Algebraic Curves

D. Zack Garza

Thursday 17th September, 2020

Contents

List of Todos

List of Definitions

List of Theorems

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.

D. Zack Garza, Thursday 17^{th} September, 2020
16:07

1 | Monday, August 24

Review of lecture one:

Theorem 1.1 ***(Finitely Generated in Towers).***
See video

- Transcendence bases
- Lüroth problem

2 | Monday August 21st

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

See also completions, residue fields.

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

Example 2.1.
The valuation rings of $\mathbb{Q}$ are $\mathbb{Z}_{(p)} \coloneqq \mathbb{Z}[\left\{ \frac{1}{\ell} \;\middle|\; \ell \neq p \right\}]$ for all primes p.

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

Exercise 2.1.
Show that a valuation ring is a local ring, i.e. it has a unique maximal ideal.

Example 2.2.
Where does the log come from?

There is a p-adic valuation:

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

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

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

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

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

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

See NT 1 notes.

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

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

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

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

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

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

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

which need not be surjective.

We can consider principle divisors with the map

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

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

3 | Friday, August 28

3.1 Field Theory

See Chapter 11 of Field Theory notes.

3.1.1 Notion 1

Definition 3.0.1 (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.

3.1.2 Notion 2

The second is being finitely generated as an algebra:

Definition 3.0.2 (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.

3.1.3 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 3.0.3 (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 3.1.

a. Show $k(t)/k$ is finitely generated by notion (3) but not by (2).
b. Show that $k[t]/k$ is (2) but not (1).

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

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

Hint: Zariski's lemma.

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

Theorem 3.1 ***(Field Theory Notes 11.19).***
If $L/K/F$ are field extensions, then L/F is finitely generated $\iff$ K/F and L/K are finitely generated.

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

Definition 3.1.1 (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 3.2*(?)*.
For ℓ/k a field extension,

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

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

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

Definition 3.2.1 (Transcendence Degree)**.**
The *transcendence degree* of ℓ/k is the cardinality of any transcendence basis.

Analogy: dimension in linear algebra.

Theorem 3.3*(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 3.4*(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 $\operatorname{trdeg}(F(x)/F) = \mathbb{1}\,[x/F \text{ is transcendental}]$.
So the degree increases when a transcendental element is added, and doesn't change when x is algebraic.
By additivity in towers, we take $k \hookrightarrow k(x_1) \hookrightarrow k(x_1, x_2) \hookrightarrow \cdots \hookrightarrow k(x_1, \cdots, x)n) = K$ to obtain a chain of length n. The transcendence degree is thus the number of indices i such that x_i is transcendental over $k(x_1, \cdots, x_{i-1})$.

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

■

Definition 3.4.1 (Function Fields)**.**
For $d \in \mathbb{Z}^{\geq 0}$, an extension K/k is *a function field in d variables* (i.e. of dimension d) if K/k is finitely generated of transcendence degree d.

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

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

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

3.2 Case Study: The Luroth Problem.

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

Theorem 3.5 ***(Luroth).***
True for $d = 1$: For any $k \subset \ell \subset k(t)$, $\ell = k(x)$.

Theorem 3.6 ***(Castelnuovo).***
Also true for $d = 2, k = \mathbb{C}$.

Theorem 3.7 ***(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 3.8 ***(Clemens-Griffiths).***
No if $d \geq 3$ and $k = \mathbb{C}$.

Unirational need not imply rational for varieties.

Exercise 3.2.
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 Luroth problem implies an affirmative answer to the inverse galois problem for $\mathbb{Q}$.

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

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

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

What's a global field?

3.3 Onto Business

Definition 3.8.1 (?).
For K/k a field extension, set $\kappa(K)$ to be the algebraic closure of k in K, i.e. special case of *integral closure*. If K/k is finitely generated, then $\kappa(K)/k$ is finite degree.
Here $\kappa(k)$ is called the *field of constants*, and K is also a function field over $\kappa(k)$.

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

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

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

Where we use the fact that from above, $\kappa(k)/k$ is finitely generated and algebraic and thus finite, and by a previous theorem, if K/k is transcendental then $K/\kappa(k)$ is as well, and thus finitely generated.

Thus if you have a function field over k, you can replace k by $\kappa(k)$ and regard K as a function field over $\kappa(k)$ instead.

4 | Sunday, August 30

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

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

In general we have a map

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

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

What about for function fields?

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

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

Exercise 4.1.
If ℓ/k is algebraic and $\ell \otimes_k \ell$ is a domain, the $\ell = k$.

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

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

Remark 1.
We'd like the tensor product of a field to be a field, or at least a domain where we can take the fraction field and get a field. This hints that we should not be tensoring algebraic extensions, but rather transcendental ones.

Exercise 4.2.
For ℓ/k a field extension,

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

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

Proposition 4.1 ***(FT 12.7, 12.8).***
Let $k_1, k_2/k$ are field extensions, and suppose $k_1 \otimes_k k_2$ is a domain. Then this is a field $\iff$ at least one of k_1/k or k_2/k is algebraic.

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

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

Exercise 4.3.
If K/k is finitely generated (i.e. a function field) and $K \otimes_k \ell$ is a domain, then $ff(K \otimes_k \ell)/\ell$ is finitely generated.

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

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

Lemma 4.2.
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 4.4.
The simplest possible case: describe $\mathbb{C}(t) \otimes_{\mathbb{R}} \mathbb{C}$, tensored as $\mathbb{R}$-algebras.

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

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

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

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

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

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

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

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

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

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

Example 4.2.

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

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 2.
This is pretty technical, but we won't have to worry if $k = k^{\frac{1}{p}}$. Equivalently, frobenius is surjective on k, i.e. k is a perfect field.

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

Reminder: the perfect fields:

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

Imperfect fields include:

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

Look up uniformizing elements and valuations.

Theorem 4.3 ***(FT 12.20).***
For field extensions K/k, TFAE

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

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

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

Regular corresponds to nonsingularity in this neck of the woods.

Remark 3.
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 4.5.

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

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

b. Show every purely transcendental extension is regular.

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

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

4.2 Example of a Non-Regular Family of Function Fields

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

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

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

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

Proposition 4.4 ***(Some Facts).***
ρ_N is surjective, and

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

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

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

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

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

We obtain a field theory diagram

$$\begin{tikzcd}
\overline{K}_N \arrow[d, "\{\pm I\}"] \arrow[dd, bend right=40, "\mathrm{GL}(2{,}\mathbb{Z}/N\mathbb{Z})"'] \\
K_N \arrow[d, "\mathrm{GL}(2{,}\mathbb{Z}/N\mathbb{Z})/\{\pm I\}"] \\
\mathbb{Q}(t)
\end{tikzcd}$$

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

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

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

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

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

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

5 | Sunday, August 30

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

5.1 Polynomials Defining Regular Function Fields

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

Exercise 5.1.
Let R_1, R_2 be k-algebras that are also domains with fraction fields K_i. Show $R_1 \otimes_k R_2$ is a domain $\iff K_1 \otimes_k K_2$ is a domain.

Denominator-clearing argument.

Definition 5.0.1 (Geometrically Irreducible)**.**
A polynomial of positive degree $f \in k[t_1, \cdots, t_n]$ is *geometrically irreducible* if $f \in \bar{k}[t_1, \cdots, t_n]$ is irreducible as a polynomial.

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

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

Exercise 5.2.
Easy:

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

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

Proposition 5.1 ***(?).***
Suppose that f is geometrically irreducible.

a. The function field K/k is regular.

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

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

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

■

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

Exercise 5.3.
Let k be a field, $d \in \mathbb{Z}^+$ such that $4 \nmid d$ and $p(x) \in k[x]$ be positive degree. Factor $p(x) = \prod_{i=1}^{r} (x - a_i)^{\ell_i}$ in $\bar{k}[x]$.

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

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

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

Exercise 5.4 (Nice, Recommended)**.**
Assume k is a field, if necessary assuming char $(k) \neq 2$.

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

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

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

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

Example of a non-rational genus zero function field.

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

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

In one variable, yes:

Theorem 5.2 ***(Regular Function Fields in One Variable are Geometrically Irreducible).***
Let K/k be a one variable function fields (finitely generated, transcendence degree one). Then

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

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

■

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

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

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

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

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

Example 5.1.
Example from earlier lecture:

$ax^p + b - y^b$

Moral: look for examples of nice function fields by taking irreducible polynomials in two variables.

This will define a one-variable function field. If the polynomial is geometrical reducible, this produces regular function fields.

Next: One variable function fields and their valuations.