6.3: 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 singularities [18] 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.

6.7 Intermediate Rings

The following is an extremely important result from commutative algebra:

[17] Schemes are a full subcategory of the much larger category of locally ringed spaces.
[18] Resolving means given K/k, we want to find a complete nonsingular affine variety whose function field is K.

Theorem 6.7.1 ***(CA 17.17).***
Let $A \subset K$ be a subring of a field, then

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

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 $\mathrm{ff}(R_v) = K$. Moreover, each valuation ring is integrally closed, although we haven't proved this yet.

Corollary 6.7.2 ***(?).***
For K/k function field, $\cap_{v \in \Sigma(K/k)} R_v = \kappa(K)$, 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.

■

Remark 6.7.3: 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 $\mathrm{trdeg}(K/k) = 1$, 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

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

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.

■

[a] See NTII, Corollary 1.60: a valuation on a field whose restriction to a finite index subfield is discrete is itself discrete.

6.8 Valuations of Every Rank

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 6.8.1 ***(?):*** If K/k is finitely generated of trdeg ≥ 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 6.8.2 ***(Constructing valuations of arbitrary rank and value group):*** Let k be a field and $K = k(t_1, \cdots, t_n)$. Set $G = \mathbb{Z}^n$ with the lex order, so $G^{\geq 0} = \mathbb{N}^n$.

- Show that $k[t_1, \cdots, t_n] = k[G^{\geq 0}]$, where the RHS is the associated semigroup ring.
- Define $v : k[G^{\geq 0}]^\bullet \to G^{\geq 0}$ 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 $v : K^\bullet \twoheadrightarrow G$ 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 6.8.3: There is a huge difference between trdeg $= 1$ and trdeg > 1, and so we'll only be working with the former case in this course.

7 Lecture 5: Places

Definition 7.0.1 (Affine Domain)
An **affine domain** R over a field k is a domain that is finitely generated as a k-algebra.

7.1 Investigating the Set of Places

We saw an interesting example of a function field in more than one variable which showed that valuations of rank larger than 1 can arise, but this does not happen for one variable function fields. That is, for K/k of transcendence degree 1, all valuations on K which are trivial on k are discrete. We'll now want to go farther and describe the places $\Sigma(K/k)$, which will be the set of points on an algebraic curve. Scheme-theoretically, this will literally be the set of closed points on a certain projective curve whose function field is K. Note that a priori, finding closed points on a curve over an arbitrary field is hard!

Recall that if A is a Dedekind domain such that $\operatorname{ff}(A) = K$, then for all $\mathfrak{p} \in \operatorname{mSpec}(A)$ there exists a discrete valuation v_p on K. I.e., every maximal ideal induces a discrete valuation that is A-regular, so the valuation ring will contain A. How is this obtained? Take a nonzero $x \in K^\times$, and take the corresponding principal fractional ideal $\langle x \rangle := Ax$, which we can factor in a Dedekind domain as $Ax = \prod_{\mathfrak{p} \in \operatorname{mSpec}(A)} \mathfrak{p}^{\alpha_\mathfrak{p}}$ with $\alpha_\mathfrak{p} \in \mathbb{Z}$. This looks like an infinite product, but for any fixed x, only finitely many α are nonzero. Note that these α are exactly what we're looking for: the $\mathfrak{p}$-adic evaluation of x is given precisely by $v_\mathfrak{p}(x) := \alpha_\mathfrak{p}$, where we are using unique factorization of ideals in Dedekind domains. Thus we have a map

$$\begin{aligned} v_{\cdot} : \mathrm{mSpec}(A) &\to \Sigma(K/A) \\ \mathfrak{p} &\mapsto v_{\mathfrak{p}}. \end{aligned}$$

So this sends a maximal ideal to a place that is A-regular, and it turns out to be a bijection.

Proposition 7.1.1 ***(?).***
The map v is a bijection, and thus we may write

$$\Sigma(K/A) \cong \mathrm{mSpec}(A).$$

Proof (?).

Claim: v is injective.
If $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{mSpec}(A)$ are two different maximal ideals. Then there exists an element $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_2$, and so $x^{-1} \in A_{\mathfrak{p}_2} \setminus A_{\mathfrak{p}_1}$. This follows since if x is not in $\mathfrak{p}_2$, its $\mathfrak{p}_2$-adic valuation is zero, and thus the $\mathfrak{p}_2$-adic valuation of x^{-1} is $-0 = 0$ as well. On the other hand, since $x \in \mathfrak{p}_1$, its $\mathfrak{p}_1$-adic valuation is positive and therefore $v_{\mathfrak{p}_1}(x^{-1}) < 0$ and x^{-1} is not in $A_{\mathfrak{p}_1}$.

Claim: v is surjective.
Let $v \in \Sigma(K/A)$, so $A \subset R_v$, i.e. take a valuation whose valuation ring contains A. Note that we're not assuming the valuation is discrete, this can be a general Krull valuation, but we're trying to show it's equal to a certain p-adic valuation. As always with a subring of a valuation ring, we can pull back the maximal ideal and consider $\mathfrak{m}_v \cap A \in \mathrm{Spec}(A)$. We're hoping that this is a maximal ideal, since maximals correspond to valuations. Since we're in a Dedekind domain, the only prime ideal we *don't* want this to be is the zero ideal of A, so suppose it were. Then $A^\bullet \subset R_v^\times$, and so $K^\times \subset R_v^\times$. This is because the only element of the maximal ideal that lies in A is zero, so every nonzero element of A is not in this maximal ideal and is thus a unit. But for any unit, its inverse is also a unit, yielding the inclusion $K^\times \subset R_v^\times$. The only way this could possibly happen is if $R_v = K$, which yields the trivial valuation ring. However, by definition, in $\Sigma(K/A)$ we've excluded the trivial valuation, so this ideal can not be zero.

So we can conclude that the pullback $\mathfrak{m}_v \cap A \in \mathrm{mSpec}(A)$, and so $A_{\mathfrak{p}} \subset R_v$. This is from viewing elements in $A_{\mathfrak{p}}$ as quotients of elements in A whose denominator have $\mathfrak{p}$-adic valuation zero. Recall that we want to show that $R_v = A_{\mathfrak{p}}$. We know $R_v \subset K$ is a proper containment, and we can use the fact that a *discrete* valuation ring is maximal among all proper subrings of its fraction field. In other words, for R a DVR, there is no ring R' such that $R \subset R' \subset \mathrm{ff}(R)$. How do you prove this? This is similar to an early exercise in commutative algebra, where we looked at all rings between $\mathbb{Z}$ and $\mathbb{Q}$, which generalized to looking at all rings between a PID and its fraction field, and a DVR is a local PID. So proving this statement is actually easier.

This is enough to show that $A_{\mathfrak{p}} = R_v$, and this $v \sim v_{\mathfrak{p}}$.

■

Remark 7.1.2: What the idea? For a general one variable function field K/k, we'll produce affine Dedekind domains R with $k \subset R \subset K$ and $\mathrm{ff}(R) = K$. This will give is subrings of this full ring of places that are mSpec of Dedekind domains. How many such domains will we need for their union to be the entire set of places? Just one won't work, since $\Sigma(K/k)$ is like a complete or projective object, and a projective variety of dimension 1 can't be covered by a single affine variety. However, it turns out that you can always cover it with 2. In fact, if you take any Dedekind domain between k and $\mathrm{ff}(K)$, the set of missing places (the ones that aren't regular for any of these domains) will be a nonempty finite set of places. So you can always cover it by finitely many, and two suffices: as a consequence of the Riemann-Roch theorem, after removing any nonempty finite set of places, you'll have the mSpec of a canonically associated Dedekind domain. We'll prove this by starting with the case of $K = k(t)$.

Claim:

$$|\Sigma(k(t)/k) \setminus \operatorname{mSpec} k[t]| = 1.$$

Question 7.1.3: Note that $k \subset k[t] \subset k(t)$ and $k[t]$ is a Dedekind domain, so this fits into the above framework, and moreover we know the maximal ideals of polynomial rings: irreducible monic polynomials. Taking all of these misses exactly one place.

How do we describe this missing place?

7.2 Describing the Missing Place

Suppose $v \in \Sigma(k(t)/k) \setminus \Sigma(k(t)/k[t])$, so the valuation ring of v contains k but does not contain $k[t]$. Then the valuation ring can not contain t, and thus $v(t) < 0$ and $v(1/t) = -v(t) > 0$. Since $k[1/t]$ is a PID, so if the valuation wasn't *tdash*regular, it's $1/t$-regular by definition. So $v \in \Sigma(k(t)/k[1/t])$. Note that $k[1/t] \cong k[t]$ as rings. How many valuations on this polynomial ring give positive valuation to $1/t$? Exactly one, since this corresponds to a prime ideal, namely $\langle 1/t \rangle$, so this unique valuation is $v = v_{\frac{1}{t}}$, the $1/t$-adic valuation.

That is, if we write $f \in k(t)$ as $(1/t)^n a(1/t)/b(1/t)$ with $a, b \in k[t]$ polynomials with nonzero constant terms, then $v_{\frac{1}{t}}(f) = n$. Note that this process is the same as the one used to compute the t-adic valuation v_t.

Recall that a valuation on a domain can be uniquely extended to its fraction field by setting $v(x/y) = v(x) - v(y)$.

Exercise 7.2.1 *(?)*: Define $v_\infty : k(t)^\times \to \mathbb{Z}$ by $p(t)/q(t) \mapsto \deg q - \deg p$.

a. Show $v_\infty \in \Sigma(k(t)/k[1/t])$.

b. Show $v_\infty \sim v_{\frac{1}{t}}$ by showing they have the same valuation ring.

c. Show that $v_\infty = v_{\frac{1}{t}}$.

Note that $1/t$ is a uniformizer for v_∞

Theorem 7.2.2 *(Complete description of places).*

$$\Sigma(k(t)/k) = \operatorname{mSpec} k[t] \coprod \{v_\infty\}.$$

Note that we know the maximal ideals – the irreducible monic polynomials – but it takes some effort to write them down. If k is algebraically closed, however, every such polynomial is linear of the form $t - \alpha$ for $\alpha \in k$. In this case, $\operatorname{mSpec} k(t) \cong k$, and so $\sigma(\bar{k}(t)/\bar{k}) = \bar{k} \coprod \{\infty\} = \mathbb{P}^1(\bar{k})$. More generally, the set of places on a rational function field will yield the scheme-theoretic set of closed points on the projective line over k, which is more complicated if $k \neq \bar{k}$ since not all closed points are k-rational. Another way to say this is that if you have a valuation, there is a residue field, and for any place on a one variable function field the residue field will be a finite degree extension of k. The degree 1 points will be the k-rational points, and so $\Sigma(k(t)/k)$ will always contain a copy of k but may have closed points of larger degree, making things slightly more complicated. This complication is handled well in both the scheme-theoretic and this valuation-theoretic approach.

7.3 Finite Generation in Towers

The next theorem is a fact from commutative algebra:

Theorem 7.3.1 *(?).*
Let A be a domain with $\operatorname{ff}(A) = K$. Suppose A is a finitely generated k-algebra, let L/K be a finite degree field extension, and let B be the integral closure of A in L. Then

a. B is finitely generated as an A-module.[a]

b. B is an integrally closed domain with $\operatorname{ff}(B) = L$ which is finitely generated as a k-algebra.

c. $\dim A = \dim B$[b]

d. If A is Dedekind, so is B.

[a] See CA notes, "Second Normalization Theorem", where normalization is a more geometric synonym for integral closure.

[b] Krull dimension, i.e. the supremum of lengths of chains of prime ideals.

Proof (?).
See Pete's CA notes sections 18 and 14. ■

Remark 7.3.2: On why these should be true: we have a NTI square

$$\begin{tikzcd} B \arrow[r, hook, "\subset"] & L \\ A \arrow[u, hook] \arrow[r, hook, "\subset"] & K \arrow[u, hook] \\ k \arrow[u, hook] & \end{tikzcd}$$

We have a domain A with a fraction field K, we take a finite degree extension L/K, and to complete the square we let B be the integral closure of A in L: the collection of elements in L satisfying monic polynomials with coefficients in A.

In our case, we're additionally assuming that A/k is finitely generated as a k-algebra.

Remark 7.3.3:
On (b): B being finitely generated as a k-algebra follows from assuming A is, and additionally that B is finitely generated as an A-module, and finite generation as a module provides finite generation as an algebra. The result follows from transitivity of finite generation of algebras.

On (c): This is just a property of integral extensions.

On (d): Use the characterization of being Noetherian, integrally closed, and Krull dimension 1. The only thing to check is that B is Noetherian, which follows from B being finitely generated as a k-algebra and applying the Hilbert basis theorem.

Remark 7.3.4: Note that we are not assuming that L/K is separable, which is an assumption that would simplify things. By the Krull-Akuzuki theorem, B will always be a Dedekind domain, but it need not be finitely generated over A. So the "stem" to k is grounding the situation: it's not just a Dedekind domain, but rather an *affine* domain: a domain that is finitely generated over a field. Note that this is much better than an arbitrary Dedekind domain!

7.4 Regularity Lemma

Proposition 7.4.1 ***(Regularity Lemma).***
Suppose that instead of $K = \mathrm{ff}(A)$, we instead have $A \subset K$ an arbitrary subring, and L/K a finite extension. Taking the integral closure B yields another NTI square:

$$\begin{tikzcd} B \arrow[r, hook, "\subset"] & L \\ A \arrow[u, hook] \arrow[r, hook, "\text{subring}"] & K \arrow[u, hook] \end{tikzcd}$$

Suppose we have an upstairs valuation v on L. Then it makes sense to restrict valuations to subfields, so

$$v \in \Sigma(L/B) \iff v|_K \in \Sigma(K/A).$$

So the original valuation is B-regular iff the restricted valuation is A-regular.

Proof (?).
$\Longleftarrow$: Since $A \subseteq B$, being B-regular implies being A-regular.

$\Longrightarrow$: Suppose $A \subset R_v$ and $x \in B$, and choose $a_0, \cdots, a_{n-1} \in A$ such that

$$p(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

We can do this precisely because B is integral over A. So we have an integral relation for x, and we want to show $v(x) < 0$ and derive some contradiction from the fact that $v(a_i) \geq 0$. Note that we aren't grounded to the base field here, so this valuation may not be discrete and is rather some arbitrary Krull valuation.

If $x \notin R_v$, then $v(x) < 0$, and we can thus write

$$v(x^n) < \min\left\{ v(a_j x^j) \;\middle|\; 0 \leq j \leq n-1 \right\} \leq v(p(x)).$$

This follows because the first term is $nv(x)$, and so the next term can only be *less* negative since $v(a_j) > 0$. But this is a contradiction, since we know $v(x^n) = v(-\sum_{j=0}^{n-1} a_j x^j)$, and we've exhibited two elements that differ by a unit ($u = -1$) which have different valuations. ■

Next, let K/k be a one variable function, we want to give a nice description of its places. We already described the places of a *rational* function field, and we know we can write the former function fields as finite degree extensions of the latter. Choosing a transcendental $t \in K$, to $K/k(t)$ is a finite extension, restricting evaluations gives a map

$$r : \Sigma(K/k) \to \Sigma(k(t)/k).$$

Claim: This is surjective with finite fibers, so it acts like a branched covering map.

This follows from NTI or NTII. The NTI method is taking an extension of Dedekind domains, taking a prime ideal downstairs, and pushing it forward to see how it factors upstairs. The NTII method is a field with a valuation and an extension of the field and you try to figure out how many ways the downstairs valuation can be extended. If the valuations are discrete, these are the same problem.

7.5 An Inequality on Degrees

Theorem 7.5.1 *(Degree Inequality (NTII, 1.3)).*
Let K be a field with v a rank one valuation with valuation ring R. Let L/K be a finite extension of degree n. Then the set of valuations on L extending v is finite and nonempty, say $\{w_1, \cdots, w_g\}$.
For $1 \leq i \leq g$, define

$$\begin{aligned} e_i(L/K) &:= \left| \frac{w_j(L^\times)}{v(K^\times)} \right| && \text{ramification index} \\ f_i(L/K) &:= [R_{w_i}/\mathfrak{m}_{w_i} : R_v/\mathfrak{m}_v] && \text{residual degree,} \end{aligned}$$

so $e_i, f_i \in \mathbb{Z}> 0$. Then

a. We have a useful inequality:

$$\sum_{i=1}^{g} e_i(L/K) f_i(L/K) \leq [L : K] = n.$$

b. If v is discrete[a] and the integral closure S of R in L is finitely generated as an R-module, then this is an equality.

[a]It will be discrete in our case. Note that this finiteness condition always holds if L/K is separable.

Remark 7.5.2: Note that a valuation can be extended in at least one way over *any* field extension, finite or not. For finite extensions, there's a more precise statement involving completing and taking a tensor product, then identifying number of valuations with the size of some mSpec over a finite-dimensional algebra over the field.

NTII shows that e_i is a finite number by looking at the exponent of the pushforward. Also note that we view $\mathfrak{m}_{w_i}$ as an ideal lying over $\mathfrak{m}_v$, and there is an inclusion of residue fields $R_v/\mathfrak{m}_v \hookrightarrow R_{w_i}/\mathfrak{m}_{w_i}$ which is in fact a finite degree field extension.

Remark 7.5.3: Part (a) already shows that r is surjective with fibers of cardinality at most $[L : K]$, but we want equality. We claim is always holds when K/k is a one variable function field and $v \in \Sigma(K/k)$. There are examples where the inequality is strict, however. In our situation, it's not just an arbitrary extension, we have the aforementioned affine "grounding" phenomenon, and all of these DVRs are going to be localizations of affine Dedekind domains. This is the key fact: arbitrary extensions of Dedekind domains are nowhere near as nice as those where the bottom one is finitely generated over a field.

Proof (First step).
We have a discrete valuation v on K, so let t be a uniformizing element[a] for v. Then the argument is that any such uniformizer t is transcendental over k. We'll do this by arguing $t \notin k$ and then that t is not algebraic over k either.
Since we're assuming v is k-regular, $t \in k \implies 1/t \in k$ and so $v(1/t) \geq 0$, since every element in k should have nonnegative valuation. But we're supposed to have $v(t) = 1$ by definition of

being a uniformizer, so t can not be in k.
Suppose that t is algebraic over k, then $k(t)/k$ is an integral extension, since we're adjoining one algebraic element. By the previous proposition we have that v is $k(t)$-regular, since being regular is preserved by integral extensions. But now rerunning the argument in the previous paragraph shows that this is a contradiction: being $k(t)$-regular would force $v(1/t) \geq 0$, but we'd still need $v(1/t) = -1$.
So t is transcendental over k, and $k[t]$ is a polynomial ring.

■

[a] An element of valuation one.

Proof (Second step).
Let

- A be the integral closure of $k[t]$ in K, and
- B be the integral closure of $k[t]$ in L.

Instead of a NTI square, we'll have the following 3-step diagram:

$$\begin{tikzcd}
k[t] \arrow[r, hook, "\subset"] \arrow[d, hook, "\subset"] & A \arrow[r, hook, "\subset"] \arrow[d, hook, "\subset"] & B \arrow[d, hook, "\subset"] \\
k(t) \arrow[r, hook, "\subset"] & K \arrow[r, hook, "\subset"] & L
\end{tikzcd}$$

So A is a Dedekind domain with $\mathrm{ff}(A) = K$, as is B with $\mathrm{ff}(B) = L$, making both A and B finitely generated $k[t]$-modules. Why? This comes from the theorem of finiteness of integral closure when the downstairs domain is grounded to a field. Since $k[t]$ is finitely generated as a k-algebra, this finiteness applies, which tells us that A finitely generated as a $k[t]$-module, as is B. But if B is finitely generated as a $k[t]$-module and $A \supseteq k[t]$ is an even larger ring, then B is finitely generated as an A-module (potentially with fewer generators).
Thus B is a finitely generated A-module, and v is $k[t]$-regular since t was a uniformizing element, making v regular on both k and t and thus $k[t]$. Then v is also A-regular by the proposition, and thus $v = v_{\mathfrak{p}}$ for some $\mathfrak{p} \in \mathrm{mSpec}(A)$ coming from our classification of A-regular valuations on a Dedekind domain.
So the valuation on K is just the $\mathfrak{p}$-adic valuation on this Dedekind domain. This means there is an equality of valuation rings $R = A_{\mathfrak{p}}$[a], the valuation ring of the Dedekind domain. So we now consider S, the integral closure of R in L. This is a NTI situation, but the downstairs Dedekind domain is a DVR, so it's local downstairs. We thus have compatibility between integral closure and localization in the form of $S = B_{\mathfrak{p}} = B \otimes_A A_{\mathfrak{p}}$. This comes from taking the whole integral closure B, and only looking at the primes lying over $\mathfrak{p}$. Base change preserves finite generation, and we know that B was finitely generated as an A-module, so S is finitely generated as an $A_{\mathfrak{p}}$-module and equality holds.

■

[a] This is the localization at $\mathfrak{p}$.

Remark 7.5.4: If $A_{\mathfrak{p}}$ was a *complete* DVR, as opposed to just some localization of an affine domain,

B will be a semilocal Dedekind domain and thus a PID, and again the number of primes it has will be the number of primes in the original Dedekind domain lying over the fixed prime $\mathfrak{p}$.

Remark 7.5.5: We're not really using valuation theory here, and this could have been phrased purely in NTI language. But even then, the degree inequality for extensions of Dedekind domains needs finite generated of the Dedekind domain as a module over the bottom Dedekind domain to ensure equality. You'd need a suitably algebraic text that considers not necessarily separable L/K, and you really do want finite generation of B over A to make this work. See Dino Lorenzini's textbook!

Exercise 7.5.6 ***(?):*** Let K/k be a one variable function field, and show that the cardinality of the set of points is given by

$$|\Sigma(K/k)| = |\{\text{monic irreducible polynomials } p \in k[t]\}| = \max(|k|, \aleph_0).$$

Remark 7.5.7: If you know that r is surjective with finite fibers, where the image is infinite (which it is here), the domain should be infinite of the same cardinality by an easy set-theoretic exercise. Note that using Möbius inversion, over a finite field there is at least one irreducible polynomial of every degree, and finitely many of a fixed degree. So the cardinality is $\aleph_0$ when k is a finite field. If we took a one variable function field over $\mathbb{C}$, we would get the cardinality of the continuum. In this case, $\Sigma(K/k)$ really is the set of points on some compact Riemann surface, although the Zariski topology will be too coarse to coincide with the induced Euclidean topology.

Remark 7.5.8: Note that affine Dedekind domains are important for us because every finitely generated field extension of k are precisely the fraction fields of affine domains over k, where the transcendence degree of the function field equals the Krull dimension of the affine domain. We're especially interested in affine domains of dimension 1 over k. We established something particularly important in this proof:

7.6 Affine Grounding and Residue Fields

Lemma 7.6.1 ***(Affine Grounding).***
Let K/k be a one variable function field and $v \in \Sigma(K/k)$ be a place on that function field. Then there exists an affine Dedekind domain A with $\mathrm{ff}(A) = K$ and a maximal ideal $\mathfrak{p} \in \mathrm{mSpec}(A)$ such that $R_v = A_{\mathfrak{p}}$.

Thus we should think of the set of places as the mSpec of finitely many affine Dedekind domains glued together. For each point (place), the basic open set around that point is the affine Dedekind domain.

Corollary 7.6.2 ***(?).***
For $v \in \Sigma(K/k)$, define the **residue field** of the local ring R_v as $k(v) \coloneqq R_v/\mathfrak{m}_v$. Then $k(v)/k$ is a finite degree extension.

Proof (of corollary).
If R is a domain with maximal ideal $\mathfrak{p}$, then the quotient map factors through the localization, giving $R/\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$:[a]

$$\begin{tikzcd} R \arrow[r] \arrow[dr] & R_\mathfrak{p} \arrow[d] \\ & R/\mathfrak{p} \end{tikzcd}$$

So by affine grounding, $k(v)$ is also $A/\mathfrak{p}$ where A is an affine Dedekind domain and $\mathfrak{p} \in \mathrm{mSpec}(A)$. This is Zariski's lemma[b] : we showed that $k(v) \cong A/\mathfrak{p}$, where A is a finitely generated algebra and thus so are its quotients. Thus $k(v)$ is not just finitely generated as a field extension, but also as a k-algebra, making $k(v)/k$ a finite extension. ■

[a] This is a truly standard fact from commutative algebra.
[b] A field extension that is finitely generated as an algebra is necessarily a finite degree extension.

Definition 7.6.3 (Degree of a Place)
The **degree** of $v \in \Sigma(K/k)$ is $[k(v) : k] \in \mathbb{Z}^{\geq 0}$.

We are especially interested in degree 1 places, i.e. those for which the residue field is equal to k itself, so we denote these by $\Sigma_1(K/k)$. In any other course, we'd call this $C(k)$, the rational points on the associated curve.

Exercise 7.6.4*(Some motivation):* Let $f \in k[x, y]$ be irreducible, so that $A := k[x, y]/\langle f \rangle$ is a 1-dimensional affine domain[19]. As above, the resude fields of maximal ideals are finite extensions of k. Show that there is a correspondence

$$\left\{ \substack{\text{Maximal ideals} \\ \mathfrak{p} \in \mathrm{mSpec}(A)} \right\} \iff \left\{ (x,y) \in k \times k \;\middle|\; f(x,y) = 0 \right\}.$$

Remark 7.6.5: Note that the polynomial above may not define a smooth geometry, there may instead be singular points:

[19] This may not necessarily be a Dedekind domain, since it need not be integrally closed.

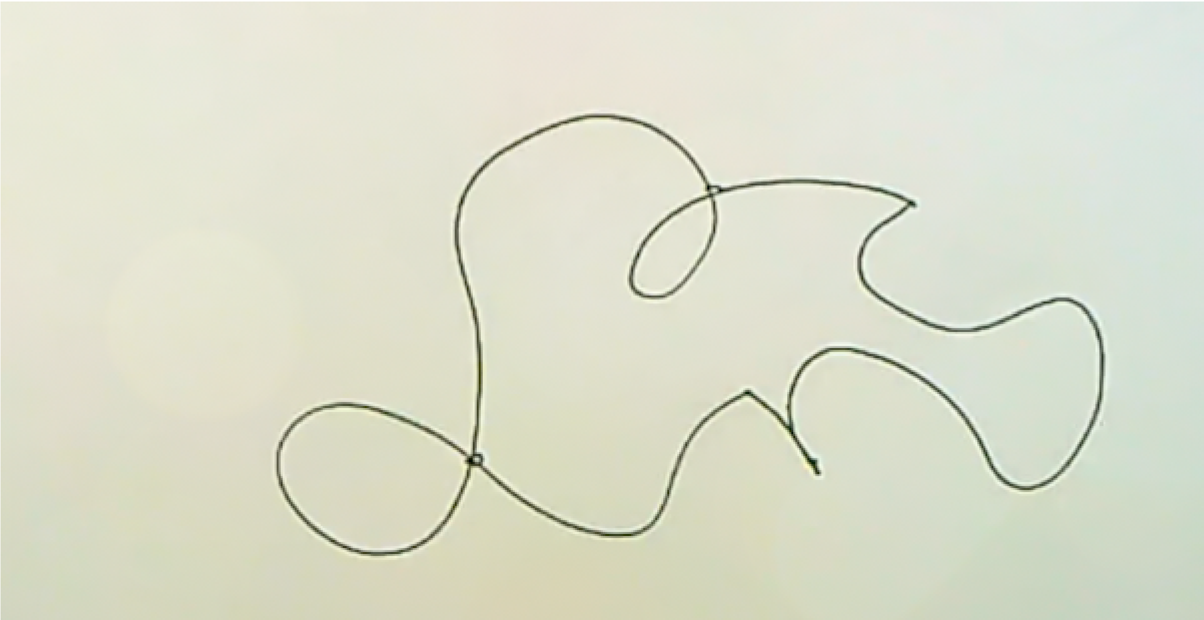

Figure 1: Image

These singular points are what stops A from being integrally closed, which is literally true when k is a perfect field.

Whereas $\Sigma(K/k)$ is always infinite, $\Sigma_1(K/k)$ may be finite or even empty. When $k = \mathbb{Q}$, it may in fact be empty "most of the time" When $k = \mathbb{Q}$, it may in fact be empty "most of the time".

Exercise 7.6.6 ***(?):*** For all $v \in \Sigma(K/k)$, the degree of the point $\deg(v)$ will be divisible by $[\kappa(K) : k]$. Thus if $\kappa(L) \supsetneq k$, then $\Sigma_1(K/k) = \emptyset$.[20]

Note that before we were writing the residue field as an extension of k, and it's worth checking that the constant subfield embeds as a subfield of the residue field as well.

Remark 7.6.7: There is a tie to CM points on modular curves: if you have a function field over $\mathbb{Q}$ which is not regular due to some proper algebraic subextension, the residue fields of all of the points on the curve will contain the algebraic closure of the field of definition. Pete had some $\mathbb{Q}(X_n)$ function field, whose constant subfield was $\mathbb{Q}(\zeta_n)$ (adjoining the nth roots of unity), and none of these modular curves over $\mathbb{Q}$ have closed points except when the residue fields contain $\mathbb{Q}(\zeta_n)$.

Remark 7.6.8: This is a way for there to not be points on the curve, so $\Sigma_1(K/k)$ is empty, but it's not the deepest reason – this is a cheap trick to produce "pointless" function fields. It can fail to have degree 1 places in many different ways!

Exercise 7.6.9 ***(?):*** Show that for for a one variable function field K/k TFAE:

1. Every $v \in \Sigma(K/k)$ has degree 1,

[20] Use the fact that the degree will be bigger than 1 when the constant field is bigger than k.

2. k is algebraically closed.

Remark 7.6.10: One half is easy, since by definition the degree of the residue field is the degree of some finite extension of the base field, but if k is algebraically closed, the degree of any finite extension is one.

Exercise 7.6.11 ***(?):*** For a field k, set $\mathbb{P}^1(k) \coloneqq \mathbb{P}(k^2)$, the projectivization of $k \times k$, i.e. the lines through the origin in $\mathbb{A}^2/k$. By taking slopes of lines, $\mathbb{P}^1(k) = k \coprod \{\infty\}$.

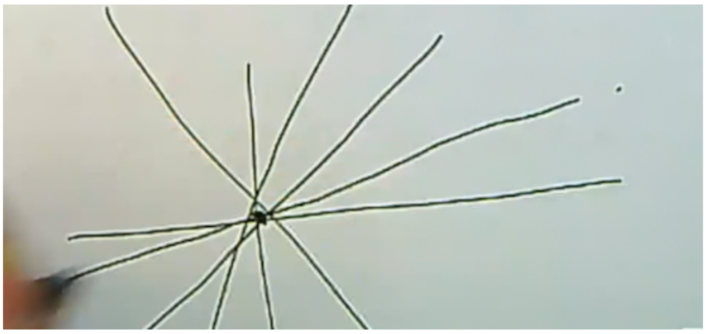

Figure 2: Image

Show that $\Sigma_1(k(t)/k) = \mathbb{P}^1(k)$, and deduce that

$$\Sigma(k(t)/k) = \mathbb{P}^1(k) \iff k = \bar{k}.$$

Next up we'll talk about how the set of places is built from affine Dedekind domains. After this, we'll be ready for chapter 2: divisors and Riemann-Roch.

8 Lecture 6: Affine Domains and Places $\Sigma(K/k)$

The aim of this lecture is to explain the difference (including some technicalities) between $\Sigma(K/k)$ and affine Dedekind domains R such that $K = \mathrm{ff}(R)$.

Recall that

- An **affine domain** over a field k is a domain that is finitely generated as a k-algebra,[21]
- An **affine Dedekind domain** is an affine domain that is also a Dedekind domain, so it is integrally closed and of Krull dimension 1,

[21]These are very rich but easier to understand: take a polynomial ring in finitely many variables and mod out by a prime ideal.

- An **affine k-order** is a one-dimensional affine domain. [22]

Example 8.0.1 ***(?):*** If $f \in k[x,y]$ is irreducible, then $k[x,y]/\langle f\rangle$ is an affine k-order. It is an affine Dedekind domain if f is *nonsingular* over k, i.e. for all $a, b \in \bar{k}$ such that $f(a,b) = 0$, the usual partial derivatives in the sense of Calculus $\dfrac{\partial f}{\partial x}$ and $\dfrac{\partial f}{\partial y}$ do not simultaneously vanish at (a,b). This is a sufficient condition, although it's not far from being necessary as well.

Remark 8.0.2: Let A/k be an affine Dedekind domain such that $\mathrm{ff}(A) = K$. Then $\mathrm{mSpec}(A) = \Sigma(K/A) \hookrightarrow \Sigma(K/k)$. This follows because $\Sigma(K/A)$ are the valuations that are not just regular on k, but also on A, (i.e. A-regular valuations) so the valuation ring contains the entirety of A. It's thus natural to ask what its complement is, i.e. those valuations which are not regular on A and give its elements negative valuation. So define

$$\Sigma(A,\infty) \coloneqq \Sigma(K/k) \setminus \Sigma(K/A),$$

the set of places at infinity with respect to A.

Example 8.0.3 ***(?):*** $\Sigma(k[t],\infty) = \{v_\infty\}$, which is the infinite place, so the terminology at least matches up!

Proposition 8.0.4 ***(Key).***
For any affine Dedekind domain A, $\Sigma(A,\infty)$ is finite and nonempty.

Remark 8.0.5: This is striking! This says that one affine Dedekind domain is giving almost all of this infinite set of places, but never all of it.

Proof (?).
By Noether Normalization [a]
there exists a $t \in A$ that that A is a finitely generated (and thus integral) $k[t]$-module, and A is the integral closure of $k[t]$ in K. Why must this be the integral closure? Any ring finitely generated over a subring will be an integral extension, and A is a Dedekind domain and thus integrally closed. So let

$$r : \Sigma(K/k) \to \Sigma(k(t)/k)$$

denote the restriction map; then by the regularity property we established in Proposition 7.4.1, we have

$$\Sigma(K/A) = r^{-1}\left(\Sigma(k(t)/k[t])\right).$$

Why? A valuation upstairs in the NTI square is regular with respect to the integral extension upstairs iff it's regular with respect to the ring it is the integral extension *of*. So regularity is preserved both ways by integral extensions. This means you can check regularity either upstairs or downstairs, allowing us to identify the above preimage.
This means that the places where are *not* A-regular upstairs are precisely those which are not $k[t]$-regular downstairs, and so we have

$$\Sigma(A,\infty) = r^{-1}\left(\Sigma(k[t],\infty)\right) = r^{-1}(v_\infty),$$

[22] These will be Noetherian by the Hilbert basis theorem, but may not be integrally closed.

since we now there is exactly one such non-regular valuation. But we showed that r was surjective with finite nonempty fibers, so we're done since our set is one of the fibers. ■

[a] This says that if you have an affine domain R of a certain Krull dimension, then it is finitely generated as a module over a subring which is a polynomial ring in $\mathrm{trdeg}(R)$ variables. This is like a stronger integral version of taking a finitely generated field extension and writing it as a finite degree field extension of a purely transcendental extension.

Remark 8.0.6: Thus is K/k is a one variable function field and A is an affine Dedekind domain with fraction field K, then $\Sigma(K/k) = \mathrm{mSpec}(A) \coprod S$ where S is finite and nonempty. Earlier we saw by affine grounding that for each $v \in \Sigma(K/k)$ there exists an affine Dedekind domain A with $v \in \Sigma(K/A)$, and thus $\Sigma(K/k)$ admits a *finite* covering by mSpec of affine Dedekind domains. The picture of what's happening is that we have $\Sigma(K/k)$ which is quasicompact with respect to the Zariski topology, which contains many mSpec, at least one of which contains v. Note that these $\mathrm{mSpec}(A_j)$ for affine Dedekind domains A_j is literally an open cover in this topology. But the open sets are so large that they all have finite complement. However, this means that instead of just an arbitrary open covering, one can choose a finite open covering: one $\mathrm{mSpec}(A_j)$ will cover all but finitely many, and we can always find at least one $\mathrm{mSpec}(A_{j'})$ covering all of the remaining points.

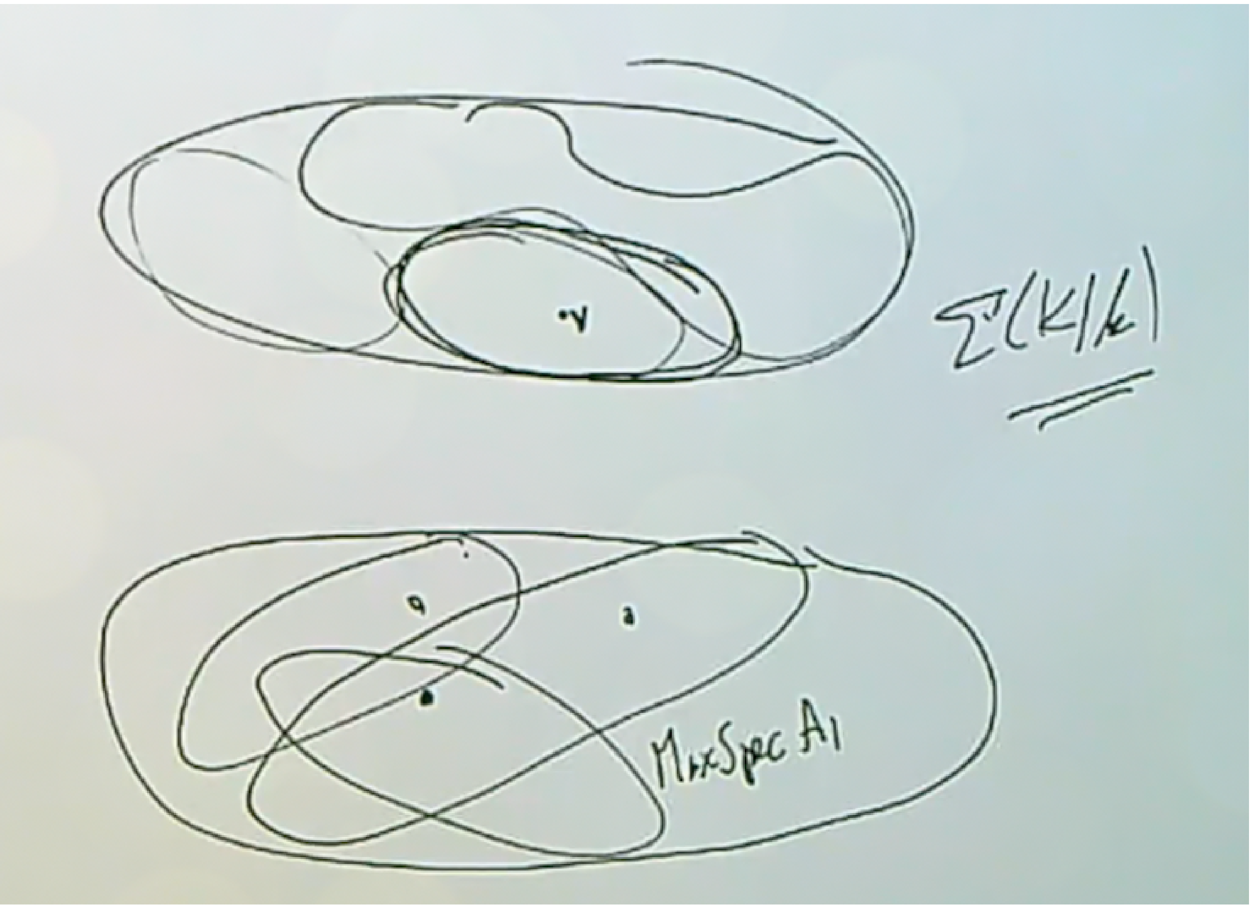

Figure 3: Image

It will in fact turn out that we only need **two** domains to cover everything.

Definition 8.0.7 (Holomorphy Rings)
For a set $S \subseteq \Sigma(K/k)$, define the **holomorphy** ring as

$$R^s := \bigcap_{v \in \Sigma(K/k) \setminus S} R_v.$$

Remark 8.0.8: This is the intersection of a bunch of valuation rings, so this contains elements that are simultaneously regular for this subset of valuations. If $S \subseteq S'$, then $R^S \subseteq R^{S'}$, due to the fact that we're taking complements and $\Sigma(K/k) \setminus S \supset \Sigma(K/k) \setminus S'$, so we're removing bigger sets and thus intersecting over fewer things. This can be thought of as relaxing some regularity conditions.

Remark 8.0.9: How to think about holomorphy rings: if you take $S = \emptyset$, you intersect over all R_v and obtain $R^\emptyset = \kappa(k)$. You get a field that is algebraic over k, so it's very small compared to the other types of field extensions that arise. We'll see that this is "unrepresentably" small.

Exercise 8.0.10 ***(Every affine Dedekind domain is a unique holomorphy ring):*** If A is an affine Dedekind domain with fraction field k, then

$$A = R^S = \bigcap_{v \in \mathrm{mSpec}(A)} R_v \qquad\qquad S = \Sigma(K/k) \setminus \mathrm{mSpec}(A).$$

Remark 8.0.11: This is a fact for any Dedekind domain, which is the intersection over all of its DVRs. You obtain the integral closure for a Dedekind domain by intersecting all of the valuation rings, but here it is already integrally closed. Its tautological that $A \subset R^S$ here, so R^S is an *overring* of a Dedekind domain: for R a domain, an **overring** is any ring T such that $R \subseteq T \subseteq \mathrm{ff}(R)$. When R is a PID, the overrings are in bijective correspondence with subsets of prime ideals (prime elements mod associates), so you get all overrings by inverting such subsets. For Dedekind domains it's more complicated. Can we classify all overrings of R when it is a Dedekind domain? The answer will eventually be yes. Under what condition is every overring a localization? When the class group is torsion. What are the relationships between the class groups of the ring R and its overrings $\widehat{R}$? It turns out that $\mathrm{cl}(\widehat{R})$ is a quotient of $\mathrm{cl}(R)$. We will show that all such overrings are of the form R^W for some W, i.e. they're obtained by intersecting some subset of the localizations of R at its maximal ideals.

Note that the holomorphy ring in the exercise is obtained from a finite set of places. Conversely, given any finite nonempty set of places, then the holomorphy of ring of all of the elements of K that are regular with respect to all but this finite number of valuations will always be an affine Dedekind domain with fraction field K.

8.1 Holomorphy Rings are Affine Dedekind Domains with Fraction Field K

Next up is the main theorem of this lecture.

Theorem 8.1.1 ***(Holomorphy rings on subsets are synonymous with affine Dedekind domains with fraction field K).***
Let K/k be a one variable function field and $S \subset \Sigma(K/k)$ finite and nonempty. Then R^S is an affine Dedekind domain with $\mathrm{ff}(R^S) = K$ and $\mathrm{mSpec}(R^S) = \Sigma(K/k) \setminus S$.

Exercise 8.1.2 ***(?):*** If $S \subset \Sigma(K/k)$ is infinite, then R^S is Dedekind with fraction field K but is *not* finitely generated as a k-algebra.

Remark 8.1.3: So what happens when you allow elements to fail regularity at an infinite set of places instead of just a finite set? From the theory of Dedekind domains, this will again be a Dedekind domain, but will be more exotic than an affine Dedekind domain. What if it were finitely generated as a k-algebra? Then it would be an affine Dedekind domain, and we have a good understanding of mSpec of these types of rings, and it would have to be a holomorphy ring with respect to some finite set. Note that holomorphy rings for different subsets are distinct.

Remark 8.1.4: We have an interesting class of rings: Dedekind domain which are holomorphy rings with respect to an infinite set of places. What are they good for? They're used in Pete's paper "Elliptic Dedekind domains revisited" to give a new proof of a theorem of Clayborne (60s, at least the third proof) that every commutative group is the ideal class group of some R^S.

Get citation.

The Dedekind domain used was a holomorphy ring R^S with respect to some infinite set S. He starts out with an elliptic function field K (so of genus 1 with a degree 1 place), and taking the standard affine coordinate ring of the curve is R^S for S the single degree 1 place. This is particularly nice, since its class group is canonically isomorphic to $C(k)$, the k-rational points of the elliptic curve. When you pass from a Dedekind domain to an overring you get some quotient of the class group. Note that there are three degrees of freedom here: you get to pick k to be any field, then K/k some function field, and then S. For this paper, k was already some weird transfinitely iterated field. The upshot here is that not only is every commutative group isomorphic to $\mathrm{cl}(T)$ for T *some* Dedekind domain, T is in particular a holomorphy ring of the form R^S. This is pretty useful, but not nearly as much as R^S for S a finite set of places.

Definition 8.1.5 (Poles and Zeros)
Let $f \in K^\times$, then a place $v \in \Sigma(K/k)$ is a **pole** of f iff $f \notin R_v$, and v is a **zero** of f iff $f \in \mathfrak{m}_v$.

Lemma 8.1.6 ***(The divisor of a rational function is well-defined.).***
Let $f \in K^\times$ be nonzero, then

$$\left|\left\{v \in \Sigma(K/k) \;\middle|\; f \notin R_v S\right\}\right| < \infty \qquad \text{(finite poles)}$$
$$\left|\left\{v \in \Sigma(K/k) \;\middle|\; f \in \mathfrak{m}_v S\right\}\right| < \infty \qquad \text{(finite zeros).}$$

So f is not regular at only a finite set of places, as as the set of points such that "$f(p) = 0$", i.e. f is in the maximal ideal which makes it zero in the residue field.

Remark 8.1.7: Thinking of f as a rational function, this says that the sets of points which are poles or zeros are both finite.

Proof (of first statement).
If $f \in \kappa(K)$, then both sets are empty, so assume otherwise that f is transcendental. This is because if f is a nonzero constant function, i.e. it is algebraic over k, and both f, f^{-1} lie in all of the valuation rings and none of the maximal ideals. Then the integral closure A of $k[f]$ in K is an affine Dedekind domain containing f.[a] But we're done: for all $v \in \Sigma(K/A)$, we have $f \in R_v$ and thus

$$\Sigma(A, \infty) = \Sigma(K/k) \setminus \Sigma(K/A),$$

which is finite by affine grounding. This is because $\Sigma(K/A)$ already has finite complement, so all but finitely many valuations are A-regular, and $f \in A$. Conversely, if f is nonconstant it can not be regular at all places since it would then lie $\kappa(K)$.

■

[a] Pete's Commutative Algebra, Theorem 18.4 (a normalization theorem).

Proof (of second statement).
Note that $f \in \mathfrak{m}_v \iff v_p(f) > 0 \iff v_p(1/f) < 0 \iff 1/f \notin R_v$, so we can just apply the first statement to $1/f$.

■

Exercise 8.1.8 ***(Function fields are always covered by*** mSpec ***of two affine Dedekind domains (too easy!)):*** Show that there exist A_1, A_2 affine Dedekind domain such that

$$\Sigma(K/k) = \Sigma(K/A_1) \cup \Sigma(K/A_2).$$

Remark 8.1.9: This will follow from a theorem we haven't proved yet. If we think of $\Sigma(K/k)$ as a compact Riemann surface, the theorem is saying that pulling out a single point (or any finite number) then what's left is mSpec(A) for A an affine Dedekind domain. So just pull out two different points.

Remark 8.1.10: The lemma is allowing us to define the divisor of a rational function. We'll define $\operatorname{Div} K$ as the free $\mathbb{Z}$-module with bases $\Sigma(K/k)$. Any divisor will be of the form

$$D = \sum_{p \in \Sigma(K/k)} n_p[p],$$

where all but finitely many of the n_p are zero. If we have a rational function $f \in K^\times$, we'll define

$$\operatorname{Div} f = \sum_{p \in \Sigma(K/k)} v_p(f)[p].$$

How do we know this is well-defined? We need $v_p(f) = 0$ for all but finitely many places p. But $v_p(f) > 0 \implies f \notin \mathfrak{m}_p$, and one part of the lemma said f can only lie in finitely many $\mathfrak{m}_p$. On the other hand, $v_p(f)$ can't be negative, since this would imply $f \notin R_v$.

This is extremely important: the map that sends a rational function to its divisor is multiplicative and additive, so this yields a subgroup of $\operatorname{Div} K$ called the **principal divisors**. The quotient is the **class group** of K, and now we are cooking with gas (as Pete's undergraduate instructor used to say).

Theorem 8.1.11 ***(Strong Approximation).***
Let $X \subsetneq \Sigma(K/k)$ be proper and let $p_1, \cdots, p_r \in X$. Let $\{x_j\}_{j=1}^r \subset K$ and $\{n_j\}_{j=1}^r \subset \mathbb{Z}$. Then there exists a single $x \in K$ such that

$$\forall 1 \leq j \leq r,\ v_{p_j}(x - x_j) = n_j$$
$$\forall p \in X \setminus \{p_j\}_{j=1}^r,\ v_p(x) \geq 0.$$

Remark 8.1.12: Note that X is allowed to be infinite, so the statement only gets stronger if we allow a maximal proper subset where its complement is just a point. If we only had the first statement, this would be *weak approximation*. The conclusion is weaker, but it applies much more generally. One first learns this in NTII, and it applies to any finite set of inequivalent norms on a field. The second statement is a requirement that x is regular. If X were *not* all but one place, we should replace it by that since it'd still satisfy the hypotheses. Enlarging X only makes the conclusion of the second statement stronger, since this is enforcing more integrality conditions.

Proof (?).
Without loss of generality, assume that the complement $\Sigma(K/k) \setminus X = \{p_0\} := S$ is a single place. We know that R^S is an affine Dedekind domain (by a theorem stated but not proved yet), so apply the *Dedekind Approximation Theorem*[a]. ■

[a] Pete's NTII, Proposition 1.17

Remark 8.1.13: Note that Stichtenoth uses Weil's proof of Riemann-Roch to prove this. Too bad he doesn't have several hundred pages of lecture notes to draw on! The difference between weak and strong approximation: weak applies to a finite set of places, and strong applies to all but one place. Later in NTII there's an adelic statement of strong approximation, which works in the more general setting of a linear algebraic group over a global field. You can take the adelic points of that group, remove one place, and ask if strong approximation holds. It turns out to depend on what kind of algebraic group you have.

8.2 Proof of Main Theorem

We return now to the proof of Theorem 8.1.1.

We're trying to show that R^S for S a finite and nonempty set of places is an affine Dedekind domain. So we need to show that it's Dedekind, and that it's finitely generated over a field.

If $\emptyset \subsetneq S_1 \subsetneq S_2$ are finite subsets of $\Sigma(K/k)$, then $R^{S_1} \subseteq R^{S_2} \subset K$. By the structure theory of Dedekind domains, [23] every overring of a Dedekind domain is again a Dedekind domain. This allows us to restrict to the case where $|S| = 1$.

[23] Pete's CA, Section 23.2.

8.2.1 Case 1

We start with the case where K is a one variable function field, since it should certainly be true there. So assume $K = k(t)$. If $S = \{v_\infty\}$ is just the infinite place, then $R^S = k[t]$ from a previous discussion. This is definitely a Dedekind domain, since it's an affine PID.

8.2.2 Case 2

The next case is one place of degree 1, so $S = \{v_{t-a}\}$ corresponds to a monic irreducible polynomial, where we use the fact that the degree of the residue field is the degree of the polynomial. Then $R^S = k\left[\dfrac{1}{t-a}\right]$. This is holomorphic at ∞, since the degree in the denominator is bigger than that of the numerator. So it lies in R_{v_∞} as well as R_{v_q} for every monic irreducible polynomial q except for $t-a$. This is a PID since it's isomorphic to a polynomial ring, and has fraction field K. (?) We certainly have a containment $\supseteq$, but the RHS is already an affine Dedekind domain whose mSpec is everything but this single place. By the theory of overrings, the only other possibility is that the RHS is bigger, but going from a Dedekind domain to a larger Dedekind domain removes elements from mSpec.

8.2.3 Case 3

Now consider the case $S = \{v_p\}$ with $\deg p := d > 1$. This corresponds to a monic irreducible polynomial of degree bigger than 1. Note that $k[t] \cong k[\alpha]$ for any transcendental α, so we can take $k[1/p] \subset R^S$. This is an affine PID, and the containment follows from the fact that $1/p$ is holomorphic at ∞ (for the same reason as above). The only way it could *not* be regular with respect to some polynomial q would be that after cancelling the numerator and denominator, q appears in the denominator, and that happens precisely at p. Now taking fraction fields, we have $\operatorname{ff} k[t] = k(t)$ and $[k(t) : k(1/p)] = d$, the degree of the denominator, which follows from this exercise:

Exercise 8.2.1 ***(Basic but important):*** If $p(t)/q(t) \in k(t)$ is a nonconstant rational function, then what is the degree $d := [k(t) : k(p/q)]$? Show that $d = \max\{\deg p, \deg q\}$.

So $k[1/p] \subset R^S$ must be proper, since $\operatorname{ff}(R^S) = K$ but $\operatorname{ff}(k[1/p])$ is a proper extension. We can't have equality, so instead let A be the integral closure of $k[1/p]$ in $k(t)$. Then A is a Dedekind domain with $\operatorname{ff}(A) = k(t)$ and $\operatorname{mSpec}(A) = \Sigma(k(t)/k) \setminus \{v_p\}$ from the following NTI square:

$$\begin{tikzcd} A \arrow[r, hook, "\subseteq"] & k(t) \\ k[1/p] \arrow[u, hook] \arrow[r, hook, "\subseteq"] & k(1/p) \arrow[u, hook] \\ k \arrow[u, dash] & \end{tikzcd}$$

Link to diagram

By affine grounding, we know $k[1/p]$ is an affine Dedekind domain, and by the second normalization theorem we know that A is finitely generated as a module over $k[1/p]$, which is in turn finitely generated as an algebra over k, making A a finitely generated k-algebra. The key ingredient in identifying $\operatorname{mSpec}(A)$ is that $1/p \in A$. By a previous exercise, we can conclude that A is a holomorphy ring, and since we know the exact excluded set is S, we can conclude $A = R^S$. This makes A an affine Dedekind domain.

For the final case, suppose S is finite and nonempty. Choose $v \in S$ and define $S_1 := \{v\}$. Then $R^{S_1} \subseteq R^S \subset K$, so R^S is a Dedekind domain since it's an overring of a Dedekind domain. A surprising fact is that $A := R^S$ is not a PID when the degree is greater than 1, and instead $\operatorname{cl}(A) \cong \mathbb{Z}/d\mathbb{Z}$ and is thus torsion. It'll be enough to show that R^S is finitely generated as an algebra (but not a module?) over R^{S_1}, which will make it a finitely generated k-algebra, and we'd really like it to be a localization. We examined this before: is every overring of a Dedekind domain a localization? A theorem of Clayborne shows that this is true when the class group is torsion.

Let $v_2 \in S \setminus S_1$, so that every such v_2 yields an ideal $\mathfrak{p}_{v_2} \in \operatorname{mSpec} R^{S_1}$. Since $\operatorname{cl}(R^S) = \mathbb{Z}/d\mathbb{Z}$, we don't know that $\mathfrak{p}_{v_2}$ is principal, but we do know that $\mathfrak{p}_{v_2}^\alpha$ is for some power α Note that localization is forgiving in the sense that inverting an element x is equivalent to inverting any power x^k (e.g. using that $1/x = x^k/x^{k+1}$). So we can write $\mathfrak{p}_{v_2}^\alpha = \langle f \rangle$, and it follows that $R^{\{v,v_2\}} = R_v[1/f]$ is an affine domain which is obtained by localizing f. Note that we can think of this overring as puncturing or removing one place (a certain maximal ideal) at a time, i.e. intersecting over all of the maximal ideals except one in order to go from $R^{S_1} = R^{\{v_1\}}$ to $R^{\{v_1,v_2\}}$. You can continue this inductively using the fact that $R_v[1/f]$ is a different Dedekind domain – since it's an overring, the corresponding class group is a quotient and thus still torsion. You could also continue this inductively by just puncturing one point at a time. You can also do it all at once: for each element in S not equal to v_1, obtain an f_j, and invert the product $\prod_j f_j$.[24]

Key fact: We're in a lucky situation where we don't have a PID, but we have a torsion class group. Anytime you pass to an overring by puncturing finitely many maximal ideals, it will always be a localization and thus monogenic as an algebra over the smaller Dedekind domain.

[24] Alternatively, see Pete's Commutative Algebra, Corollary 23.6.

8.3 Case 3: Fixed Proof

The remainder of the proof will go toward reducing to the first step of a function field and exactly one place. We'll apply the Riemann-Roch theorem, however this does not rely on results on holomorphy rings, so there's no logical circularity. As usual, we lose no generality by replacing k with $\kappa(K)$ and just assuming that $\kappa(k) = k$.

Let $S \subset \Sigma(K/k)$ be finite and nonempty. Then by Riemann-Roch there exists an $f \in K^\times$ having poles precisely at the elements of S, i.e. f is regular away from S.

> Recall that poles were defined as elements not in R_v. This is motivated by considering meromorphic functions f on $\mathbb{C}$, then the order of vanishing of f at p is a discrete valuation, and if that valuation is negative then p is a pole.

Note that we're specifying the poles but not their orders, and allowing poles of arbitrary orders would still allow us such a rational function by a result like the Riemann inequalities, which is easier to prove than the Riemann-Roch theorem. You can also obtain such a function from the Strong Approximation theorem.

Since f has poles, it's nonconstant, so we have a nontrivial map $r : \Sigma(K/k) \to \Sigma(k(f)/k)$ to a rational function field and thus $r^{-1}(\infty) = S$ since the poles all like above the place at ∞. The analogy here is a holomorphic function f from a compact Riemann surface to $\mathbb{P}^1_{/\mathbb{C}}$, in which case $f^{-1}(\infty)$ is the set of poles. Since $k[f]$ is a polynomial ring, we can take the integral closure of $k[f]$ in K, say B, in which case B is an affine Dedekind domain and $\mathrm{mSpec}(B) = \Sigma(K/k) \setminus S$.

The picture is as follows: think of $k(f)$ as the Riemann sphere with the point ∞ and $\Sigma(K/k)$ as a Riemann surface above it, then S is the preimage of ∞.

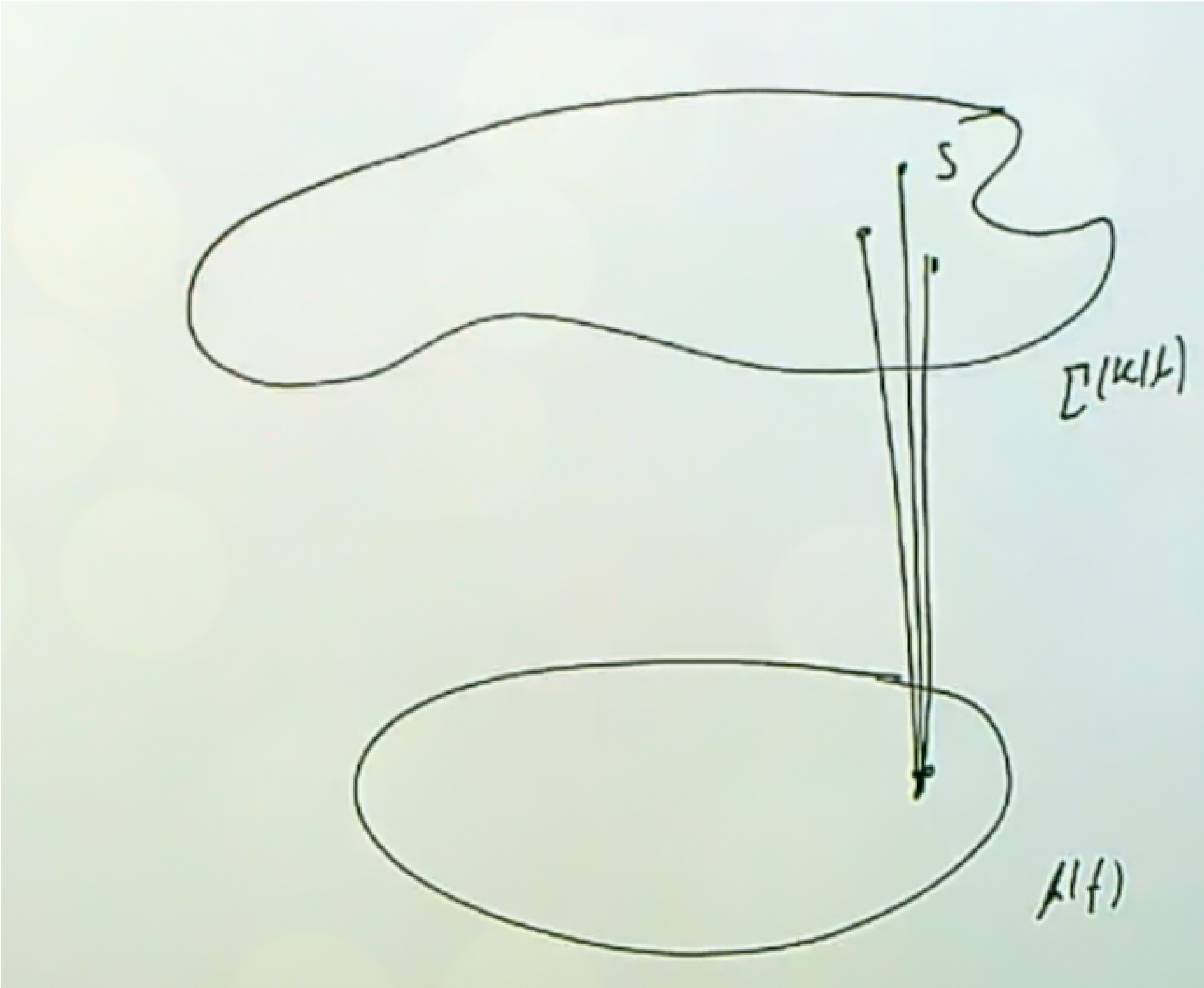

Figure 4: Image

If you have an upstairs valuation $v \in \Sigma(K/k)$ in an integral extension, then it is regular upstairs iff its restriction downstairs is regular. Completing the NTI square yields

$$\begin{tikzcd}
B \arrow[r, hook, "\subseteq"] & K \\
k[f] \arrow[u, hook, "\subseteq"] \arrow[r, hook, "\subseteq"] & k(f) \arrow[u, hook, "\subseteq"]
\end{tikzcd}$$

Link to diagram

Here B is the integral closure. So if we take a valuation in K, it is B-regular iff its restriction to $k(f)$ is A-regular. But R_v contains $k[f]$ iff it contains f, since it's already a k-valuation, so the non-regular valuations are those that restrict to ∞.

Now if you have an extension of Dedekind domains, then the maximal ideals upstairs are everything which restricts to a finite place downstairs. So those that don't restrict to a finite place restrict to ∞, which is precisely the preimage of ∞. With the identification of $\mathrm{mSpec}(B) = \Sigma(K/k) \setminus S$,we have $B \subset R^S$ since every valuation in the complement of S is regular at B by this argument. Since $B \subset R^S \subset K$, we can use the classification of overrings of Dedekind domains, and the mSpec corresponds to precisely the maximal ideals that are being intersected. The only way this could be a *proper* extension would be if the mSpec shrank, but then R^S would be the holomorphy ring attached to a larger set than S. So we obtain an equality.

■

9 Lecture 7: Riemann-Roch

9.1 Divisors

Definition 9.1.1 (Divisor group)
The **divisor group** $\mathrm{Div}\, K$ is the free $\mathbb{Z}$-module with basis $\Sigma(K/k)$, so

$$\mathrm{Div}\, K := \bigoplus_{p \in \Sigma(K/k)} \mathbb{Z}.$$

Thus every $D \in \mathrm{Div}\, K$ is of the form $D = \sum_{p \in \Sigma(K/k)} n_p p$ where $n_p \in \mathbb{Z}$ and are almost all zero, recalling that a point $p \in \Sigma(K/k)$ is an equivalence class of valuations.

Definition 9.1.2 (Effective Divisor)
A divisor $D = \sum n_p p$ is **effective** iff $n_p \geq 0$ for all p and write $D \geq 0$.

Definition 9.1.3 (Support of a divisor)
The **support** of a divisor D is the set of places $p \in \Sigma(K/k)$ such that $n_p(D) \neq 0$. Note that this is always a finite set, and the zero divisor is the unique divisor supported on $\emptyset$.

Definition 9.1.4 (Partial order on divisor)
We write $D_1 \leq D_2$ iff $D_2 - D_1 \geq 0$ is effective. Note that this holds iff for all places $p \in \Sigma(K/k)$, if $D_1 = \sum_p m_p p$ and $D_2 = \sum_p n_p p$, then $m_p \leq n_p$ for all p.

This is a partially ordered commutative group, which came up when we were talking about groups of divisibility. It's a reasonable group when studying domains with nice factorization properties: if

R is a UFD with a set of principal prime ideals[25] denoted $\Sigma(R)$, then the group of divisibility $G(R)$ is isomorphic to $\bigoplus_{(p)\in\Sigma(R)} \mathbb{Z}$ as a partially ordered commutative group.

There is an analogy: comparing UFDs to Dedekind domains, we trade unique factorization of elements for factorization of ideals, and the group of all fractional ideals in a Dedekind domain is a free commutative group on its set of prime ideals. So $\operatorname{Div} K$ is analogous to the group of divisibility of a UFD and to the group of fractional ideals of a Dedekind domain, the latter of which is the closer analogy. So $\operatorname{Div} K$ is a geometric or projective analog of the group of fractional ideals, and is more than an analogy as we'll see later.

Definition 9.1.5 (Degree of a Divisor)
There is a group morphism

$$\begin{aligned} \deg : \operatorname{Div} K &\to \mathbb{Z} \\ D = \sum_p n_p p &\mapsto \sum_p n_p \deg p. \end{aligned}$$

Its kernel is denoted $\operatorname{Div}^0 K$, the **degree zero divisors**. Note that if $k = \bar{k}$, then $\deg p = 1$ for all p.

Remark 9.1.6: Note that this is similar to the augmentation in a group ring. This construction can be done with any free $\mathbb{Z}$-module, and makes sense because only finitely many terms are nonzero. Recall that to define the degree of a place $v \in \Sigma(K/k)$, we consider $R_v := \left\{x \in K \;\middle|\; v(x) \geq 0\right\}$ and $\mathfrak{m}_v := \left\{x \in K \;\middle|\; v(x) > 0\right\}$, and $k(v) := R_v/\mathfrak{m}_v$ is the residue field. Note that $k(v)$ is a field extension of k by composing $k \hookrightarrow R_v \twoheadrightarrow k(v)$, and we proved used affine grounding and Zariski's lemma that this was a finite degree extension. We can then define $\deg v := [k(v) : k]$. Note that it's more natural to think of valuations v as points p.

Definition 9.1.7 (Index of a divisor)
The **index** of K is defined as

$$I(K) := |\operatorname{coker} \deg|.$$

[a]

[a] This quantity made an appearance near the end of Pete's advanced course on elliptic curves.

Remark 9.1.8: Note that $I(K)$ is nonzero, since we can think of $p \in \operatorname{Div} K$ as the divisor with $n_q = \mathbb{1}[q = p]$, so the image contains a subset consisting of all degrees of all places, so the image is of the form $d\mathbb{Z}$ for some d. Some other characterizations:

- $\deg(\operatorname{Div} K) = I(K)\mathbb{Z}$, so $I(K)$ is the generator of the degree ideal.
- $I(K)$ is the least positive degree of a divisor on K.
- $I(K) = \gcd\left(\left\{\deg p \;\middle|\; p \in \Sigma(K/k)\right\}\right)$, i.e. the gcd of the closed points.

[25] Note that primes in a UFD are principal.

The last characterization follows because we have generators of Div K given by "skyscraper" divisors p where $n_q = 1 \iff p = q$, so the image is the subgroup of $\mathbb{Z}$ generated by the degrees of the points, i.e. the gcd of the degrees.

Exercise 9.1.9 ***(?):*** Let K/k be a one variable function field.

a. Show that if $\Sigma_1(K/k) \neq \emptyset$ then $I(K) = 1$.

b. Later we will show that if $|k| < \infty$ then $I(K) = 1$ but $\Sigma_1(K/k)$ may be empty. Try to show this.

c. Show that if $k = \bar{k}$ then $I(K) = 1$.

Remark 9.1.10: (a) follows from the Riemann hypothesis for curves over a finite field, although this is not how you should prove it. It was proved by F.K. Schmidt much earlier in the 20th century, and this is the basic way of understanding the zeta function of a curve.
(b) says that over a finite ground field, you may not have any degree 1 places. You can try constructing a hyperelliptic curve over a finite field $\mathbb{F}_q$ with no rational points, which is always possible if the genus is large compared to the size of $\mathbb{F}_q$.

Lemma 9.1.11 ***(?).***
For a nonzero rational function $f \in K^\times$ we have $v_p(f) = 0$ for almost every place $p \in \Sigma(K/k)$.

Proof (?).
See previous lecture, in particular Lemma 8.1.6. ■

This says that the set of places for which the valuation is nonzero is finite, so except for finitely many places the valuation is zero. This allows us to define the divisor of a rational function:

$$\begin{aligned} (\,\cdot\,) : K^\times &\to \operatorname{Div} K \\ f &\mapsto (f) := \sum_p v_p(f) p, \end{aligned}$$

which is a group morphism.

Exercise 9.1.12 ***(?):*** Show that $(f) = 0 \iff f \in \kappa(K)$, which we're assuming is equal to k. This happens when it has neither zeros nor poles, so it's an intersection of all of the R_v, which is the integral closure of k in K. In general, this would mean that f is algebraic over k. So $\ker(\,\cdot\,) = k^\times$.

Definition 9.1.13 (Poles and Zeros of Elements of K)
For any $D \in \operatorname{Div} K$ one may uniquely write it as $D = D_+ - D_-$, which are both effective divisors and so $D_+, D_- \geq 0$, and the uniqueness follows from requiring $\operatorname{supp}(D_+) \cap \operatorname{supp}(D_-) = \emptyset$. Note that this is just collecting positive and negative n_p into each term, and leaving out all divisors for which $n_p = 0$.
For $f \in K^\times$, we define

$$\begin{aligned} (f)_+ &:= \text{the divisor of zeros of } f \\ (f)_- &:= \text{the divisor of poles of } f, \end{aligned}$$

where we can note that $(f) = (f)_+ - (f)-$.

The next proposition shows that these geometric divisors can be interpreted in terms of $\mathbb{F}_q$ points.

Proposition 9.1.14 ***(?).***
Let $f \in K \setminus k$ be transcendental.

a. Let B_0 be the integral closure of $k[f]$ in K, which is an affine Dedekind domain of K, i.e. its fraction field is K.[a]

Then

$$fB_0 = \prod_{j=1}^{r} p_j^{a_j} \implies (f)_+ = \sum_{j=1}^{r} a_j p_j.$$

b. Let B_∞ be the integral closure of $k[1/f]$ in K, which is an affine Dedekind domain of K. Then

$$\left(\frac{1}{f}\right) B_\infty = \prod_{j=1}^{s} q_j^{b_j} \implies (f)_+ = \sum_{j=1}^{s} b_j q_j.$$

[a] As usual for an extension of Dedekind domains, we push forward an ideal (maybe principal) into its integral closure and see how it factors.

Exercise 9.1.15 ***(?):*** Prove this proposition.

Remark 9.1.16: This says that pushing forward an ideal and looking at the factorization is precisely what's needed to determine the divisor of zeros. There aren't many new ideas for this proof, the point is that the set of places upstairs is being controlled by mSpec of Dedekind domains.

Slogan 9.1.17: In any affine coordinate chart, the divisor of a function is a principal fractional ideal.

9.2 The Degree of the Divisor of a Rational Function is Zero

Corollary 9.2.1 ***(Excruciatingly Important: the degree of the divisor of any rational function is zero.).***
Let $f \in K \setminus k$ be transcendental, then

a. $\deg(f)_+ = [K : k(f)] = \deg(f)_-$

b. $\deg(f) = 0$.

Remark 9.2.2: Here think of f as a holomorphic map from a curve to $\mathbb{P}^1_{/\mathbb{C}}$, and the degree of this extension is the degree of the corresponding branched cover. For $\mathbb{C}$, this is literally the cardinality of any finite fibers. Note that (a) follows by symmetry sense $k(f) \cong k(1/f)$.

Proof (?).
This comes down to NTI. We know $\deg(f)_+ = \sum j = 1^r a_j \deg p_j$. In $K/k(f)$, the places $p_1, \cdots, p_r$ all lie over the degree 1 place v_f of $k(f)$. The places where upstairs you have a zero are the places where to coordinate downstairs is equal to zero, which corresponds to the irreducible polynomial in f given by f itself. Since the residue field at v_f downstairs is k itself, since it is $k[f]/\langle f\rangle$. So the downstairs places has degree 1, and so the degree of the upstairs places, whatever the residue field is, its degree over k is equal to its degree over the downstairs residue field. Thus the geometric $\deg p_j$ coincides with the residual degree f_i, and a_i is the ramification index in the extension of Dedekind domains $B_0/k[f]$.

So we have a degree equality,

$$\sum_{j=1}^{r} a_j \deg p_j = \sum e_j f_j = [K : k(f)],$$

where the second equality follows from having an extension of Dedekind domains with this nice finite generation hypothesis. We similarly get $[k : k(f)] = \deg(f)_-$.

Note that part (b) follows immediately, since $(f) = (f)_+ - (f)_-$ implies that

$$\deg(f) = \deg(f)_+ - \deg(f)_- = [k : k(f)] - [k : k(f)] = 0.$$

■

Remark 9.2.3: We have two different things that sound like the degree of a rational function. We define the degree of a rational function $f \in K \setminus k$ as $[K : k(f)]$, otherwise it is the degree (number of sheets) of the corresponding branched covering of $\mathbb{P}^1$. But note that we also attached a divisor to f, which may be confusing, be hard to confuse in practice because we found that $\deg(f) = 0$ always.

Definition 9.2.4 (Principal Divisors)
The divisor of a rational function is called **principal**, we define $\operatorname{Prin} K$ to be the group of principal divisors.

Exercise 9.2.5 *(*$\operatorname{Prin} K$ ***is a group*****):** For $f, g \in K^\times$, show that

a. $(1/f) = -(f)$,

b. $(fg) = (f) + (g)$,

c. $\operatorname{Prin} K \leq \operatorname{Div}^0 K$ is a subgroup (since we know they're degree zero).

Definition 9.2.6 (Linear Equivalence)
For $D_i \in \operatorname{Div} K$, we set $D_1 \sim D_2 \iff D_1 - D_2 \in \operatorname{Prin} K$, in which case we say these divisors are **linearly equivalent**.

Remark 9.2.7: Near the end of the course we'll see why this is good terminology: it's related to morphisms of projective space attached to linear systems.

Definition 9.2.8 (Divisor Class Group)
We define the **divisor class group** as

$$\operatorname{cl} K := \operatorname{Div} K/\sim = \operatorname{Div} K/\operatorname{Prin} K.$$

But note that there's something between $\operatorname{Prin} K$ and $\operatorname{Div} K$, namely $\operatorname{Div}^0 K$:

Definition 9.2.9 (Degree 0 Divisor Class Group (Important! Fundamental!))
We define the **degree 0 divisor class group** as

$$\operatorname{Cl}^0 K := \operatorname{Div}^0 K/\sim = \operatorname{Div}^0 K/\operatorname{Prin} K.$$

Remark 9.2.10: This is extremely important! Attached to a curve is a Jacobian abelian variety, a nice group variety whose dimension is equal to the genus of the curve, and the k-rational point of the Jacobian will become a commutative group that is isomorphic to $\operatorname{Div}^0 K$.

Exercise 9.2.11 ***(?):*** Show that we have the following exact sequences:

a.
$$1 \to k^\times \to K^\times \xrightarrow{(\cdot)} \operatorname{Prin} K \to 0.$$

b.
$$0 \to \operatorname{Cl}^0 K \to \operatorname{Cl} K \xrightarrow{\deg} I(K)\mathbb{Z} \to 0.$$

Deduce that $\operatorname{Cl} K \cong \operatorname{Cl}^0 K \oplus \mathbb{Z}$.

Remark 9.2.12: For (a), we saw that rational functions that have zero divisors are constants, assuming that $\kappa(K) = k$. For (b), because principal divisors have degree zero, the degree map factors through the quotient. The deduction comes from that fact that we have a free and hence project $\mathbb{Z}$-module, yielding a splitting.

Exercise 9.2.13 ***(Very important, Pete insists that someone solves it!):***

a. Show that $\operatorname{Div}^0 k(t) = \operatorname{Prin} k(t)$.

b. Deduce that $\deg : \operatorname{Cl} k(t) \xrightarrow{\sim} \mathbb{Z}$ and $\operatorname{cl}^0 k(t) = 0$.

Remark 9.2.14: Note that $I(K) = 1$ in this case since both the t-adic or ∞-adic valuation have degree one. Moral: the class groups are not interesting on rational function fields. You have to take a degree zero divisor on a rational function field and build a rational function whose divisor is any given degree. This is extremely useful!

Remark 9.2.15: More general if K/k has genus zero (e.g. a rational function field), then working over $\mathbb{C}$ we would have $\operatorname{Cl}^0 K$ equal to the points of some compact complex Lie group of $\mathbb{C}$-dimension g, so a large complex torus, unless $g = 0$. So if $k = \bar{k}$, $\operatorname{Cl}^0 K$ will be uncountably infinite when $g > 0$. If not, it might trivial, or it might be anything in between.

The following result appears in a 1973 paper of Rosen, where he attributes it to F. K. Schmidt. It gives a close relationship between $\mathrm{Cl}^0 K$ and the class groups $\mathrm{Cl}\, R^S$ of the affine Dedekind domains of K. This shows that instead of $\mathrm{Cl}^0 K$ just being an analogue of the class group of a Dedekind domain, there's almost the same. If you fix K, $\mathrm{Cl}^0 K$ is just one group attached to it, but there are infinitely many R^S since there are infinitely many places. So these groups can not be equal, since we could change the size of S to obtain overrings of Dedekind domains, where the resulting class groups are quotients. So you could kill finitely many elements in the class group of the Dedekind domain by just passing to an overring by adding finitely more places.

Theorem 9.2.16 ***(Rosen).***
Let $S \subset \Sigma(K/k)$ be nonempty and finite, and recall that the holomorphy ring was defined as

$$R^S = \cap_{v \in \Sigma(K/k)} R_v.$$

Define the following:

- $D^0(S)$: the degree 0 divisors with support in S.
- $P(S) := \mathrm{Prin}\, K \cap D^0(S)$, the principal divisors supported in S.
  - Divisors of rational functions all of whose zeros and poles lie in S.
- d_S: The least positive degree of a divisor supported on S.
  - Note that this is different to the index in that we restrict to S, and is thus a multiple of $I(K)$.

Then there is an exact sequence

$$0 \to D^0(S)/P(S) \xrightarrow{\iota} \mathrm{Cl}^0 K \xrightarrow{\alpha} \mathrm{Cl}\, R^S \xrightarrow{\beta} C(d/I(K)) \to 0.$$

Proof (?).
See NTII, Theorem 3.27. ■

Remark 9.2.17: Note that the kernel $D(S)/P(S)$ could be infinite but is always finitely generated. The map α is induced by

$$\begin{aligned} \alpha' : \mathrm{Div}\, K &\to \mathrm{Frac}\, R^S \\ \sum n_p p &\mapsto \prod_{p \in \mathrm{mSpec}\, R^S} p^{n_p}, \end{aligned}$$

where we note that $\mathrm{mSpec}\, R^S \subset \Sigma(K/k)$, and in fact $\Sigma(K/k) = \mathrm{mSpec}\, R^S \coprod S$. We can do this because if p is already in $\mathrm{maxSpec} R^S$, we raise it to an appropriate power, and otherwise, for the finitely many $p \in S$ we just get rid of them. But this kills of some elements, namely those things supported in S, hence the kernel in the exact sequence.

Note that the last group appearing is finite cyclic of order $d/I(K)$. If you just looked at $D^0(S)$ before modding out by principal divisors, if you didn't impose degree zero, the subgroup would be isomorphic to $\mathbb{Z}^{|S|}$. But there's a linear condition that the degree is equal to zero, which cuts down the dimension by 1, yielding $\mathbb{Z}^{|S|-1}$. It's hard to say how much $P(S)$ is cutting down the size.

Remark 9.2.18: The moral is that there is a map, but the kernel and cokernel both depend on S. If you understand $\operatorname{Cl}^0 K$, however, you have a good handle on all $\operatorname{Cl} R^S$.

Exercise 9.2.19*(?)*:

a. Show that $D^0(S) \cong \mathbb{Z}^{|S|-1}$.

b. Suppose S consists of a single place whose degree is the quantity d_S appearing in the previous theorem, the least positive degree of a divisor supported on S. Show that there is an exact sequence

$$0 \to \operatorname{Cl}^0 K \xrightarrow{\alpha} \operatorname{Cl} R^S \xrightarrow{\beta} C(d_S/I(K)) \to 0.$$

c. Deduce that α is an isomorphism iff $I(K) = d$.

d. Deduce that if $p \in \Sigma(k(t)/k)$ has degree d, then $\operatorname{Cl} R^{\{p\}} \cong \mathbb{Z}/d\mathbb{Z}$.

e. Deduce that if $S = \{p\}$ and $\deg p = 1$, then $\alpha : \operatorname{Cl}^0 K \to \operatorname{Cl} R^S$ is an isomorphism.

Remark 9.2.20: Note that if you're given a finite set of places and ask for all of the rational functions that have zeros and poles only at those places, it is difficult to determine how close that is to filling out the entire degree zero divisor class group? If you have two degree 1 points p_i, so $|S| = 2$, do you have a rational function whose divisor is $p_1 - p_2$? Probably not, because then the divisor of such a function would have degree 1. You can continue this line of thought, but already using elliptic function fields you can see that all of these algebraic possibilities can occur.

Remark 9.2.21: Note that in the case where S is a single point of degree d, then d_S is equal to the degree of the point d. On the other extreme, consider what happens when $I(K) = 1$. Then $C(d_S)$ is cyclic of order d, so in (c) if we have a rational function field, we know it has degree 1 places (like $0, \infty$), and the class group is zero. So if you take one place on $\mathbb{P}^1$ of degree d and look at the correspond affine Dedekind domain of functions that are regular away from that one place $R^{\{p\}}$, then the class group is nontrivial and it's thus not a PID. Note that $\operatorname{Cl}^0 \mathbb{P}^1$ is trivial, and puncturing it has an effect on the divisor class.

Exercise 9.2.22*(?)*:

a. Suppose $\operatorname{Cl}^0 K$ is finite, and show that every $\operatorname{Cl} R^S$ is finite. [26]

b. Suppose $\operatorname{Cl}^0 K$ is finitely generated, and show that for all finite nonempty $S \subset \Sigma(K/k)$, there exists a finite $S' \supset S$ such that $\operatorname{Cl} R^{S'}$ is trivial.

Remark 9.2.23: This is the positive characteristic version of one of the basic finiteness theorems from NTI: the ring of integers of any number field has finite class group. But the S-class group is always finite, since it's a quotient of the class group, and that's what's happening here. It's enough to show that the $\operatorname{Cl}^0 K$ and $C(d_S/I(K))$ appearing in the SES in the previous theorem are finite,

[26] Later we will show that $\operatorname{Cl}^0 K$ is finite when k is finite.

since the first term can only cut down the size. The groups $\operatorname{Cl} R^S$ when k is finite are analogues of the S-class groups of number fields. In the function field case, you can't get away from the S-class group, since if $S = \emptyset$ then R^S is not an interesting Dedekind domain: it's just $\kappa(K)$. So you have to put something at ∞ to even get a 1-dimensional domain, whereas in the number field case, you always have a finite nonempty set of nonarchimedean places.

This allows us to deduce from the finiteness of this one geometric group the finiteness of S-class groups in the characteristic p case. If done correctly, this can be used to prove the finiteness of class groups of all number fields, e.g. if you do things in an adelic way in NTII.

Theorem 9.2.24 ***(Trotter, 1988).***
The ring $R[\cos\theta, \sin\theta]$ of real trigonometric polynomials is not a UFD, while $\mathbb{C}[\cos\theta, \sin\theta]$ is a PID.

Remark 9.2.25: Trotter shows that using $\sin(\theta)\sin(\theta) = (1+\cos(\theta))(1-\cos(\theta))$ exhibits non-unique factorization, since the terms appearing are non-associate irreducible elements in an integral domain. See Pete's list of exercises. Note that given an affine Dedekind domain how one figures out what the infinite places are concretely, but this will come up when discussing hyperelliptic curves.

Remark 9.2.26: One exercise applies Rosen's theorem to show that $\operatorname{Cl}\mathbb{R}[\cos(\theta), \sin(\theta)] = \mathbb{Z}/2\mathbb{Z}$ while $\operatorname{Cl}\mathbb{C}[\cos(\theta), \sin(\theta)] = 1$. What's happening is that over $\mathbb{R}$, there is perhaps one degree 2 place at ∞, but after extending scalars to $\mathbb{C}$ it breaks up into two degree 1 places.

10 | Lecture 8: Riemann-Roch Spaces (Part 1)

10.1 Setup for the Riemann-Roch Theorem

Setting up for the single most important theorem in the course: the Riemann-Roch theorem. We start by motivating this by considering the following property of $K := k(t)$: for any degree 1[27] place $p \in \Sigma(K/k)$, there exists an $f \in K^\times$ such that $(f)_- = p$. In other words, f is a rational function with a simple pole at the given place, and no other poles. Why? We just know precisely what all of the places are for this function field.

If $p = \infty$, we can just take $f(t) = t$, since any polynomial is regular away from ∞ and the valuation is $-\deg(f) = -1$ The other places p correspond to $t - \alpha$ (the uniformizing element) for $\alpha \in k$, since they correspond to other points on $\mathbb{A}^1_{/k}$, and so we can take $f(t) = 1/(t-\alpha)$. This f is regular at infinity since the degree of the numerator is larger than the degree of the denominator, and the denominator doesn't vanish at any other place.

Remark 10.1.1: With some thought, it can be found that this is a *characteristic* property of rational function fields: if $f \in K$, a one variable function field, and $\deg(d)_- = 1$[28] then the degree

[27] So the residue field of the corresponding DVR is k itself rather than some proper finite degree extension.
[28] Recall that this is the divisor pole.

of the function is equal to the degree of the divisor of the zeros and the divisor of the poles, and thus the degree of the extension $[K : k(t)] = 1$ and thus $K = k(t)$ is rational. So having a rational with a simple pole at only one point *only* happens in you're in a rational function field.

On the other hand, we both wanted and used in our discussion of holomorphy rings the fact that given a nonempty finite subset $S \subset \Sigma(K/k)$, we want to find a rational function $f \in K^\times$ has poles at all of the points in S, so $\operatorname{supp}(f)_- = S$. Better yet, we'd like a bound on the degree of any such f, i.e. the orders of all of these poles. If S is a single place, unless the function field is rational, we can't require the function to have a pole of degree 1 at that point. But can it admit a pole of degree at most 10, for example? This is what motivates the Riemann-Roch spaces and the Riemann-Roch theorem. If you're trying to give a quantitative bound on how high of an order of a pole you have to allow in order to have a rational function, this comes from a key invariant called the *genus* of the function field. The theorem that will tell us about the existence of rational functions with poles of prescribed degrees in terms of the genus is precisely the Riemann-Roch theorem, so that's where we are headed.

10.2 The Riemann-Roch Space

Definition 10.2.1 (Riemann-Roch Space of D (Key Definition))
For $D \in \operatorname{Div} K$, the **Riemann-Roch space** of D is defined as

$$\mathcal{L}(D) := \left\{ f \in K^\times \;\middle|\; (t) \geq -D \right\} \cup \{0\}.$$

Remark 10.2.2: This will turn out to be a k-vector space, and is a sub k-vector space of K. One of the first things we'll prove is that it's always finite dimensional. This is only interesting when D is linearly equivalent to an effective divisor, so we should think of D as having a nonnegative degree, and in fact itself being an effective divisor. So this is the space of rational functions that have prescribes poles of a prescribed order.

Question 10.2.3: Does $\mathcal{L}(D)$ contain any rational functions other than zero?

Answer 10.2.4: For any nonzero $f \in \mathcal{L}(D)^\bullet$, the divisor $D + (f)$ is effective, since $(f) \geq -D$, and also linearly equivalent to D. If D is not linearly equivalent to an effective divisor, this is just the zero vector space.

Exercise 10.2.5 ***(?):*** Let $K = k(t)$ and $n \in \mathbb{Z}^{\geq 0}$. Show that

$$L(n\infty) = \left\{ f \in k[t] \;\middle|\; \deg f \leq n \right\}$$

and in particular is a k-vector space of dimension $n + 1$.[29]

Remark 10.2.6: Note that ∞ is a degree 1 place, and multiplying it by n yields an effective divisor. The Riemann-Roch space here is comprised of rational functions that regular away from ∞, which are polynomials, whose pole at ∞ has order at worst n. But the order of a pole at infinity is its

[29] Recall that ∞ is the $1/t$-adic place.

degree as a polynomial, since the ∞-adic valuation is the negative degree, so this yields polynomials of degree at most n.

10.3 Working with Divisors

Lemma 10.3.1 *(?)*.
For $D \in \operatorname{Div} K$,

$$\mathcal{L}(D) \neq \{0\} \iff 0 \text{ is equivalent to an effective divisor.}$$

Proof (?).
$\implies$: If $f \in \mathcal{L}(D)^\bullet$, then $D + (f)$ is effective and linearly equivalent to zero.
$\impliedby$: If $D' \geq 0$ and $D' \sim D$, then $D' = D + (f) \geq 0$. So $(f) \geq -D$ and thus $f \in \mathcal{L}(D)$. ∎

Example 10.3.2 *(?)*: $\mathcal{L}(0) = \left\{ f \;\middle|\; (f) \geq 0 \right\} \cup \{0\}$, which consists of rational functions with no poles (so their divisor is the zero divisor), and thus $\mathcal{L}(0) = \kappa(K)$. I.e., these are the constants: they are regular everywhere and have no zeros or poles. We would like this space to have k-dimension 1, so we impose $\kappa(K) = k$.

Exercise 10.3.3 *(?)*:

a. Show that for all D, $\mathcal{L}(D) \in \mathrm{Vect}_k$.
b.

$$D \sim D' \implies \mathcal{L}(D) \cong_{\mathrm{Vect}_k} \mathcal{L}(D').$$

Remark 10.3.4: You can frame the above as taking rational functions with poles of certain orders, and analyzing the orders of poles of their sums. If you take D' and write it as $D + (f)$ for f a rational function, then f should produce this isomorphism. The moral: $\mathcal{L}(D)$ only depends on the linear equivalence class of D.

Exercise 10.3.5 *(?)*: Let $D \in \operatorname{Div}^0 K$ be a degree zero divisor, then TFAE:

a. $\dim \mathcal{L}(D) \geq 1$
b. $\dim \mathcal{L}(D) = 1$,
c. D is principal, i.e. the divisor of a rational function or linearly equivalent to zero.

Slogan 10.3.6: The only way a degree zero divisor can have a nontrivial Riemann-Roch space is if it's linearly equivalent to zero.

10.4 Subspaces and Dimension of Riemann-Roch Spaces

Lemma 10.4.1 *(?).*
Let $A \leq B^a$ in $\operatorname{Div} K$, then

a. $\mathcal{L}(A) \leq_{\mathrm{Vect}_k} \mathcal{L}(B)$ is a subspace,
b. $\dim \mathcal{L}(B)/\mathcal{L}(A) \leq \deg B - \deg A = \deg(B - A)$.

[a] These are formal linear combinations of places, so the coefficients in front of each place in A should be less than the corresponding coefficient for B, or equivalently $B - A$ is effective.

Remark 10.4.2: Since $B \geq A$, you can think of this as starting with A and adding an effective divisor to get B, namely $A + (B - A) = B$. How much does that decrease the dimension of the Riemann-Roch space? At most, by the degree of $B - A$ as a divisor.

Corollary 10.4.3 *(?).*
For $D \in \operatorname{Div} K$,

a. If $\deg D < 0$ then $\mathcal{L}(D) = 0$.
b. If $\deg(D) \geq 0$ then $\dim_k \mathcal{L}(D) \leq \deg(D) + 1 < \infty$.

Remark 10.4.4: This shows that Riemann-Roch spaces are always finite dimensional, and also gives a simple upper bound on that dimension.

Proof (of corollary).
For (a), a divisor of negative degree is not linearly equivalent to an effective divisor, so we might as well assume it's effective.
For (b), the dimension of $\mathcal{L}(D)$ doesn't change if D is replaced by a linearly equivalent divisor, so wlog assume D is effective. Now write $D = \sum_{i=1}^{r} p_i$ as a sum of not necessarily distinct places, and use the lemma: each time you add an effective divisor, the dimension either stays the same or increases by at most the degree of the added divisor. So start with the zero divisor, use the fact that $\dim_k \mathcal{L}(0) = 1$, and apply the lemma r times. This yields a space of dimension at most $1 + \sum \deg p_i = \deg D$.

■

Proof (of lemma, part (a)).
If $A \leq B$ and $f \in \mathcal{L}(A)$, then $(f) \geq -A$. Since $-A \geq -B$, we have $(f) \geq -A \geq -B$, so $f \in \mathcal{L}(B)$.

■

For the next part, it's perhaps easiest to consider the case $k = \bar{k}$ so everything has degree 1. If you go from a divisor to adding a single degree 1 place, this lemma says that if you increase your Riemann-Roch space by either allowing a pole at a point you didn't allow before or allowing a pole of order 1 greater, then the dimension increases by at most 1.

Proof (of lemma, part (b)).
From the previous argument, we see that it's enough to do this one place at a time. So we can easily reduce to the case $B = A + P$ for P some place of degree not necessarily equal to 1 (since we're not assuming $k = \bar{k}$), using that fact that $B \geq A$. So choose an element $t \in K$ such that

$$v_p(t) = v_p(B) = v_p(A) + 1,$$

since B is built from A by adding a single copy of P. For $f \in \mathcal{L}(B)$, we have by definition[a]

$$v_p(f) \geq -v_p(B) = -v_p(t),$$

and so by bringing t to the other side we get $v_p(ft) \geq 0$ and thus $ft \in R_p$ (the corresponding local ring). This allows us to define a k-linear map

$$\begin{aligned} \psi : \mathcal{L}(B) &\to k(P) = R_p/\mathfrak{m}_p \\ f &\mapsto ft \mod \mathfrak{m}_p. \end{aligned}$$

In words, we multiply f by t to make it p-adically regular, then look at its image in the residue field. The kernel is precisely those elements x such that multiplying by t lands in the maximal ideal $\mathfrak{m}_p$, which means that $v(x)$ as 1 more than it could have been. So the kernel is all elements such that multiplying by t and taking the valuation gives at least one, thus

$$\ker \psi = \left\{ f \in \mathcal{L}(B) \;\middle|\; v_p(f) \geq -v_p(t) + 1 = -v_p(A) \right\} = \mathcal{L}(A),$$

which follows since B and A only differ at P, since $B = A + P$, so the divisors A, B have the same coefficient at every other place. We thus have the following diagram:

$$\begin{tikzcd} 0 \arrow[r, hook] & \mathcal{L}(A) \arrow[r, hook] \arrow[drr, "\psi"] & \mathcal{L}(B) \arrow[r, two heads] & \mathcal{L}(B)/\mathcal{L}(A) \arrow[r, two heads] \arrow[d, hook, dotted, "\exists\iota"] & 0 \\ & & & k(P) = R_p/\mathfrak{m}_p \arrow[r] & \cdots \end{tikzcd}$$

Link to diagram
where we can conclude that the indicated injection exists, and thus

$$\dim \mathcal{L}(B)/\mathcal{L}(A) \leq [k(p) : k] = \deg P.$$

■

[a] Note that v_p is the p-adic valuation, i.e. the coefficient of P in the divisor as a formal linear combination of points.

Fact 10.4.5: For $p \in \Sigma(K/k)$ with residue field k_p and $[k_p : k] = d$, defining K_p as the completion of K with respect to $|\cdot|_p$, there is an isomorphism $K_p \cong k_p((t))$, a formal Laurent series field. One issue is that if $d = 1$ then $k \subset k_p$, but not for general $d \geq 2$. However, taking the completion results in $k \subset K_p$ again. This shouldn't be too surprising from the perspective of local fields in NTII. There is a structure theory of complete discretely valued fields. This is an *equicharacteristic* such field, i.e. the characteristic of the field agrees with that of the residue field, and all equicharacteristic discretely valued fields will be isomorphic to a ring of formal Laurent series. This isn't a fact of the geometry of curves.

10.5 Bounds on Dimensions

Definition 10.5.1 ($\ell(D)$: The dimension of a Riemann-Roch space)
For $D \in \operatorname{Div} K$, define

$$\ell(D) := \dim_k \mathcal{L}(D).$$

Exercise 10.5.2*(?)*: If $D \in \operatorname{Div} k(t)$, show that

$$\ell(D) = \begin{cases} \deg(D) + 1 & \deg D \geq 0 \\ 0 & \text{else.} \end{cases}$$

Remark 10.5.3: Recall that in a rational function field, every degree zero divisor is principal, and if you adjust by a principal divisor, you don't change $\ell(D)$. This means that in any rational function field, any two divisors of the same degree are going to be linearly equivalent, and thus $\ell(D)$ will only depend on $\deg D$. So rational function fields are much simpler than the fully general case.

Problem. (The Riemann-Roch Problem)
Give good upper and lower bounds on $\ell(D)$ and especially $\ell(nD)$ as a function of n.

Remark 10.5.4: The stronger version of knowing $\ell(D)$ in all cases is unsolvable. If we knew the dimension of every Riemann-Roch space, then we would know too much! E.g. about Weierstrass points on elliptic curves. (?) Looking at positive multiples nD of a single divisor is common. If D is a single point, then the support of the divisor is the collection of places that appear with nonzero coefficients, nD has the same support. This is analogous to not allowing poles at new points, but rather allowing poles at the same points of higher order. So it's reasonable to ask about asymptotic behavior of $\ell(nD)$ in n. Secretly this is a kind of Hilbert function computation: if you have a graded algebra and you look at dimensions of its graded pieces, then there is a theorem that the Hilbert function is a polynomial for $n \gg 1$. Here, $\ell(nD)$ will be a linear polynomial for $n \gg 1$ by the Riemann-Roch theorem, so there are some stabilization phenomena, but given a random divisor of low degree it is difficult to determine $\ell(D)$.

Remark 10.5.5: The last corollary gave us a lower bound:

$$\deg(D) \geq 0 \implies \deg(D) - \ell(D) \geq -1.$$

This can also be thought of as an lower bound on $\ell(D)$ in terms of $\deg(D)$, and next up we'll try to find an upper bound:

Proposition 10.5.6*(?)*.

There exists a $\delta = \delta(K/k) \in \mathbb{Z}$ such that for all $A \in \operatorname{Div} K$, we have

$$\deg A - \ell(A) \leq \delta.$$

11 | Lecture 8: Riemann-Roch Spaces (Part 2)

Recall the proposition we ended with last time:

Proposition 11.0.1 *(?).*
There exists a $\delta = \delta(K/k) \in \mathbb{Z}$ such that for all $A \in \operatorname{Div} K$, we have

$$\deg A - \ell(A) \leq \delta.$$

Exercise 11.0.2 ***(?):*** This proposition is enough to show the existence of rational functions whose polar divisor has as its support any finite subset $S \subset \Sigma(K/k)$.

Most of the lecture will be the proof of this statement.

11.1 Proof of Upper Bound

Rewriting Lemma 10.4.1 yields

$$A_2, A_2 \in \operatorname{Div} K,\ A_1 \leq A_2 \implies \deg A_1 - \ell(A_1) \leq \deg A_2 - \ell(A_2).$$

We now proceed to prove Proposition 11.0.1 in several steps.

11.1.1 Step 1

Choose an $x \in K \setminus k$ and set $B \coloneqq (x)_-$.

Claim: There exists a $C \geq 0$ such that for all $n \geq 0$,

$$\ell(nB + C) \geq (n+1) \deg B.$$

So we give ourselves a certain effective divisor: the divisor of poles of an arbitrary nonconstant element. We can then get a preliminary asymptotic lower bound, not on the same Riemann-Roch space, but on a new one after augmenting the space by some fixed effective divisor C.

Proof (?).
Since $K/k(x)$ has finite degree, let $u_1, \cdots, u_d$ be a basis for K consisting of finitely many rational functions. Note that $d = [K : k(x)]$, and is also equal to $\deg B$ since B was a divisor of poles. Noting that the divisor groups are free commutative groups, so taking any finite number of elements in $\bigoplus \mathbb{Z}$, we can find an element that is less than or equal to all of them. Thus we can choose a $C \geq 0$ such that

$$(u_i) \geq -C \qquad \forall 1 \leq i \leq d.$$

Since the u_i are $k(x)$-linearly independent in K, the functions $\left\{ x^i u_j \;\middle|\; 0 \leq i \leq n,\ 1 \leq j \leq d \right\}$ are k-linearly independent, since any k-linear relation would immediately yield a $k(x)$-linear relation among the u_i.
Exercise 11.1.1*(?):* If $f_i \in \mathcal{L}(D_i)$, so the poles of f are no worse than D_i, then the poles of $f_1 f_2$ are bounded by $D_1 + D_2$ and thus $f_1 f_2 \in \mathcal{L}(D_1 + D_2)$.
Now we can note that there are $(n+1)d = \deg B$ many elements here, and moreover, these all lie in $\mathcal{L}(nB + C)$ since each $(u_j) \geq -C$ and $(x) \geq -B$ and $i \leq n$. From this we can conclude

$$\ell(nB + c) \geq (n+1)d = (n+1)\deg B.$$

■

11.1.2 Step 2

We'll now show that throwing in the fixed divisor C can't increase the Riemann-Roch space that much, and in fact

$$\ell(nB + C) \leq \ell(nB) + \deg C,$$

and so we get a bound

$$\begin{aligned} \ell(nB) &\geq \ell(nB + C) - \deg C \\ &\geq (n+1)\deg B - \deg C \\ &= \deg(nB) + ([K : k(x)] - \deg C) \\ &:= \deg(nB) \pm \gamma, \end{aligned}$$

which shows that

$$\forall n \geq 0,\ \deg(nB) - \ell(nB) \leq \gamma. \tag{1}$$

A problem here is that γ depends upon everything that we've done so far, and this inequality only holds for multiples of a fixed divisor (an infinite ray emanating from B).

11.1.3 Step 3

Claim: For all $A \in \operatorname{Div} K$, there exist $A_1, D \in \operatorname{Div} K$ and $n \geq 0$ such that $A \leq A_1$, $A_1 \sim D$, and $D \leq nB$. I.e. although it can't literally be true that $A \leq nB$, it will be up to linear equivalence.

To see this, set $A_1 := \max(A, 0)$. Using the bound from equation (1), for $n \gg 0$ we have

$$\begin{aligned} \ell(nB - A_1) &\geq \ell(nB) - \deg A_1 \\ &\geq \deg(nB) - \gamma - \deg A_1 \\ &> 0, \end{aligned}$$

and so there exists a $z \in \mathcal{L}(nB - A_1)^\bullet$, a nontrivial element in the linear system.

Remark 11.1.2: The first inequality is an application of our lemma because A_1 is effective, which was the point of this maneuver. I.e., in order to get from $nB - A_1$ to nB, we added A_1, which can only increase the dimension of the space by at most $\deg A_1$. Finally, in the last inequality, we use the fact that B has positive degree since it's a divisor of poles of a nonconstant rational function, and the remaining terms don't depend on n, so we can make $\deg(nB)$ arbitrarily large.

So now set $D := A_1 - (z)$, then $A_1 \sim D$ and since it's in the linear system,

$$(z) \geq -(nB - A_1) = A_1 - nB$$

so $-(z) \leq nB - A_1$ and by adding A_1 to both sides, we obtain

$$0 = A_1 - (z) \leq nB.$$

What have we shown? For any divisor D, we can make it less than nB for some n, up to linear equivalence.

11.1.4 Step 4

Finally, for $A \in \operatorname{Div} K$, choose A_1, D as in the previous step, so $A \leq A_1 \sim D \leq nB$. Then

$$\begin{aligned} \deg A - \ell(A) &\leq \deg(A_1) - \ell(A) && \text{using } A \leq A_1 \\ &= \deg(D) - \ell(D) && \text{changing within linear equivalence class} \\ &\leq \deg(nB) - \ell(nB) \\ &\leq \gamma. \end{aligned}$$

■

11.2 Genus

Definition 11.2.1 (Genus (Important!))
The **genus** of K/k is defined as

$$g \coloneqq \max_{A \in \operatorname{Div} K} (\deg(A) - \ell(A) + 1).$$

This exists by the Proposition 11.0.1, since this set is bounded above.

Exercise 11.2.2 ***(?):*** Show that $g \geq 0$ always and

$$g(k(t)/k) = 0.$$

Remark 11.2.3: Note that if the $+1$ is mostly a correction factor to match up with the topological genus of $\mathbb{P}^1_{/\mathbb{C}}$. That the genus is non-negative should come from the lower bound we had from before. It turns out that over $k = \mathbb{C}$, this genus will agree on the nose with the topological genus of the corresponding compact Riemann surface.

Theorem 11.2.4 ***(Riemann's Inequality).***
If K/k is a function field of genus g,

a. For all $A \in \operatorname{Div} K$,

$$\ell(A) \geq \deg(A) + 1 - g.$$

b. There exists a $c = c(K) \in \mathbb{Z}$ such that for all $A \in \operatorname{Div} K$,

$$\deg(A) \geq c \implies \ell(A) = \deg(A) - g + 1.$$

Remark 11.2.5: This says that the dimension of the linear system is very close to the degree of the corresponding divisor, and is only off by a constant factor g. Part (a) is literally just a rearrangement of the definition of the genus. Part (b) says that if you assume A has sufficiently large degree, this upper bound becomes an equality.

Proof (of b).
By the definition of g, since it is a maximum there exists an A_0 such that

$$g = \deg(A_0) - \ell(A_0) + 1.$$

Set $c \coloneqq \deg(A_0) + g$. Then if $\deg(A) \geq c$, we have

$$\begin{aligned}
\ell(A - A_0) &\geq \deg(A - A_0) - g + 1 \\
&\geq c - \deg(A_0) - g + 1 \\
&= 1,
\end{aligned}$$

so there exists a $z \in \mathcal{L}(A - A_0)^\bullet$ since the dimension is at least 1.
Now set $A' \coloneqq A + (z)$, and note that $A' \geq A_0$. Thus

$$\begin{aligned}
\deg(A) - \ell(A) &= \deg(A') - \ell(A') \\
&\geq \deg(A_0) - \ell(A_0) && \text{by the lemma} \\
&= g - 1.
\end{aligned}$$

By maximality of the genus, we have $\deg(A) - \ell(A) \leq g - 1$, which forces equality ■

Next up: how to we make this inequality into an equality? It turns out that there is some different divisor D' and we can subtract off $\ell(D')$, and that will be the Riemann-Roch theorem.

12 | Lecture 9 (Todo)

13 | Lecture 10A (Todo)

14 | Lecture 10B (Todo)

15 | Lecture 10C (Todo)

16 | 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 direction product with respect to $\left\{R_v \;\middle|\; v \in \Sigma(K/k)\right\}$:

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

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 16.0.1: 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 $x \mapsto [x, x, \cdots]$, 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 kth 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 $D \in \operatorname{Div} K$, we set

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

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 16.0.2 *(?):*

a. Show that $\mathcal{A}_K(D)$ is an k-subspace of $\mathcal{A}_K$.[30]

b. Show that (just as for the Riemann-Roch space) $D_1 \leq D_2 \implies \mathcal{A}_K(D_1) \subseteq \mathcal{A}_K(D_2)$.

Lemma 16.0.3 *(?).*

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

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

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

Why? Once you multiply by t, note that we're looking in the pth component. The condition before was that the valuation at the pth component was at least $-v_p(D_2)$, but

[30] Consider scaling by nonzero constants, where the valuation of constants are zero.

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 16.0.4 *(2.13)*.
For all D,

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

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

Remark 16.0.5: 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

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

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 $\ker(\sigma_2) \subset \operatorname{im}(\sigma_1)$. So take an element $\alpha \in \mathcal{A}_K(A_1) \mod \mathcal{A}_K(A_1)$ 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

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

■

Proof (Step 2).
We can now compute the dimension of this quotient. Using step 1 and Lemma 2.12, we get

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

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 $A_1 \in \operatorname{Div} K$, 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 $B \in \operatorname{Div} K$, 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:

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

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 $\alpha \in \mathcal{A}_K(B) + K$.

■

[a] This "cone structure" on divisors is very useful!

Corollary 16.0.6 ***(2.14).***
This can be applied to the zero divisor:

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

Exercise 16.0.7 ***(?):*** Corollary 2.14 shows that if $K = k(t)$ is the rational function field, then we have $\mathcal{A}_K(0) + K = \mathcal{A}_K$.[31] Show this directly.

[31] So every Adele differs from a rational function by an effective Adele.

Remark 16.0.8: 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.

17 Lecture 11B: Weil's Proof of Riemann-Roch (TODO)

18 Lecture 11C: Weil's Proof of Riemann-Roch (TODO)

19 Lecture 12: Chapter 3, Curves Over a Finite Field

19.1 Finiteness of Class Groups

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 $\mathrm{Cl}^0(K)$ is finite as well, which is the main result we'll prove today.

19.2 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).

19.2.1 Splitting of Places

Question 19.2.1: Given a place in K, how does it split (or not) in K_r?

Remark 19.2.2: 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 19.2.3 *(?)*.
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 19.2.4: 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 19.2.5 *(?)*:

- 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 19.2.6: 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 $\operatorname{mSpec}(\widehat{K_v} \otimes_K L)$, where the hat denotes completing K with respect to the valuation. The e, f, g can all be computed as well.[32]

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.

[32] See Pete's NTII notes, Theorem 1.64.

Exercise 19.2.7 *(?):*

a. Show that $\mathbb{F}_{q^d} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r} \cong \mathbb{F}_{q^l}^{d'}$ where $l = \operatorname{lcm}(d, r)$ and $d' = \gcd(d, r)$.

b. Generalize this to the case when k_p/k and ℓ/k are both cyclic galois extensions.

19.3 Degree 1 Places and Rational Points on a Curve

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

Corollary 19.3.2 *(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 of $v \in \Sigma(K/\mathbb{F}_q)$ 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 19.3.3: 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.

19.4 Finiteness of Places and Rational Points

Lemma 19.4.1 *(?).*

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]

■

[a] There 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.

■

19.5 Finiteness of Class Group

Proposition 19.5.1 ***(Finiteness of class group).***
The degree 0 divisor class group $\mathrm{Cl}^0(K)$ 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 $\mathrm{Cl}^0(K)$, 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

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

If you have any degree n divisors, then $\mathrm{Cl}^n K$ will be a coset of $\mathrm{Cl}^0 K$. 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 $\mathrm{Cl}^n K$ for $n \gg 0$.

In particular, choose $n \geq g$ the genus such that $\delta \mid n$, and let $D \in \mathrm{Div}^n K$. 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 $\mathrm{Cl}^n K$ 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 $\mathrm{Cl}^n K$ to be finite. The result follows because $\mathrm{Cl}^n K$ is a coset of $\mathrm{Cl}^0 K$, all of which have the same size, and the index is finite.

■

[a] By a theorem of Schmidt, we'll later prove that $\delta = 1$.

Definition 19.5.2 (Class Number of K)
The **class number** of K is defined as

$$h := \left|\mathrm{Cl}^0 K\right|.$$

Remark 19.5.3: 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 $\mathrm{Cl}^0 K + A(\mathbb{F}_q)$. 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 $\mathbb{P}^N_{/\mathbb{F}_q}$, and so $|A(\mathbb{F}_q)| \leq \left|\mathbb{P}^N_{/\mathbb{F}_q}\right| < \aleph_0$.

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 $h \to \infty$ in some sense, which is not proved by showing that $|A(\mathbb{F}_q)| \to \infty$, and we'll instead prove it using methods closer to what we're seeing in this course.

Up next: setting up the zeta function.

20 | Lecture 13: Splitting Places

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

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

Question 20.0.1: What happens to places when making this scalar extension? I.e., how to places in K decompose in K_r?

Remark 20.0.2: This is related to an Algebraic Number Theory I problem: for $v \in \Sigma(K_{/\mathbb{F}_q})$ above an affine Dedekind domain R such that $v \in \Sigma(K/R)$, let S be the integral closure of K in K_r. Then we want to factor $p_v S$?

Not quite sure.

20.1 How Places Split

Lemma 20.1.1 ***(Key lemma about how places split.).***
Suppose $d := \deg(v)$. Then K_r/K is galois, so we have $efg = r$. In fact, $c = 1$, so $f = \dfrac{r}{\gcd(d,r)}$ and $g = \gcd(d,r)$ and each place $w \in \Sigma(K_r/\mathbb{F}_{q^r})$ has degree $\dfrac{d}{\gcd(d,r)}$.

Remark 20.1.2: We have the following cases:

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

- The extension *splits completely* iff $r \mid d$,
- All w dividing v have degree 1 iff $d \mid r$.

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

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

20.2 Counting Effective Divisors

Lemma 20.2.1 *(?).*
Suppose $C \in \mathrm{Cl}(K)$, then

- The number of effective divisors $D \in [C]$ is given by
$$\frac{q^{\ell(C)} - 1}{q-1},$$
where $\ell(C)$ is the dimension of the linear system associated to the divisor class C, and this is the dimension of a projective space over $\mathbb{F}_q$.
- For all $n > 2g-2$ with $\delta \mid n$, we have
$$A_n = h\left(\frac{q^{n+1-g} - 1}{q-1}\right).$$

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

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

■

Remark 20.2.2: This is the sharpest result possible: the canonical divisor has degree $2g - 2$ and is special, so this fails for the canonical class.

The upshot: there are three piece of information:

- N_r, the number of $\mathbb{F}_{q^r}$ rational points,
- $\left|\Sigma_d(K_{/\mathbb{F}_q})\right|$ the number of closed points / places of degree d,
- A_n the number of effective divisors of degree n,

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

20.3 Hasse-Weil Zeta Functions

There is a general theory that will unify

- The Riemann zeta function, thought of as the zeta function of $\mathbb{Z}$,
- The Dedekind zeta function, attached to the ring of integers over a number field,
- The Hasse-Weil zeta function of a one variable function field over a finite field,

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

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

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

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

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

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

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

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

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

which allows us to write

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

Question 20.3.1: Where we're going: how does $Z(t)$ depend on K?

Answer 20.3.2: It turns out that it only depends on $A_0, A_1, \cdots, A_{2g-2}$, and thus $Z(t)$ depends on only finitely much information. We will

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

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

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

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

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

These are approximately in order of difficulty. The first two will follow from Riemann-Roch, but the third will be much deeper. This is essentially a positive characteristic analogue of the usual Riemann hypothesis. Note that we're in a global field, the positive characteristic analog of a number field, and for number fields the Riemann hypothesis is the single outstanding problem. In the function field case, it is a theorem!

Proposition 20.3.3 ***(Formula for the zeta function exhibiting rationality).***
Let $K_{/\mathbb{F}_q}$ have genus g and $\delta = I(K)$ the index, the least positive degree of a divisor.[a]

a. If $g = 0$, then

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

b. If $g \geq 1$, then $Z(t) + F(t) + G(t)$ where

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

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

so F involves summing over all divisor classes of degree at most $2g-2$, and G is a term coming from Riemann-Roch involving the class number h.

[a] It will turn out (by a theorem of Schmidt) that $\delta = 1$ in the case of a finite ground field.

Remark 20.3.4: Note that as a consequence, it will definitely be rational in q, and will have a simple pole at $t = 1$. There's no major idea for the proof: when the degree of the divisor class is sufficiently large, we just have an exact formula. If it is smaller, than the formula involves the dimension of the linear system.

20.4 Proof of Rationality

Proof (of rationality of $Z(t)$).
Recall that $\ell(C)$ is the dimension of the associated Riemann-Roch space.
When $g = 0$, by Riemann-Roch we have $\mathrm{Cl}^0(K) = 0$ over any ground field $\Bbbk$ (see exercises), and so $h = 1$. Since every $n \geq 0$ satisfies $n \geq 2g-2$ when $g = 0$, if $\delta \,\Big|\, n$ we have

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

and since $A_n = 0$ unless n is divisible by δ, we have

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n = \sum_{n=0}^{\infty} A_{\delta n} t^{\delta n} = \sum_{n=0}^{\infty} \frac{q^{\delta n+1} - 1}{q-1} t^{\delta n}.$$

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

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

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

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

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

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

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

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

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

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

The next result will be the following theorem:

Theorem 20.4.2 ***(Schmidt, 1910ish).***
For all $K_{/\mathbb{F}_q}$,

$$\delta = I(K) = 1.$$

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

21 Lecture 14: The Hasse-Weil Zeta Function

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

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

which is a formal power series with integer coefficients.

Remark 21.0.1: Recall that we have proved that it is a rational function of t, and in particular when $g = 0, \delta = 1$ [33] 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

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

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

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

Remark 21.0.2: This is analogous to the Dedekind zeta function of a number field K, in which case

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

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

Theorem 21.0.3 ***(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 21.0.4: 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 nth roots of unity in $\mathbb{C}$.

Lemma 21.0.5 ***(?).***
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/dth roots of unity, then raising to the dth power gives them multiplicity d. On the RHS, this is an exercise in cyclic groups: consider the nth power map on $\mathbb{Z}/r\mathbb{Z}$ and compute its image and kernel. As ξ ranges over rth roots of unity, ξ^m ranges over all r/dth roots of unity, each occurring with multiplicity d. Substituting $X = t^{-m}$ and multiplying both sides by t^r yields the original result.[a]

■

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

21.1 Comparing Zeta Functions After Extending Scalars

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

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

Proof (?).
We have an Euler product formula

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

where the sum is over places of the function field.[a]
Exercise 21.1.2: 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, where each place p^r has degree m/d.
In order to compare $Z_r(t)$ to $Z(t)$, we collect the p' into ones that have the same fiber. We then can range over all p first, then over all p' in the fiber above p, yielding

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

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

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

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

Combining all of this yields

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

■

[a] 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.

Remark 21.1.3: 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.

21.2 Proof That $\delta = 1$

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

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

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

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

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

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

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

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

■

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

Remark 21.2.1: We can also conclude that every genus zero function field $K_{/\mathbb{F}_q}$ is isomorphic to $\mathbb{F}_q(t)$ and thus rational, since such a function field rational iff it has index one. Why? By Riemann-Roch, index one implies existence of a divisor of degree one, and taking a genus zero curve says that every divisor of nonnegative degree is linearly equivalent to an effective divisor. Thus if you have a divisor of degree one, you have an effective divisor of degree one, which makes the function field a degree one extension of a rational function field.

Exercise 21.2.2 ***(?):*** Let $K = \mathbb{F}_q(t)$, then show that $g = 0, \delta = 1$, and

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

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

Thus for rationality of the zeta function, we can get rid of the δ cluttering up formulas.

21.3 The Functional Equation

Going back to the plan, we wanted to show

1. Rationality: $Z(t) \in \mathbb{Q}(t)$ and thus $Z(t) = P(t)/Q(t)$,
2. Understand the degrees of P and Q in terms of the genus, and
3. Ask about the roots of $P(t)$ to understand the analog of the Riemann Hypothesis for Dedekind zeta functions

We'll want to establish a functional equation, as is the usual yoga for zeta functions, since it helps establish a meromorphic continuation to $\mathbb{C}$. The algebraic significance of the functional equation is that it aids in understand several equivalent packets of data:

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

Theorem 21.3.1 ***(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: ti gives the dimension in terms of the dimension of a complementary divisor.
Take a canonical divisor $\mathcal{K} \in \operatorname{Div}(K)$, 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

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

We can thus compute

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

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

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

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

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

and thus

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

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

■

21.4 The L Polynomial

Definition 21.4.1 (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

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

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

Question 21.4.2:

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

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

22 | Lecture 15: The L-Polynomial

22.1 Big List of Important Facts

Recall that we had $Z(t) + F(t) + G(t)$:

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

Note that $F(t)$ is a polynomial of degree at most $2g-2$, and clearing denominators in $G(t)$ yields a polynomial of degree at most $2g$

Definition 22.1.1 (The L-polynomial)
The L-polynomial is defined as

$$L(t) \coloneqq (1-t)(1-qt)Z(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n \in \mathbb{Z}[t].$$

It turns out that the degree bound of $2g$ is sharp, and the coefficients closer to the middle are most interesting:

Theorem 22.1.2 *(?).*
Let $K/\mathbb{F}_q$ be a function field of genus $g \ge 1$, then

a. $\deg L = 2g$.
b. $L(1) = h$
c. $L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right)$.
d. Writing $L(t) = \sum_{j=1}^{2g} a_j t^j$,

- $a_0 = 1$ and $a_{2g} = q^g$.
- For all $0 \le j \le g$, we have $a_{2g-j} = q^{g-j} a_j$.
- $a_1 = |\Sigma_1(K/\mathbb{F}_q)| - (q+1)$, which notably does not depend on g.

- Write $L(t) = \prod_{j=1}^{2g}(1-\alpha_j t) \in \mathbb{C}[t]$ [a]

e. The $\alpha_j \in \overline{\mathbb{Z}}$ [b] (which were *a priori* in $\mathbb{C}$) and can be ordered such that for all $1 \le j \le g$, we have $a_j a_{g+j} = q$. [c]

f. If $L_r(t) = (1-t)(1-q^r t)Z_r(t)$ then $L_r(t) = \prod_{j=1}^{2g}(1-\alpha_j^r t)$, where K_r is the constant extension $K\mathbb{F}_{q^r}/\mathbb{F}_{q^r}$

[a] The polynomial isn't monic, but rather has a constant coefficient, so this expansion is somewhat more natural than (say) $\prod(t-\alpha)$.

[b] $\overline{\mathbb{Z}}$ denotes the algebraic integers.

[c] This is the first hint at the Riemann hypothesis: if for example they all had the same complex modulus, this would force $|a_j| = \sqrt{q}$. Thus proving that they all have the same absolute value is 99% of the content!

Note that the α_j are reciprocal roots.

22.2 Proofs

22.2.1 The degree of L and $L(1)$

Proof (of a).
We saw from $Z(t) = F(t) + G(t)$ that $\deg L \le 2g$. Equality will follow from the proof of (d) part 1, since this would imply that $a_{2g} = q^g \neq 0$.

■

Proof (of b).
Our formula $Z(t) = F(t) + G(t)$ and Schmidt's theorem (showing $\delta = 1$) gives

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

where we've expanded G but not F because it involves various $\ell(D)$ which are difficult to compute. It is some polynomial though, and we can evaluate L at 1 to get $L(1) = h$. Thus the class number is the sum of the coefficients!

■

22.2.2 Functional Equation

Proof (of c).
This follows easily from the functional equation for $Z(t)$, which we already established using the Riemann-Roch theorem:

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

We can compute

$$\begin{aligned}
q^g t^{2g} L\left(\frac{1}{qt}\right) &= q^g t^{2g}\left(1-\frac{1}{qt}\right)\left(1-\frac{1}{t}\right)Z\left(\frac{1}{qt}\right) \\
&= q^{g-1}t^{2g-2}(1-t)(1-qt)Z\left(\frac{1}{qt}\right) \\
&= (1-t)(1-qt)Z(t) \\
&\coloneqq L(t),
\end{aligned}$$

where we've distributed one q and two ts in the first steps.

■

22.2.3 Coefficients a_j for $j = 0, 1, 2g$ and Duality

Proof (of d).
Using the functional equation from (c), we can write

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) = \left(\frac{a_{2g}}{q^g}\right) + \left(\frac{a_{2g-1}}{q^{g-1}}\right) t + \cdots + \left(a_0 q^g\right) t^{2g},$$

where we're correcting by enough in t but not enough in q and seeing what we get. Equating coefficients, for $0 \leq j \leq g$ we have

$$a_{2g-j} = q^{g-j} a_j. \tag{2}$$

Using the fact that A_0 is the number of effective degree zero divisors, which is only zero, we have $A_0 = 1$ and we can multiply formal power series to obtain

$$\begin{aligned} L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g} &= (1-t)(1-qt) \sum_{n=0}^{\infty} A_n t^n \\ &= \left(1 - (q+1)t + qt^2\right)\left(1 + A_1 t + A_2 t^2 + \cdots\right) \\ &= 1 + \left(A_1 - (q+1)\right) t + \cdots . \end{aligned}$$

From this, we can read off

- $L(0) = a_0 = 1$
- $a_1 = A_1 - (q+1) = \Sigma_1(K/k) - (q+1)$
- $a_{2g} = a_{2g-0} = q^{g-0} a_0 = a^g$ by taking $j = 0$ in equation (2), and thus $\deg L = 2g$.

■

22.2.4 Absolute Values of Roots / RH

Proof (of e (the most interesting!)).
Consider the **reciprocal polynomial**

$$L^{\perp}(t) := t^{2g} L\left(\frac{1}{t}\right) = t^{2g} + a_1 t^{2g-1} + \cdots + q^g.$$

The original polynomial had $\mathbb{Z}$ coefficients and constant term 1, so this polynomial is monic and has a nonzero constant term. Thus its roots are patently nonzero algebraic integers in $\overline{\mathbb{Z}}^{\bullet}$.
If $L^{\perp}(t) = \prod_{j=1}^{2g} (t - \alpha_j)$, then

$$L(t) = t^{2g} L^{\perp}\left(\frac{1}{t}\right) = \prod_{j=1}^{2g} (1 - \alpha_j t)$$

and if the roots of $L(t)$ are r_j, then the roots of $L^{\perp}(t)$ are the reciprocal roots $1/r_j$ and vice-versa. This shows the first assertion that $r_j \in \overline{\mathbb{Z}}$ as well.
The most interesting part is what follows. Making the substitution $t = qu$ and using (c) we

get

$$\begin{aligned} L^{\perp}(t) &= \prod_{j=1}^{2g}(t-\alpha_j) \\ &:= t^{2g}L\left(\frac{1}{t}\right) \\ &= q^{2g}u^{2g}L\left(\frac{1}{qu}\right) && \text{by (c).} \end{aligned}$$

Using $u = t/q$, we can write

$$\begin{aligned} q^g L(u) &= q^g \prod_{j=1}^{2g}(1-\alpha_j u) \\ &= q^g \prod_{j=1}^{2g}\left(1-\frac{\alpha_j}{q}t\right) \\ &= q^g \prod_{j=1}^{2g}\frac{\alpha_j}{q}\prod_{j=1}^{2g}\left(t-\frac{1}{\alpha_j}\right) \\ &= \prod_{j=1}^{2g}\left(t-\frac{q}{\alpha_j}\right), \end{aligned}$$

where we've pulled out a factor of $-\alpha_j/q$ and in the last step we've used that $\prod_{j=1}^{2g}\alpha_j = q^g$.
This follows because the α_j are the roots of $L^{\perp}$, which has even degree, so the product of all of the roots is equal to the constant term of $L^{\perp}$, which is the leading term of L, which we showed was q^g.
This says that if we take these roots α_j as a multiset and replace each α_j with q/α_j, we get the same multiset back. I.e., this multiset is stable under the involution

$$\begin{aligned} \mathbb{C}^{\times} &\to \mathbb{C}^{\times} \\ z &\mapsto \frac{q}{z}. \end{aligned}$$

This almost pairs up the elements of this finite set of roots, except it may have fixed points. The complex numbers α such that $\alpha = q/\alpha$ are precisely $\pm\sqrt{q}$. So group the α_i^{-1} into

- k **pairs** of nonfixed points, where $\alpha_i \neq q/\alpha_i$,
- m points such that $\alpha_i = \sqrt{q}$,
- n points such that $\alpha_i = -\sqrt{q}$.

So we'd like to show that m and n are both even, so when we're pairing roots with reciprocals these get paired with themselves. We know $2k + m + n = 2g$, so $m + n$ is even. We also know that

$$
\begin{aligned}
q^g &= \prod_{j=1}^{2g} \alpha_j \\
&= q^k \left(\sqrt{q}\right)^m \left(-\sqrt{q}\right)^n \\
&= (-1)^n q^{k+\frac{m}{2}+\frac{n}{2}} \\
&= (-1)^n q^g .
\end{aligned}
$$

This forces n to be even, and since $m = 2g - 2k - n$, m must be even as well.

■

Proof (of f).
We used Dirichlet's character-style decomposition of $Z(t)$ in Schmidt's theorem, and we'll use it again here. Write

$$
\begin{aligned}
L_r(t^r) &= (1-t^r)(1-q^r t^r) Z_r(t^r) \\
&= (1-t^r)(1-q^r t^r) \prod_{\xi \in \mu_r} Z(\xi t) \\
&= (1-t^r)(1-q^r t^r) \prod_{\xi \in \mu_r} \frac{L(\xi t)}{(1-\xi t)(1-q\xi t)} \\
&= \prod_{\xi \in \mu_r} L(\xi t),
\end{aligned}
$$

where we've used that

$$
\begin{aligned}
\prod_{\xi \in \mu_r} \frac{1}{1-\xi t} &= 1 - t^r \\
\prod_{\xi \in \mu_r} \frac{1}{1-q\xi t} &= 1 - q^r t^r
\end{aligned}
$$

which leads to all of the denominators canceling. We can then expand $L_r(t^r)$ as a product to compute

$$
\begin{aligned}
L_r(t^r) &= \prod_{\xi \in \mu_r} L(\xi t) \\
&= \prod_{\xi \in \mu_r} \prod_{j=1}^{2g} (1 - \alpha_j q t) \\
&= \prod_{j=1}^{2g} \prod_{\xi \in \mu_r} (1 - \alpha_j q t) && \text{since these are finite products} \\
&= \prod_{j=1}^{2g} (1 - \alpha_j^r t^r).
\end{aligned}
$$

From this we can conclude that $L_r(t) = \prod_{j=1}^{2g}(1-\alpha_j^r t)$, since t^r is just an indeterminate and these are all identities of polynomials.

■

22.3 Applications and Corollaries

22.3.1 Counting Rational Points

Corollary 22.3.1 *(?).*

Suppose $K/\mathbb{F}_q$ is genus $g \geq 1$ and $L(t) = \prod_{j=1}^{2g}(1-\alpha_j t)$. Then for all $r \in \mathbb{Z}^{\geq 0}$, we have a nice expression for N_r:

$$N_r := |\Sigma_1(K_r/\mathbb{F}_{q^r})| = q^r + 1 - \sum_{j=1}^{2g}\alpha_j^r.$$

Proof (?).

Let $L_r(t) = \sum_{j=1}^{2g} a_{j,r} = \prod_{j=1}^{2g}(1-\alpha_j^r t)$, so $a_{1,r} = -\sum_{j=1}^{2g}\alpha_j^r$. Then using (d) part 3, we can write

$$|\Sigma_1(K_r/\mathbb{F}_{q^r})| = q^r + 1 + a_{1,r} = q^r + 1 - \sum_{j=1}^{2g}\alpha_j^r.$$

This follows from consider $\prod(1-\alpha_j^r t)$, where extracting the t^1 coefficient involves choosing $-\alpha_j^r$ once and 1 from all of the remaining terms, and then you sum over the disjoint possibilities.

■

Remark 22.3.2: We'd really like to compute the coefficients of the L polynomials, since we can solve a polynomial equation to get the roots. But the Galois groups of these polynomials may not be solvable, so the term $\sum \alpha_j^r$ will in general be some symmetric function in the complex roots. Note that any symmetric polynomial in the roots is also a symmetric polynomial in the coefficients.

22.3.2 Relating Rational Points to Coefficients

Corollary 22.3.3 *(?).*

For $K/\mathbb{F}_q$ a function field, define

$$S_r := N_r - (q^r + 1) = -\sum_{j=1}^{2g} \alpha_j^r.$$

Note that $N_r = |\Sigma(K_r/\mathbb{F}_{q^r})|$ is the number of $\mathbb{F}_{q^r}$-rational point. Then

a. $L'(t)/L(t) = \sum_{r=1}^{\infty} S_r t^{r-1}$.
b. $a_0 = 1$, and for all $1 \le i \le g$,

$$ia_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1}.$$

Remark 22.3.4: What's the usefulness here? If you only have the coefficients of the L polynomials, taking the logarithmic derivative gives access to these quantities S_r. The second formula is a recursive expression for the a_i in terms of the S_i. So you can compute the coefficients of the L polynomial by counting $\mathbb{F}_{q^r}$-rational points on your curve (or places on your function field) for $r = 1, 2, \cdots, g$. Similarly, if you have all of the coefficients for a Z polynomial, you can solve for the S_i.

Proof (of a).

Essentially just a computation. Logarithmically differentiating both sides of $L(t) = \prod_{j=1}^{2g}(1 - \alpha_j t)$ and expanding in a geometric series yields

$$\begin{aligned}
\frac{L'(t)}{L(t)} &= \sum_{j=1}^{2g} \frac{-\alpha_j}{a - \alpha_j t} \\
&= \sum_{j=1}^{2g} (-\alpha_j) \sum_{r=0}^{\infty} (\alpha_j t)^r \\
&= \sum_{r=1}^{\infty} \left(\sum_{j=1}^{2g} (-\alpha_j^r) \right) t^{r-1} \\
&= \sum_{r=1}^{\infty} S_r t^{r-1}.
\end{aligned}$$

■

Proof (of b).

Clearing denominators and equating coefficients in $L'(t) = L(t) \sum_{r=1}^{\infty} S_r t^{r-1}$ yields the result immediately, since the ia_i are what appear as coefficients in the derivative of a formal power series, whereas the RHS is a Cauchy product.

■

Remark 22.3.5: The moral: to compute zeta functions, you don't have to enumerate divisors and compute dimensions of Riemann-Roch spaces. Note that the Riemann-Roch theorem tells us something interesting about these dimensions, but doesn't compute the dimension outright! Instead, it suffices to compute $\mathbb{F}_{q^r}$-rational points for $r \leq g$.

A few lectures ago we discussed the places on a hyperelliptic function field, including a place at infinity. Computing the zeta function of a hyperelliptic curve involves plugging in x-values and determining if it is

- A nonzero non-square: no y-values,
- Zero: exactly one y-value,
- A nonzero square: two y-values.

This is what happens at the finite places. To handle the place at ∞, there is a recipe for the degree of the polynomial in terms of the coefficients. So for any hyperelliptic function field (and in particular, for any elliptic function field) we have a concrete algorithm for computing their zeta functions. Note that this is not necessarily a *good* algorithm: it still involves plugging in many values and checking if things are squares in finite values. It seems that most people who compute a lot of zeta functions mostly focus on hyperelliptic function fields.

How are you going to compute zeta functions or even places for more complicated function fields? The Riemann-Hurwitz formula says that since any function field is a finite degree extension of a rational function field, the curve is given as a degree 2 branched cover of $\mathbb{P}^1$, it suffices to compute the fibers of this cover in order to get point counts.

23 Lecture 16 (Todo)

24 Lecture 17 (Todo)

25 Lecture 18 (Todo)

26 Lecture 19 (Todo)

27 Lecture 20 (Todo)

28 Lecture 21 (Todo)

29 Lecture 22 (Todo)

30 Lecture 23 (Sketch)

What is an isogeny?

What is an Artin-Schreier extension?

What is Kummer theory?

What are Weil differentials?

What are Kahler differentials?

What is the Riemann Hurwitz formula?

Corollary 30.0.1 *(?).*
Let k be a perfect field of characteristic $p > 0$, $d \in \mathbb{Z}^{\geq 0}$ with $\gcd(d, p) = 1$, and let $f \in k[x]$ and $L := K(p^{-1}(f))$. Then $[L : K] = p$ and L/k is a regular function field of genus $g =$

$\frac{1}{2}(p-1)(d-1)$ that is unramified away from ∞.

30.1 Artin-Schreier Extensions of Function Fields

Fact 30.1.1: For k a field, $\operatorname{ch}(k) = p > 0$, and $a, b \in k$, TFAE:

1. $k(\wp^{-1}(a)) = k(\wp^{-1}(b))$

2. a and b generate the same cyclic subgroup of $k/\wp(k)$.

In particular, if $K(\wp^{-1}(u))/k$ is an Artin-Schreier extension, then for all $x \in k$, $k(\wp^{-1}(u-(x^p-x))) = k(\wp^{-1}(u))$.

Lemma 30.1.2 ***(?).***
Let k a *perfect* field of characteristic $p > 0$, K/k a function field, $u \in K$, and $\mathfrak{p} \in \Sigma(K/k)$.

- There exists a $z \in K$ such that $z_v := v_{\mathfrak{p}}(u-(z^p-z))$ satisfies either
  - $z_v \geq 0$, or
  - $z_v \leq 0$ and $z_{\mathfrak{p}}$ is prime to p.
- There exists a most one $m \in \mathbb{Z}$ that is negative and prime to p such that for some $z \in K$ we have $v_{\mathfrak{p}}(u-(z^p-z)) = m$. If such an m exists, it is given by $m = \max\left\{ v_{\mathfrak{p}}(u-(z^p-z)) \;\middle|\; z \in K \right\}$.
- It follows that precisely *one* of the two alternatives in the first statement holds.

Theorem 30.1.3 ***(Genus Formula for Artin-Schreier Extensions).***
Let k a *perfect* field of characteristic $p > 0$, K/k a function field, $u \in K$, $L := K(\wp^{-1}(u))$, $\mathfrak{p} \in \Sigma(K/k)$, and set

$$M_{\mathfrak{p}} := \begin{cases} |m| & \text{if there exists a } z \in K \text{ such that } v_{\mathfrak{p}}(u-(z^p-z)) = m \\ -1 & \text{if there exists a } z \in K \text{ such that } v_{\mathfrak{p}}(u-(z^p-z)) \geq 0 \end{cases}.$$

Then

a. If $M_{\mathfrak{p}} = -1$, then $\mathfrak{p}$ is unramified in L.

b. If $M_{\mathfrak{p}} \geq 1$, then $\mathfrak{p}$ is totally ramified in L. Letting $\tilde{\mathfrak{p}}$ be the unique place lying over $\mathfrak{p}$, then

$$d(\tilde{\mathfrak{p}}/\mathfrak{p}) = (p-1)(M_{\mathfrak{p}}+1) \qquad \text{(wild ramification).}$$

c. Suppose there exists a $\mathfrak{p}$ such that $M_{\mathfrak{p}} \geq 1$. Then $[L : K] = p$, L/k is regular, and we have a genus formula

$$g_L = pg_K + \left(\frac{p-1}{2}\right)\left(-2 + \sum_{p \in \Sigma(K/k)} (M_p + 1) \deg p\right).$$

31 Lecture 24: Hermitian Function Fields (Sketch)

What is an elementary p-group?

What is geometrically irreducible?

Theorem 31.0.1 ***(Stichtenoth Prop 6.4.1).***
Let k be a perfect field of characteristic $p > 0$, $q := p^s$ some power of p, $K := k(x)$. Let $u \in k^\times$ and suppose $T^q + \mu T$ splits in k.[a] Let $f \in k[x]$ with $\deg(f) = M$ where $p \not\mid M$. Then

a. The polynomial

$$P(x, y) := y^q + uy - f(x) \in k[x]$$

is geometrically irreducible, and so $L := \mathrm{ff}(k[x, y]/\langle p \rangle)$ is a regular function field over k.

b. We have $[L : K] = q$.

c. $A := \left\{\gamma \in k \;\middle|\; \gamma^q + u\gamma = 0\right\}$ is an order q subgroup of $\mathbb{G}_a/k := (k, +)$. Moreover, for all $\sigma \in \mathrm{Aut}(L/K)$, there exists a unique $\gamma(\sigma) \in A$ such that $\sigma(y) = y + \gamma(\sigma)$ and $\sigma \mapsto \gamma(\sigma)$ yields an isomorphism $\mathrm{Aut}(L/K) \xrightarrow{\sim} A$.

d. No finite place of K ramifies in L, while p_∞ is totally ramified. If $\tilde{p}_\infty/p_\infty$, then $d(\tilde{p}_\infty/p_\infty) = (q-1)(M+1)$.

e. We have

$$g_L = \left(\frac{1}{2}\right)(q-1)(m-1).$$

[a] When $u = -1$, this recovers q-Artin-Schreier extensions.

Next up: one of the most important function fields of all time!

Definition 31.0.2 (Hermitian Function Field)
Set $A_q := \mathbb{F}_{q^2}(x, y)$ and consider the polynomial

$$y^q + y = x^{q+1}.$$

Then $u = 1, M = q + 1$, and $g = \left(\frac{1}{2}\right)(q)(q-1) = \binom{q}{2}$.

Theorem 31.0.3 ***(?).***

$$\left|\Sigma_1(A_q/\mathbb{F}_{q^2})\right| = q^3 + 1.$$

What are the Weil bounds?

Corollary 31.0.4 ***(Ihara).***
If $K/\mathbb{F}_q$ is a maximal function field of genus g, then

$$g \leq \left(\frac{1}{2}\right)(q - \sqrt{q}).$$

Fact 31.0.5: If $K/\mathbb{F}_{q^2}$ is maximal, then $N_1 = q^2 + 1 + 2gq = q^2 + q - \sum_{j=1}^{2g} \alpha_j$. Applying the RH, $|\alpha_j| = q$, and it follows that $\alpha_j = -q$ for all j and thus

$$L(t) = (1 + qt)^{2g}.$$

Theorem 31.0.6 ***(Kleiman, Serre).***
If $K/\mathbb{F}_q \subset L/\mathbb{F}_q$ is a finite extension of function fields, then $L_K(t)$ divides $L_L(t)$.

Corollary 31.0.7 ***(?).***
If $L/\mathbb{F}_{q^2}$ is maximal, so is $K/\mathbb{F}_{q^2}$.

Theorem 31.0.8 ***(Stichtenoth?).***

$$\mathrm{Aut}(A_1/\mathbb{F}_{q^2}) \cong \mathrm{PGU}_3(\mathbb{F}_{q^2}),$$

the *projective unitary group*, which is of order $q^3(q^2-1)(q^3+1)$.

Remark 31.0.9: The size of this group G_q is asymptotically $G_q \sim q^8$, while $g(A_q) \sim \frac{q^2}{2}$, so this is a lot of automorphisms compared to the sizes of automorphism groups of Riemann surfaces. More precisely, $G_q > 16g(q)^4$.

Theorem 31.0.10 ***(Stichtenoth).***
For any other function field K/k for any field k, $|\mathrm{Aut}(K/k)| < 16g^4$.

Remark 31.0.11: This only happens in positive characteristic, when $\mathrm{ch}(k), g, q$ match up in a very specific way. So Hermitian function fields are the algebraic curves with the most symmetries.

Theorem 31.0.12 ***(Hurwtiz).***
In characteristic zero, if $g \geq 2$ then $|\mathrm{Aut}(K/k)| \leq 84(g-1)$.

32 | Lecture 25: Differential Pullback Theorem (Sketch)

This will recover the Riemann-Hurwitz formula by taking degrees.

Lemma 32.0.1 ***(?).***
Let $K/k \subset L/\ell$ be a finite degree extension of function fields, and suppose K/k is regular and L/K is separable. Then ℓ/k and L/ℓ are separable and $L\ell$ is regular.

$$\begin{tikzcd}
 & L & \\
K \arrow[ur, dash, "\text{separable}"] & & \ell \arrow[ul, dash] \\
 & k \arrow[ul, dash, "\text{regular}"] \arrow[ur, dash] &
\end{tikzcd}$$

Link to diagram

Recall some facts/definitions:

- The **adele ring of** K is defined as

$$\mathcal{A}_K \coloneqq \prod_{v \in \Sigma(K/k)}' K$$

which is a *restricted direct product*, i.e. each element $\alpha \in \mathcal{A}_K$ has the property that for almost every p, the p-adic valuation of the pth coordinate $v_p(\alpha_p) \geq 0$. There is a diagonal embedding

$$\begin{aligned} K &\hookrightarrow \mathcal{A}_K \\ f &\mapsto (f, f, \cdots). \end{aligned}$$

- For any divisor $D \in \mathrm{Div}\, K$, define

$$\mathcal{A}_K(D) \coloneqq \left\{ \alpha \in \mathcal{A}_K \;\middle|\; v_p(\alpha_p) \geq -v_p(D) \ \forall p \right\},$$

the adelic analog of the Riemann-Roch space.

- A space of linear forms

$$\Omega(D) \coloneqq \left\{ \omega : \mathcal{A}_K \to A \;\middle|\; \ker \omega \supseteq K + \mathcal{A}_K(D) \right\}$$

where $D_1 \leq D_2 \implies \Omega_K(D_2) \leq \Omega_K(D_1)$.

- $\Omega_K := \varinjlim_D \Omega_K(D)$.
- For any $\omega \in \Omega_K^\bullet$, $(\omega) := \max\left\{D \,\middle|\, \omega = 0 \text{ on } \mathcal{A}_K(D) + K\right\}$.
- $\mathcal{A}_{L/K} = \left\{\alpha \in \mathcal{A}_L \,\middle|\, \alpha q_1 = \alpha q_2 \text{ if } Q_1, Q_2/p\right\} \leq_{\mathrm{Vect}_\ell} A_L$
- The **adelic trace map**

$$\begin{aligned} \mathrm{Tr}_{L/K} : \mathcal{A}_{L/K} &\to \mathcal{A}_K \\ \alpha &\mapsto \mathrm{Tr}_{L/K}(\alpha)/p = \mathrm{Tr}_{L/K}(\alpha_Q) \qquad \text{for any } Q/p. \end{aligned}$$

Theorem 32.0.2 ***(?).***
Let $\omega \in \Omega_K$, then there exists a unique $\omega^* \in \mathcal{A}_L$ such that

- For all $\alpha \in \mathcal{A}_{L/K}$, we have $\mathrm{Tr}_{\ell/k}\,\omega^*(\alpha) = \omega(\mathrm{Tr}_{L/K}(\alpha))$.

ω^* is formally denoted $\mathrm{Cotr}_{L/K}(\omega)$ and called the **cotrace** of ω.

Theorem 32.0.3 ***(?).***
If $K/k \subset L/\ell$ is a finite extension of function fields with K/k regular, then for all $\omega \in \mathcal{A}_K^\bullet$, we have $\omega^* \in \mathcal{A}_L^\bullet$. Moreover,

$$(\omega^*) = \iota_{L/K}((\omega)) + D(L/K).$$

Taking degrees yields the Riemann-Hurwitz formula.

33 | Indices

33.1 ToDos

List of Todos

33.1 Definitions

Definitions

33.1 Theorems

Theorems

33.1 Exercises

Exercises

33.1 Figures

List of Figures

34 Bibliography

[1] H. Stichtenoth. *Algebraic function fields and codes*. Springer, 2009.