Chapter 8
Curves

def. A *curve* is an irreducible alg variety of dimension 1.

Points of a curve have local rings of dim $= 1$.

Prop. (from CA): (A, m) Noetherian local domain of dimension 1.
Then are equivalent:
1) A is regular, i.e. $\dim_k m/m^2 = 1$; $k = A/m$.
2) A is integrally closed
3) m is principal
4) A is a PID and all ideals are powers of m.

Such A is a *discrete valuation ring*, with a valuation

$v: A - 0 \to \mathbb{Z}$ $(v(0) = \infty)$

s.t. $\forall f \in A - 0$ is $f = \alpha \cdot t^{v(f)}$, $m = (\underset{\text{uniformizer}}{t})$, $\alpha \in A^\times$.

A discrete valuation satisfies:
1) $v(fg) = v(f) + v(g)$
2) $v(f+g) \geq \min(v(f), v(g))$
$=$ if $v(f) \neq v(g)$

If $p \in C$ is a regular point of a curve, then a uniformizer at p is $t \in \mathcal{O}_{X,p}$ s.t. $m_p = (t)$.

also called „local parameter"

That means, t has a „simple zero" at p, or a vanishing of order 1, and $v(f)$ can be thought of as the order of zero/pole of f at p:

$$f = \alpha \cdot t^{v(f)} \quad \text{where } v(f) \in \mathbb{Z} \text{ and } \alpha \in \mathcal{O}_{X,p}^{\times}.$$

Moral: curves are easier to study because regular local rings are dvr's, and singularities can be resolved via normalization: any normal curve is regular.

Of course, curves are „simple" geometrically but not arithmetically: Fermat's Last Thm is a statement about curves! (over $\mathbb{Z}$)

§ Classification of projective curves

Thm. X, Y projective regular curves. Then $X \underset{Bir}{\sim} Y \iff X \cong Y$.

Non-Ex: 1) $\mathbb{P}^1 \underset{Bir}{\simeq} \mathbb{A}^1$ – not projective

2) $\mathbb{P}^1 \times \mathbb{P}^1 \underset{Bir}{\simeq} \mathbb{P}^2$ – not curves

3) $\mathbb{P}^1 \underset{Bir}{\simeq} Z_+(x^3 - y^2 z)$ – not regular

Extension lemma. X curve, $p \in X$ regular point, $\varphi : X - p \to \mathbb{P}^n$ morphism.
Then $\exists !\ \Phi : X \to \mathbb{P}^n$ that extends φ.

Proof. We can assume X affine, because it's enough to extend φ to an open nbhd of p.

Let $D = D_+(x_0) \subset \mathbb{P}^n$. We can assume $V := \varphi^{-1}(D) \subset X$ is a non-empty open.

Then $\varphi : V \to D \simeq \mathbb{A}^n$ is given by $(f_1, \dots, f_n)$, $f_i = \dfrac{g_i}{g_0} \in \mathcal{O}_X(V)$.

Let
$$\Phi : X \to \mathbb{A}^{n+1}$$
$$x \mapsto (g_0(x), g_1(x), \dots, g_n(x)).$$

If $\Phi(p) \neq 0$, we get an extension

nbhd of p where g_i's don't vanish simultaneously

$$\begin{tikzcd} W \arrow[r, "\Phi"] \arrow[dr, bend right, "\varphi"'] & \mathbb{A}^{n+1} - 0 \arrow[d, "\pi"] \\ & \mathbb{P}^n \end{tikzcd}$$

and win.

Want: change Φ to guarantee $\Phi(p) \neq 0$.

Let $t \in \mathcal{O}_{X,p}$ be a uniformizer,

then $\forall\, g_i = \alpha_i(t) \cdot t^{v_i}$ where $\alpha_i(t) \in \mathcal{O}_{X,p}$ does not vanish at p.

Define $v := \min(v_0, \dots, v_n)$

$\rightsquigarrow \mu_i := v_i - v \geq 0$ and $\exists j: \mu_j = 0$.

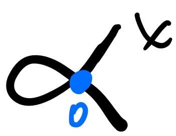
We replace each g_i by

$\tilde{g}_i := g_i \cdot t^{-v} = \alpha_i(t) \cdot t^{\mu_i}$ – defined in a neighborhood of p

$\Rightarrow$ not all $\tilde{g}_i$ vanish at p,

and $\pi \circ \tilde{\Phi}$ extends φ to a nbhd of p, because $\frac{\tilde{g}_i}{\tilde{g}_0} = \frac{g_i}{g_0}$ where both are defined.

Non-Ex: fails for singularities



$y^2 = x^3 + x^2$

$$X \dashrightarrow \mathbb{P}^1$$
$$(x,y) \mapsto (x:y)$$

does NOT extend to 0!

Cor. X curve, $p \in X$ regular pt, Y projective var.
Then $\forall$ rational map $\varphi: X \dashrightarrow Y \subseteq \mathbb{P}^m$
extends to a morphism near p.

Proof: Let $U \ni p$ open nbhd s.t.
$\varphi: U - p \to Y$ is a morphism.

Then φ extends to
$\varphi: U \to \mathbb{P}^m$, and $\varphi(U) \subseteq Y$ because
$Y \subseteq \mathbb{P}^m$ is closed $\Rightarrow$
$\varphi^{-1}(Y) \subseteq U$ is closed and contains $U - p \Rightarrow \varphi^{-1}(Y) = U$.

Proof of Thm.

X, Y projective regular curves,

we have
$$\begin{array}{ccc} X & \dashrightarrow & Y \\ \cup\!| & & \cup\!| \\ U & \xrightarrow[\varphi]{\sim} & V \end{array}$$
isom with inverse ψ.

By Cor., φ and ψ extend to morphisms.

We get that $\varphi \circ \psi = id_V$ and $\psi \circ \varphi = id_U$
on non-empty open sets
$\Rightarrow$ by separatedness, $=$ on X and Y,
so φ and ψ are inverse isoms.

Fundamental thm for curves

K/k a f.g. field extension with $\text{tr deg}_k K = 1$
$\Rightarrow \exists!$ regular projective curve X
up to isom. s.t. $k(X) \simeq K$ as k-extensions.

Cor. There is a contravariant equivalence of cats:

$$\left\{\begin{array}{c}\text{regular curves over } k \\ + \text{dominant rational maps}\end{array}\right\}^{op} \simeq \left\{\begin{array}{c}\text{f.g. } k\text{-extensions of tr deg } 1 \\ + k\text{-algebra homs}\end{array}\right\}$$

Earlier we proved analogous equivalence for all irreducible varieties and fin. gen. field extensions of k, and now we know that all tr deg 1 extensions correspond to curves.

Fundamental Thm

Proof: Uniqueness follows from the Thm because two such curves X and X' would be birational, since
$$k(X) \simeq k(X') \text{ as } k\text{-extensions.}$$

Existence: K/k tr deg $1 \Rightarrow \exists\, x \in K$:
K is finite separable over $k(x)$.

That means, $\exists f \in K$ s.t. $K = k(x)[f]$ and f is a root of an irreducible polynomial

$$y^n + a_{n-1}(x)y^{n-1} + \ldots + a_0(x) = 0.$$

This equation defines a curve C in $\mathbb{A}^2$, with $k(C) \simeq K$.

Then $\overline{C} \subset \mathbb{P}^2$ is a projective curve.

We define X as the normalization of $\overline{C}$, it's a regular curve with $k(X) \simeq k(\overline{C}) \simeq k(C) \simeq K$.

Fact: X is a projective curve.
(follows from the general construction of normalization, which we skipped).

Over $\mathbb{C}$: there are bijections:

regular projective complex curves

$\Updownarrow$

fin. gen. $\mathbb{C}$-extensions of tr deg 1

$\Updownarrow$ hard!

compact connected 1-dim complex mfds (Riemann surfaces)

Geometry, algebra and analysis come together!

§ Elliptic curves

Let k alg closed, char $k \neq 2$

Elliptic curve: $C = \{y^2 = x(x-\lambda)(x-\mu)\} \subset \mathbb{A}^2$,
$\lambda \neq \mu \in k^\times$.

Thm. Elliptic curves are not rational,
i.e. $C \underset{bir}{\not\sim} \mathbb{P}^1$.

Reason: they have different genus
$g(\mathbb{P}^1) = 0$ vs $g(\overline{C}) = 1$

  (pictures over $\mathbb{C}$)

and genus is a birational invariant.
Genus: over $\mathbb{C}$ — # holes in the Riemann surface
over k — more complicated definition.

Proof: can assume $\lambda = 1$, $\mu = -1$ (same proof).
Let $K := k(x)$, and
Let $L := k(C) = K(y)$ where $y^2 = x(x-1)(x+1)$.
Want: $L \not\cong k(t)$.

Claim 1: $\forall$ valuation $v: L^\times \to \mathbb{Z}$ $v(x)$ is even.

Proof: $\cdot\, v(x) = 0$ — ok

• $v(x) > 0 \Rightarrow v(x-1) = \min(v(x), v(-1)) = v(-1) = 0$

$\qquad\qquad\qquad\; v(x+1) = v(1) = 0$

$$\Rightarrow \underset{2v(y)}{\underset{\shortparallel}{v(y^2)}} = v(x) + \underset{v(x)}{\underset{\shortparallel}{v(x-1)+v(x+1)}}$$

• $v(x) < 0 \Rightarrow v(x-1) = v(x+1) = v(x)$

$\Rightarrow 2v(y) = 3v(x) \Rightarrow v(x)$ even.

Claim 2: Let $g \in k(t)$. If $v(g)$ is even $\forall$ valuation $v : k(t)^\times \to \mathbb{Z}$, then g is a square.

Proof: $k = \bar{k}$, so we can factor

$$g(t) = \prod (t-a_i)^{n_i}, \quad n_i \in \mathbb{Z},\ a_i \in k.$$

We have $n_i = \mathrm{ord}_{a_i}(g)$, if they all are even then g is a square.

$k(t) = \mathrm{Frac}\, k[t]_{(t-a_i)}$

Claim 3: $x \in L$ is not a square.

Proof: L is a 2-dim. K-vector space with basis $\{1, y\}$.

Assume $x = (a+by)^2$, $a, b \in K$.

Then $x = a^2 + 2aby + b^2 x(x-1)(x+1)$

$\underset{\text{coeff at } y}{\Rightarrow 2ab = 0} \underset{\text{char} \neq 2}{\Rightarrow}$ either $a = 0$ or $b = 0$.

If $b = 0$, then $x = a^2$ in $K = k(x)$, but $\mathrm{ord}_0^K(x) = \overset{\overset{2v(a)}{\nparallel}}{1}$.

If $a = 0$, then $(x-1)(x+1)$ is a square in K, but it has $\mathrm{ord}_1^K = 1$. $\lightning$