Lecture Notes for Algebraic Geometry I

Lecture delivered by Emmanuel Kowalski
Notes by Lin-Da Xiao and David Burgschweiger

2018 ETH

Contents

About the notes

In this notes we mainly focus on the algebraically closed fields.

1 Classical varieties

1.1 Feb 27th: Algebraic sets and morphisms

https://imaginary.org/programs

1.1.1 Affine algebraic sets

Recall: $V(I) \subset \mathbb{A}^n = \{x | \forall f \in I, f(x) = 0\}$.

Definition 1.1. Closed subspaces of $\mathbb{A}^n$ are called **affine algebraic sets** and irreducible algebraic sets are called **affine algebraic varieties**

Definition 1.2. Given Y an affine algebraic set in $\mathbb{A}^n$, we define the **coordinate ring** $\mathcal{O}(Y)$ as $K[X_1, ..., X_n]/I(Y)$.

Definition 1.3. Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be affine algebraic sets. A **morphism** $X \longrightarrow Y$ of affine algebraic sets is a map $f : X \longrightarrow Y$ of the underlying sets such that there exist polynomials $f_1, ..., f_n \in k[T_1, ..., T_m]$ with $f(x) = (f_1(x), ..., f_n(x))$ for all $x \in X$.

We denote the category of affine algebraic sets over K as Alg_K

Theorem 1.4. Let $Y_1 \subset \mathbb{A}^n, X_1, ..., X_n$, $Y_2 \subset \mathbb{A}^m, T_1, , ..., T_m$ affine algebraic sets. There are bijections

$$\begin{aligned} & \mathrm{Hom}_{K-\mathsf{Alg}}(\mathcal{O}(Y_2), \mathcal{O}(Y_1)) \\ & \xleftrightarrow{(*)} \{(f_1, ..., f_m) \in K[X]^m | \forall x \in Y_1, (f_1(x), ..., f_m(x)) \in Y_2)\} \\ & \xleftrightarrow{(**)} \{f : Y_1 \longrightarrow Y_2 | \forall \varphi \in \mathcal{O}(Y_2), \varphi \circ f \text{ is in } \mathcal{O}(Y_1)\} \\ & = \mathrm{Hom}_{\mathsf{Alg}_K}(Y_1, Y_2) \end{aligned}$$

Proof. Key observation:

To give $(f_1, ..., f_m) \in K[X]^m$ is "the same " as giving a ring morphism $g_0 : K[T] \longrightarrow K[X] : T_i \mapsto f_i$, which gives by composition $g_1 = \pi_1 \circ g_0$, where $\pi_1 : K[X] \longrightarrow \mathcal{O}(Y_1)$ is the canonical projection.

$$g_1 : K[T] \longrightarrow \mathcal{O}(Y_1)$$

which has a factorization

$$\begin{tikzcd} K[T] \arrow[r, "g_1"] \arrow[d, "\pi_2"] & \mathcal{O}(Y_1) \\ \mathcal{O}(Y_2) \arrow[ur, "g"] & \end{tikzcd}$$

iff $g_1(I(Y_2)) = 0$, which means

$$g_1(\varphi) = \text{"replace } T_i \text{ by } f_i \text{ in } \varphi\text{"}$$

belongs to $I(Y_1)$ if $\varphi \in I(Y_2)$.

This condition is equivalent to if $x \in Y_1$, then $g_1(\varphi)(x) = 0$. That means $\varphi(f_1(x), ..., f_m(x)) = 0$ for $\varphi \in I(Y_2)$, i.e., $(f_1(x), ..., f_m(x)) \in Y_2$. If $x \in Y_1$. In the statement, this gives the $(*)$ bijection. Any k-algebra morphism $\mathcal{O}(Y_1) \longrightarrow \mathcal{O}(Y_2)$ comes from $K[T] \longrightarrow \mathcal{O}(Y_1)$ s.t. it vanishes on $I(Y_2)$.

For the bijection $(**)$, suppose

$$g : Y_1 \xrightarrow{g} Y_2 \xrightarrow{\varphi} K$$

sends $\varphi \in \mathcal{O}(Y_2)$ to $\varphi \circ g \in \mathcal{O}(Y_1)$. Then the map

$$\begin{aligned} \mathcal{O}(Y_2) &\longrightarrow \mathcal{O}(Y_1) \\ \varphi &\longmapsto \varphi \circ g, \end{aligned}$$

is a K-algebra morphism.

As for the reverse direction, given g a K-algebra morphism $\mathcal{O}(Y_2) \longrightarrow \mathcal{O}(Y_1)$, we get a $\tilde{g} : Y_1 \longrightarrow Y_2$ by the $(*)$ isomorphism.

$$\tilde{g}(x) = (f_1(x), ..., f_m(x))$$

then we have $\varphi \circ g \in \mathcal{O}(Y_1)$ for $\varphi \in \mathcal{O}(Y_2)$. One checks that this shows that the first and third sets are the same. $\square$

Define morphism $Y_1 \longrightarrow Y_2$ by the second(and third) set. Composition in the obvious way and identity is a morphism. $\Longrightarrow$ get a category (Alg_K) of affine algebraic sets over K.

Corollary 1.5. $Y \mapsto \mathcal{O}(Y)$, $g \mapsto [\varphi \mapsto \varphi \circ g]$ is a functor: $(\mathsf{Alg}_K) \longrightarrow (K{-}\mathsf{Alg})^{opp}$.

Proposition 1.6. The "image" of this functor is the category of finitely generated K-algebras which are reduced.

Proof. A is finitely generated reduced K-algebra. (Because A is finitely generated, $\exists n \geq 1$, so that $K[X_1, ..., X_n]/I \cong A$). Then "$A$ is reduced"$\Longleftrightarrow$ I is radical ideal. $\Longrightarrow A = \mathcal{O}(V(I))$, where $V(I) \subset \mathbb{A}^n$. $\square$

Corollary 1.7. There is a equivalence of categories between

$$(\text{Algebraic sets over } K) \longleftrightarrow (\text{finitely generated reduced } K\text{-Algebras.})$$

Example 1.8.

(1) $\mathbb{A}^1 \longrightarrow V(Y^2 - X^3 - X^2) \subset \mathbb{A}^2$, $t \mapsto (t^2 - 1, t(t^2 - 1))$

(2) $\mathbb{A}^1 \longrightarrow V(Y^2 - X^3) \subset \mathbb{A}^2$: $t \longmapsto (t^2, t^3)$ is a bijection but Not an isomorphism.

(3) Assume K with characteristic $p > 0$, $K \supset \mathbb{F}_p$. $Y = V(f_1, ..., f_m)$ where $f_i \in \mathbb{F}_p[X] \subset K[X]$. Consider the morphism:

$$\begin{aligned} Y &\longrightarrow Y \\ (x_1, .., x_n) &\longmapsto (x_1^p, ..., x_n^p). \end{aligned}$$

It is bijective and homeomorphism but not an isomorphism if $dim(Y) \geq 1$.

Proposition 1.9. $Y = V(I) \subset \mathbb{A}^n$

(1) The points of Y are in bijection with maximal ideals $I \subset \mathcal{O}(Y)$ by

$$Y \ni x \longmapsto \{f \in \mathcal{O}(Y) | f(x) = 0\}$$

(2) We have a bijection

$$\mathcal{O}(Y) \longleftrightarrow \text{ Hom}_{Alg_K}(Y, \mathbb{A}^1)$$

Proof. (1) $I_x := Ker(ev_x : \mathcal{O}(Y) \longrightarrow K)$, where $ev_x : f \mapsto f(x)$, since the evaluation map is surjective $[1 \mapsto 1]$, we get an isomorphism

$$\mathcal{O}(Y)/I_x \xrightarrow{\sim} K,$$

so I_x is maximal in $\mathcal{O}(Y)$.

Conversely, if $I \subset \mathcal{O}(Y)$ is maximal, we get $I = I'/I(Y)$ for $I' \subset K[X]$ maximal.

Nullstellensatz says $\exists (x_1, ..., x_n) \in \mathbb{A}^n$ s.t., $I' = (X_1 - x_1, ..., X_n - x_n)$.

Since $I' \supset I(Y)$, we get $(x_1, .., x_n) \in Y$. Then we check that $\mathcal{O}(Y) \longrightarrow \mathcal{O}(Y)/I \cong K$ is just given by $f \mapsto f(x_1, ..., x_n)$. That means $I = I_x$.

(2) We saw in 1.4, that there is a bijection between sets

$$\text{Hom}_{\mathsf{Alg}_k}(Y, \mathbb{A}^1) \longleftrightarrow \text{ Hom}_{K-\mathsf{Alg}}(\mathcal{O}(\mathbb{A}^1), \mathcal{O}(Y)).$$

But $\text{Hom}_{K-\mathsf{Alg}}(\mathcal{O}(\mathbb{A}^1), \mathcal{O}(Y)) = \text{ Hom}_{K-\mathsf{Alg}}(K[X], \mathcal{O}(Y)) \cong \mathcal{O}(Y)$ (by $g : \mathcal{O}(\mathbb{A}^1) \longrightarrow \mathcal{O}(Y)$, $g \mapsto g(X)$) $\square$

1.1.2 Projective Algebraic sets: Introduction

Projective sets can have a good notion of "compactness".

N.B. Any $Y \in (\mathsf{Alg}_K)$ is **quasi-compact**(open cover have a finite subcover).

Definition 1.10. $\mathbb{P}^n_K = \mathbb{P}^n$ can be either defined as

"**the set of lines in $\mathbb{A}^{n+1}$ that pass through the origin**"

or

"**the equivalence classes of points in $K^{n+1}\backslash\{0\}$ with the equivalence relation $x \sim y$ iff $x = \lambda y$ for some $\lambda \in K$**" and we use the notion $[x_0 : ... : x_n]$ for the equivalence class of $(x_0, .., x_n)$

These two definitions are equivalent:

Given a line $l \in \mathbb{A}^1 \longleftrightarrow$ hyperplane in K^{n+1}, corresponds to a equation

$$a_0X_0 + ... + a_nX_n = 0$$

with at least one of a_i non-zero.

Conversely, from $[x_0 : .. : x_n]$, we we get the corresponding hyperplane/line trivially.

Notes the following fact:

$$\mathbb{P}^n = \cup_{0 \leq i \leq n} H_i,$$

where $H_i = \{[x_0, ..., x_n] | x_i \neq 0\}$ and there is a bijection

$$\begin{aligned}
&H_i \longrightarrow K^n \\
&[x_0 : ... : x_n] \longmapsto \left(\frac{x_0}{x_i}, ..., \widehat{\frac{x_i}{x_i}}, .., \frac{x_n}{x_i} \right) \\
&[y_1 : ... : y_{i-1} : 1 : y_i : ... : y_n] \longleftarrow\!\shortmid (y_1, ..., y_n)
\end{aligned}$$

We define from linear algebra some notions in $\mathbb{P}^n$. A line in $\mathbb{P}^n$ is the image by the projection $K^{n+1}\backslash\{0\} \longrightarrow \mathbb{P}^n$ of the **two** dimensional affine subspace. In particular, this notion of line also join two points. For example, the projective line joining $p = [1 : 0 : 0]$ and $q = [a : b : c]$ has the coordinates $[u + va : vb : vc], u, v \in K$.

Example 1.11. $l_1, l_2 \subset \mathbb{P}^2$ lines $l_1 \cap l_2$ is a line if l_1 and l_2 are identical and would be a single point otherwise.

Observation: If $f \in K[X_0, ..., X_{n+1}]$ is homogeneous, then for $x \in \mathbb{P}^n$, it makes no sense to say somthing like "$f(x) \in K$" but the zero-loci or the set where $f(x) \neq 0$ does make sense.

Definition 1.12. A **projective algebraic set** $S \subset \mathbb{P}^n$ is

$$S = \{x \in \mathbb{P}^n | f_1(x) = ... = f_m(x) = 0\},$$

where $f_1, ..., f_m$ are homogeneous of some degrees.

An irreducible projective algebraic set is called a **projective variety**

Notation: $V(f_1, .., f_n)$

Example 1.13. $V(Y^2Z - X^3 - XZ^2) \subset \mathbb{P}^2$.

Let $0 \leq i \leq n$, then $S \cap H_i = \{[x_0 : ... : x_n] \in S | x_i \neq 0\}$ is , via the bijection $H_i \longrightarrow K^n$, in bijection with an affine algebraic set $S_1 \subset \mathbb{A}^n$ given by $\tilde{f}_1(y) = ... = \tilde{f}_m(y) = 0$, where $\tilde{f}_i(y_1, .., y_n) = f_i(y_1, ..., y_{i-1}, 1, y_i, ..., y_n)$

1.2 Mar 2nd: Projective algebraic sets and regular functions

Recall: $\mathbb{P}^n_K = K^{n-1} - \{0\}/\sim$, and $H_i := \{[x_0 : ... : x_n] | x_i \neq 0\}$ is in bijection with $\mathbb{A}^n$. $V(f_1, ..., f_m) = \{x \in \mathbb{P}^n | \forall i, f_i(x) = 0\}$, where $f_1, ..f_m$ are homogeneous.

More generally, we can define

$$V(I) = V(\text{homogeneous element of } I) = V(\cup_{d \geq 0} I_d \text{ as a set})$$

where I is an homogeneous ideal of $K[X_0, ..., X_n]$ that is $I = \oplus_{d \geq 0} I_d$, I_d the the degree d piece of $K[X_0, ..., X_n]$.

Conversely, given $S \subset \mathbb{P}^n$, we can define

$$I(S) := \text{ideal generated by homogeneous polynomials that vanishes on } S$$

Lemma 1.14. This is indeed a homogeneous ideal, i.e., $I(S) = \oplus_d I(S)_d$

Proof. $f \in I(S) \implies f = \sum_{i \in I} g_i f_i$, where f_i is homogeneous and vanishes on S. We can expand each g_i as $\sum_j g_{ij}$, where each g_{ij} is homogeneous in $I(S)$. Then we know $f \in \oplus I(S)_d$ and the converse is clear. □

Lemma 1.15. The projective sets $V(I)$ where I is homogeneous form the closed sets of a topology. It is called the **Zariski topology** (same name for the induced topology on projective sets).

Example 1.16. $H_0 \subset \mathbb{P}^n$ and $\sigma : H_0 \cong \mathbb{A}^n$. Under this bijection, with respect to the Zariski topologies, the σ is a homeomorphism.

$$f \in K[X_0, ..., X_n] \text{ homogeneous} \rightsquigarrow V(f) \subset \mathbb{P}^n$$

$$\tilde{f} = f(1, X_1, ..., X_n) \in K[X_1, .., X_n] \rightsquigarrow V(\tilde{f}) \subset \mathbb{A}^n$$

and $\sigma(V(f)) = V(\tilde{f})$.

Definition 1.17. $Y \subset \mathbb{P}^n$ is projective algebraic set, $S(Y) = K[X_0, ..., X_n]/I(Y)$ is called **homogeneous coordinate ring**

Remark 1.18. Elements in $S(Y)$ are not functions on Y. The geometric meaning of $S(Y)$ will be explained latter with the language of schemes.

We now want to define morphisms of projective algebraic sets. We have to look at it more carefully because we can not simply copy the affine definition.

Definition 1.19. $Y \subset \mathbb{P}^n$ projective, let $V \subset Y$ be an open subsets of Y.

(1) $f : V \longrightarrow K$ continuous is called **regular** on Y if $\forall x \in Y$, $\exists U$ open $x \in U$, $\exists f_1, f_2 \in K[X_0, ..., X_n]$ homogeneous of same degree such that $f_2(x) \neq 0$ for all $x \in U$ and $f(x) = \frac{f_1(x)}{f_2(x)}$ for $x \in U \cap Y$

(2) Y_1, Y_2 are projective sets in $\mathbb{P}^n, \mathbb{P}^m$, $f : Y_1 \longrightarrow Y_2$ is a **morphism** if f is continuous and for any $U \subset Y_1$ open and any $\varphi : U \longrightarrow K$ regular, the composite $\varphi \circ f : f^{-1}(U) \longrightarrow K$ is regular.

<u>Note</u>: IN (2), one can not restrict to φ regular on Y_2 because often the space of such function is reduced to K

Proposition 1.20. For $\mathbb{P}^n$, the space of regular functions on $\mathbb{P}^n$ is K.

Proof. The case $n = 1$ implies the general case: if $f : \mathbb{P}^n \longrightarrow K$ regular, and $x \neq y$ in $\mathbb{P}^n$, the line joining x to y in $\mathbb{P}^n$ is "isomorphic" to $\mathbb{P}^1$ and $f|_L$ is regular so constant, hence $f(x) = f(y)$.

For $n = 1$, suppose x, y are arbitrary points and let $U \ni x$, $V \ni y$ be open neighbourhoods such that $f|_U = f_1(x)/f_2(x)$ and $f|_V = g_1(x)/g_2(x)$ where f_1, f_2, g_1, g_2 are homogeneous polynomials and f_1, f_2 have the same degree as well as g_1, g_2. We may assume that f_1 and f_2 are coprime and also g_1, g_2 are coprime. Hence on $U \cap V$,

$$f_1 g_2 = g_1 f_2.$$

We know that $U \cap V$ is infinite so this implies $f_1 = g_1$ and $f_2 = g_2$. Since x and y were arbitrary points we conclude that $f = f_1(x)/f_2(x)$ on all of $\mathbb{P}^1$ hence f is a constant. □

Concretely: To say that $f : Y_1 \subset \mathbb{P}^n \longrightarrow Y_2 \subset \mathbb{P}^m$ is a morphism of projective algebraic sets. It reduces to $\forall x \in Y_1, \exists U$ open containing x s.t. there exists $f_0, ..., f_m \in K[X_0, ..., X_{n+1}]$ homogeneous of same degree, with no common zero in U, such that $\forall y \in U \cap Y_1$, $f(y) = [f_0(y) : ... : f_m(y)]$. It is easy to see that if f is of this form, then it is a morphism.

The converse is left as an exercise.

Example 1.21.

(1) Let $g \in Gl_n(K), n \geq 1$. Define

$$f_g : \mathbb{P}^n \longrightarrow \mathbb{P}^n$$

$$[x_0 : ... : x_n] \longmapsto [g(x_0, ..., x_n)]$$

is a morphism. In fact, it is an isomorphism. $f_g^{-1} = f_{g^{-1}}$. It also has some other properties: $f_g = f_{\lambda g}, \lambda \neq 0$ and we get an induced group morphism

$$\begin{array}{ccc} PGL_{n+1}(K) & = & GL_{n+1}(K)/K^\times \\ \big\downarrow & & \\ Aut_{proj}(\mathbb{P}^n) & & \end{array}$$

which is an isomorphism. A special case is $Aut_{hol}(\mathbb{CP}^1) = PGL_2(\mathbb{C})$

$$g \longmapsto \left[z \mapsto \frac{az+b}{cz+d} \right]$$

(2) $K = \mathbb{C}$. One can do holomorphic geometry (using holomorphic functions instead of polynomials). IN $\mathbb{C}^n$,we get a much more complicated picture [e.g. $V(\sin z)$] is a an infinite sets in $\mathbb{P}^n_{\mathbb{C}}$, however Chow proved that the holomorphic sets and the projective algebraic sets are the same (Serre "GAGA" principle compares many different invariant of both categories.)

(3) Consider the map $S := V(Y^2Z - X^3 - XZ^2) \xrightarrow{f} \mathbb{P}^1$, $[x : y : z] \mapsto [y : z]$.
Claim, this is a morphism of projective sets.
This means that there is no solution to $Y^2Z - X^3 - XZ^2 = 0$ with $Y = Z =$

0. (But $[x : y : z] \mapsto [x : z]$ is not a morphism because $[0 : 1 : 0] \in S$). f is surjective but not injective $[x : y : z]$ and $[x : -y : z]$ have same image. This works in field K with Char $K \neq 2$.

(4) $\mathbb{P}^1 \xrightarrow{v} \mathbb{P}^2$, $[x : y] \mapsto [x^2 : xy : y^2]$ (special case of Veronese embedding). This is a morphism. The image of v is equal to $S = V(Y_1^2 - Y_0Y_2) \subset \mathbb{P}^2$. In fact, σ gives an isomorphism $\sigma : \mathbb{P}^1 \longrightarrow S$ with inverse given by

$$\tau : S \longrightarrow \mathbb{P}^1$$

$$[y_0 : y_1 : y_2] \mapsto \begin{cases} [Y_1 : Y_2] \text{ if } Y_2 \neq 0 \\ [Y_0 : Y_1] \text{ if } Y_0 \neq 0 \end{cases}$$

τ is a morphism defined on all of S, because if $[y_0 : y_1 : y_2] \in S$ satisfies $y_0 = y_2 = 0$, it would implie $y_1^2 = y_0y_2 = 0 \Longrightarrow y_1 = 0$

$$\tau \circ \sigma([x : y]) = \tau([x^2 : xy : y^2]) \quad = \begin{cases} [xy : y^2] = [x : y], y \neq 0 \\ [x^2 : xy] = [x : y], x \neq 0 \end{cases}$$

therefore $\tau \circ \sigma = id_{\mathbb{P}^1}$ and $\sigma \circ \tau = id_S$ can proved similarly

One can not find f_0, f_1 in $K[Y_0, Y_1, Y_2]$ s.t. $\tau([y_0 : y_1 : y_2]) = [f_0(y) : f_1(y)]$ globally for all $y \in S$

1.3 Mar 5th: Exercise class

The content covered can be found in Hartshorne, p50ff Proposition 7.4 and Theorem 7.5.

1.4 Mar 6th: Rational/birational maps

$Y \subset \mathbb{A}^n$ algebraic if Y is irreducible, then $\mathcal{O}(Y)$ is an integral domain. Let $K(Y)$ be its quotient field. What is the geometric meaning of $K(Y)$? It is called the **function field** of Y.

We will see

Theorem 1.22. For Y_1, Y_2 affine varieties (irreducible) $K(Y_1) \cong K(Y_2)$ as fields $\Longleftrightarrow \exists U_1 \subset Y_1$ open dense subset and $\exists U_2 \subset Y_2$ open dense subset such that U_1 and U_2 are isomorphic.

Definition 1.23. (Quasi-affine and quasi-projective) varieties)

1. **quasi-affine variety** V is an open subset $V \subset Y$, where $Y \subset \mathbb{A}^n$ is an affine variety. $[V \neq \emptyset \implies V$ dense in $Y \implies V$ irreducible $]$. It is given by the Zariski's topology from Y.
   (1') $V \subset Y \subset \mathbb{P}^n$ where V is an open subset of Y is **quasi-projective**, where Y is projective variety.

2. A regular function $f : V \longrightarrow K = \mathbb{A}^1$, where V is quasi-affine is an f such that for all $x \in V$, $\exists U \subset V$ open containing x s.t., $\forall x \in V$, $f(x) = \frac{f_1(x)}{f_2(x)}$ where $f_1, f_2 \in \mathcal{O}(\mathbb{A}^n)$ and $f_2(x) \neq 0$ on U.
   (2') V is quasi-projective variety a regular function f is $\frac{f_1(x)}{f_2(x)}$ f_i homogeneous of same degrees.

3. If V_1, V_2 are <u>Varieties</u> (of any of the four types), then $f : V_1 \longrightarrow V_2$ is a **morphism** if for al open $U \subset V_2$ all $\varphi : U \longrightarrow K$ regular, the composition $\varphi \circ f : f^{-1}U \longrightarrow K$ is also regular.

N.B.

1. This makes sense because if $U \subset V_2$, where V_2 is quasi affine U open, $\implies$ $U \subset V_2 \subset Y$ so U is also quasi-affine in $\mathbb{A}^n$

2. <u>Exercise</u> If f is regular on V, then f is continuous $V \longrightarrow \mathbb{A}^1$. (check that $f^{-1}(\{a\})$ is closed, use that closedness is a local condition.)

3. In the (quasi)-affine case, it is enough to check that $\varphi \circ f$ is regular on V_1 for φ regular on V_2.

4. <u>Notation</u>:
   $$\mathcal{O}(V) = \{f : V \longrightarrow K | \text{ regular}\}$$
   This is a ring of with unity, and because of the condition that for open $V \subset Y$ in a variety Y, either $\mathcal{O}(V) = 0, V \neq \emptyset$ or V is dense in Y, $\implies$ $\mathcal{O}(V)$ integral domain.

Example 1.24.

1. $GL_n(K) = \{x \in M_{n\times n}(K) | \det(x) \neq 0\} \subset \mathbb{A}^{n^2}$ is quasi-affine since $\det : M_{n\times n}(K) \longrightarrow K$ is continuous and not emptyset.

2. In fact, for any $0 \neq f \in \mathcal{O}(\mathbb{A}^n)$
   $$U_f = \{x \in \mathbb{A}^n | f(x) \neq 0\}$$

is a quasi-affine variety.

Fact: There is an isomorphism

$$\sigma = \begin{cases} U_f \longrightarrow Y = \{(x,y) \in \mathbb{A}^{n+1} | yf(x) = 1\} \\ x \longmapsto \left(x, \dfrac{1}{f(x)}\right) \end{cases}$$

with inverse $(x,y) \overset{\pi}{\longmapsto} x$. (Indeed, $\pi \circ \sigma = Id_{U_f}$, $\sigma \circ \pi = Id_Y$) and π is a morphism: Consider $\varphi \in \mathcal{O}(U_f)$

$$Y \xrightarrow{u} U_f \xrightarrow{\varphi} K$$

then $\varphi \circ \pi(x,y) = \varphi(x)$.

Indeed, for any $x \in U_f$, $\exists f_1, f_2 \in \mathcal{O}(\mathbb{A}^2)\varphi(x) = \frac{f_1(x)}{f_2(x)}, f_2(x) \neq 0$, one can show: assume $f_2(x) = f(x)^d$ then

$$\varphi(x) = \frac{f_1(x)}{f(x)^d} = f_1(x)y^d$$

for $(x,y) \in Y$, so this is regular.

(2) σ is a morphism

$$U_f \xrightarrow{\sigma} Y \xrightarrow{\varphi} K$$

$\varphi \in \mathcal{O}(Y) = K[X_1, ..., X_n, Y]/(Yf(x) = 1)$

$$\begin{aligned} \varphi \circ \sigma(x) = \varphi(x, 1/f(x)) &= \left(\sum_j a_j Y^j\right)|_{Y=1/f(X)} \\ &= \sum_j a_j(x)/f(x)^j \in \mathcal{O}(U_f) \end{aligned}$$

3. $\mathbb{P}^n = \cup_{0 \le i \le n} H_i$, with $H_i = \{[x_0 : ... : x_n] | x_i \neq 0\}$, $H_i \subset \mathbb{P}^n\}$ open , so quasi-projective. The map

$$\begin{cases} H_i \xrightarrow{f_i} \mathbb{A}^n \\ [x_0 : ... : x_n] \longmapsto (\dfrac{x_0}{x_1}, ..., \dfrac{x_{i-1}}{x_i}, \dfrac{x_{i+1}x_i}{,} ..., \dfrac{x_n}{x_i}) \end{cases}$$

is an isomorphism.

Definition 1.25. Y variety, $K(Y) = \{(U,f) | \emptyset \neq U \subset Y \text{ open }, f \in \mathcal{O}(U)\}/\sim$, where $(U_1, f_1) \sim (U_2, f_2)$ iff $f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}$

Fact: $\sim$ is an equivalence relation. We define

$$(U_1, f_1) + (U_2, f_2) = (U_1 \cap U_2, f_1 + f_2)$$

$$0 := (Y, 0), \quad 1 := (Y, 1)$$

Proposition 1.26. Y is quasi-affine, $U \subset Y$ open nonempty.

1. $\mathcal{O}(Y) \hookrightarrow \mathcal{O}(U) \hookrightarrow K(Y)$
   $f \longmapsto f|_U \mapsto (U, f)$
2. $K(Y)$ is a field, and identifies with the fraction field of $\mathcal{O}(Y)$ and of $\mathcal{O}(U)$.
3. if Y is an affine variety, then $\mathcal{O}(Y)$ as defined above coincides with $\mathcal{O}(Y) = K[X_1, ..., X_n]/I(Y)$ as defined in previous sections.

(3′) If $Y = U_f$ for $0 \neq f$ in $\mathcal{O}(\mathbb{A}^n)$, then $\mathcal{O}(Y) = \{f_1/f^d | f_1 \in \mathcal{O}(\mathbb{A}^n, d \geq 0\} = \mathcal{O}(\mathbb{A}^n)_f$ the localization at f.

Proof. (1), The morphism $\mathcal{O}(Y) \longrightarrow \mathcal{O}(U) \longrightarrow K(Y)$ are injective because any $U \subset Y, \neq \emptyset$ is dense.

(2) Let $(U, f) \neq 0$ in $K(Y)$, then $\exists x_0 \in U$, $f(x_0) \neq 0$ in a $V \subset U$, $x_0 \in V$

$$f(x) = \frac{f_1(x)}{f_2(x)}, f_1, f_2 \in \mathcal{O}(\mathbb{A}^n), f_2 \neq 0 \text{ in } V$$

in particular, $f_1(x_0) \neq 0$ and $(U \cap \{f_1(x) \neq 0\}, \frac{f_2(x)}{f_1(x)}) \in K(Y)$, where $U \cap \{f_1(x) \neq 0\} \neq \emptyset$ is the inverse of (U, f) in $K(Y)$.

By (1), $K(Y) \supset \mathcal{O}(Y)$.

Let $(U, f) \in K(Y)$, pick $x \in Y$ so that around x, $f(x) = \frac{f_1}{f_2}$, $f_i \in \mathcal{O}(\mathbb{A}^n)$, then $(U, f) = \frac{(Y, f_1)}{(Y, f_2)}$, so $K(Y)$ is the fraction field of $\mathcal{O}(Y)$.

(3) Write $\mathcal{O}'(Y) = K[X]/I(Y)$. Note $K[X.., Y]/I(Y)$ identifies to a ring of functions on Y, the claim is that this ring is $\mathcal{O}(Y)$.

Observation: For $x \in Y$, to say that $f : Y \longrightarrow K$ is "regular at x" means precisely that $f \in \mathcal{O}'(Y)_{I_x}$, where $I_x = \{f \in \mathcal{O}'(Y) | f(x) = 0\}$. (Localization at a maximal ideal)

So

$$\begin{aligned} \mathcal{O}(Y) &= \bigcap_{x \in Y} \mathcal{O}'(Y)_{I_x} \\ &= \bigcap_{\mathfrak{m} \subset \mathcal{O}'(Y)} \mathcal{O}'(Y)_{\mathfrak{m}} \\ &= \mathcal{O}'(Y) \end{aligned}$$

the second equality from Nullstellensatz and the third from commutative algebra.

(3′) Similarly, using characterization of maximal ideals in $A_f, f \neq 0$ □

Definition 1.27. K(Y) is called the fraction or function field of Y

Example 1.28. $K(\mathbb{A}^n) = K(\mathbb{P}^n) = K(X_1, .., X_n)$

Definition 1.29. (Rational maps) Y_1, Y_2 varieties. A **rational map** $f : Y_1 \dashrightarrow Y_2$ is a pair $(U, \tilde{f})$ where $U \neq \emptyset$ in Y_1 and $\tilde{f} : U \longrightarrow Y_2$ is a morphism with $(U, \tilde{f}) = (U', \tilde{f}')$ iff

$$\tilde{f}|_{U \cap U'} = \tilde{f}'|_{U \cap U'}$$

[Check: this is coherent, i.e., this is an equivalence relation]

Definition 1.30. $f : Y_1 \dashrightarrow Y_2$ is a **dominant** if its image $\tilde{f}(U) \subset Y_2$ is dense.

Example 1.31. (1) there is a bijection $\{Y \dashrightarrow \mathbb{A}^1\} = K(Y)$

$$\begin{array}{cc} (U, \tilde{f}) & (U, f) \\ \tilde{f} : U \longrightarrow \mathbb{A}^1 \text{ morphism} & f : U \longrightarrow K \text{ regular} \end{array}$$

So it is enough to check

$$\mathrm{Hom}_{Var}(U, \mathbb{A}^1) = \mathcal{O}(U)$$

Left as exercise

(2) $Y, f_1, f_2, f_3 \in \mathcal{O}(Y)$

$$\begin{cases} Y \dashrightarrow \mathbb{P}^2 \\ x \longmapsto [f_1(x) : f_2(x) : f_2(x)] \end{cases}$$

defined on $\{x | f_i(x) \text{ are not all zero}\}$, which is open if any of the 3 sections is non-zero.

Theorem 1.32. Y_1, Y_2 varieties

$\exists \{Y_1 \overset{f}{\dashrightarrow} Y_2 | f \text{ dominant}\}$

$\overset{bij}{\longleftrightarrow}$

$K(Y_2) \longrightarrow K(Y_1)$

Corollary 1.33. Y_1, Y_2 varieties. Y_1 and Y_2 are birational

iff $K(Y_1)$ is isomorphic to $K(Y_2)$

iff $\exists U \subset Y_1$ open $\neq \emptyset$ $\exists V \subset Y_2$, open $\neq \emptyset$ so that U and V are isomorphic as varieties.

Corollary 1.34. Any variety Y of dimension $d \geq 0$ is birational to a hypersurface $V \subset \mathbb{P}^{d+1}$

Proof. (1) Given $Y_1 \overset{f}{\dashrightarrow} Y_2$ dominant, we want a morphism $K(Y_2) \longrightarrow K(Y_1)$.

Let $(U, \tilde{f}) = f$, (V, φ), $\varphi : V \longrightarrow K$ in $K(Y_2)$

$$\varphi \circ f : \tilde{f}^{-1}(V) \longrightarrow K$$

is in $K(Y_1)$, provided $\tilde{f}^{-1}(V)$ is dense, it is enough that $\tilde{f}^{-1}(V) \neq \emptyset$, $\tilde{f}(U) \cap V \neq \emptyset$, since V is open and $\tilde{f}(U)$ is dense.

(2) Given $i : K(Y_2) \longrightarrow K(Y_1)$. Let $\tilde{Y_2} \subset Y_2 \subset \mathbb{A}^n$ open quasi-affine so that $K(Y_2) = K(\tilde{Y_2}) = Frac(\mathcal{O}(\tilde{Y_2}))$

Let $X_1, .., X_n$ be the coordinates in $\mathbb{A}^n$ as elements of $\mathcal{O}(\tilde{Y_2})$, then let

$$f_j = i(X_j) \in K(Y_1)$$

$f_j \longleftrightarrow (U_j, \tilde{f_j})$ with $U_j \subset Y_1$ dense and $\tilde{f_j} \in \mathcal{O}(U_j)$. Then $f_j \longleftrightarrow (U, \tilde{f_j})$, $U := U_1 \cap ... \cap U_n$ still dense.

Define $U \longrightarrow \tilde{Y_2} \hookrightarrow Y_2$ by

$$x \longmapsto (\tilde{f}_1(x), ..., \tilde{f}_n(x)).$$

This is a rational map $Y_1 \dashrightarrow Y_2$

□

1.5 Mar 9th: Continue and Nonsingular varieties

Recall

Theorem 1.35. Y_1, Y_2 varieties

$$\{\text{dominant } Y_1 \dashrightarrow Y_2\} \longleftrightarrow \{K(Y_2) \hookrightarrow K(Y_1)\}$$

Corollary 1.36. The followings are equivalent:

- Y_1 and Y_2 are birational
- the function field $K(Y_1)$ and $K(Y_2)$ are isomorphic
- $\exists \emptyset \neq U \subset Y_1$, $\emptyset \neq V \subset Y_2$ and isomorphism between U and V

Proof. The last condition implies the second because $K(Y_1) = Frac(\mathcal{O}(U)) \cong Frac(\mathcal{O}(V)) = K(Y_2)$. Assume we have rational maps

$$\begin{tikzcd} Y_1 \arrow[r, dashed, "f_2"] & Y_2 \arrow[r, dashed, "f_2"] & Y_1 \end{tikzcd}$$

with $f_2 \circ f_1 = id_{Y_1}, f_2 \circ f_1 = id_{Y_2}$.

Let $f_1 = (U', \tilde{f}_1), f_2 = (V', \tilde{f}_2)$

$$\begin{tikzcd} Y_1 \arrow[rr, dashed, "f_1"] & & Y_2 \arrow[rr, dashed, "f_2"] & & Y_1 \\ U' \arrow[u, hook] \arrow[urr, "\tilde{f}_1"'] & & V' \arrow[u, hook] \arrow[urr, "\tilde{f}_2"'] & & \end{tikzcd}$$

$$f_2 \circ f_1 = (Y_1, Id_{Y_1})$$

so $\tilde{f}_2(\tilde{f}_1(x)) = x$ if $\tilde{f}_1(x) \in V'$. Similarly, $f_1 \circ f_1 = (\tilde{f}_2^{-1}(U'), \tilde{f}_1 \circ \tilde{f}_2)$. Define $U = \tilde{f}_1^{-1}(\tilde{f}_2^{-1}(U')) \subset U'$, which is a dense open subset. Also we have $V = \tilde{f}_2^{-1}(\tilde{f}_1^{-1}(V'))$.

<u>Claim</u>: $U \xrightarrow{\tilde{f}_1} V \xrightarrow{\tilde{f}_2} U$ and then $\tilde{f}_1|_U, \tilde{f}_2|_U$ are reciprocal isomorphism.

We check that if $x \in U$, then $\tilde{f}_1(x) \in V$. Let $y = \tilde{f}_1(x) \in V'$ so $\tilde{f}_2(y) = \tilde{f}_2(\tilde{f}_1(x)) = x$ so $\tilde{f}_1(\tilde{f}_2(y)) = \tilde{f}_1(x) \in V' \Longrightarrow y \in V$. Similarly for f_2. $\square$

Definition 1.37. A **rational variety** Y is a variety Y birational to $\mathbb{P}^n$ for some n (or to $\mathbb{A}^n$). BY the theorem above we know $\exists n, K(Y) \cong K(X_1, ..., X_n)$.

A **unirational variety** Y is a variety s.t. there is a dominant $\mathbb{P}^n \dashrightarrow Y$ for some n, by theorem above $\exists n, K(Y) \hookrightarrow K(X_1, ..., X_n)$ We obviously have

$$\text{Unirational} \Longleftarrow \text{rational}$$

but

$$\text{Unirational} \overset{?}{\Longrightarrow} \text{rational}$$

For char $= 0$: $\dim Y = 1$ or 2, Luroth and some italian showed that unirational curves or surfaces are rational.

First example in char 0 of non-rational unirational varieties were provided by Clemens-Griffith: certain cubic hypersurfaces in $\dim 3$.

Iskovskih-Manin "general " quantic hypersurfaces of $\dim 3$.

Corollary 1.38. Any variety Y is birational to a hypersurface in $\mathbb{P}^{\dim(Y)+1}$ or $\mathbb{A}^{\dim(Y)+1}$.

Proof. Let $d = \dim(Y) = \dim(\mathcal{O}(Y))$. Then a fact in commutative algebra says $K(Y)$ is a finite separable extension of $K(X_1, ..., X_d) =: E$. By the primitive element theorem, there exists $\alpha :\in K(Y)$ such that $K(Y) = E(\alpha)$. Let $f \in E[T]$ be the minimal polynomial of α.

Write

$$f = \sum_{i=0}^{n} a_i T^i = \sum_{i=0}^{n} \frac{b_i}{c_i} T^i,$$

where $a_i \in E$ and $a_i, b_i \in A = K[X_1, ... X_d]$

$\implies \tilde{f}(\alpha) = 0$ where $\tilde{f} = (\prod c_i) f \in A[T] = K[X_1, ..., X_d, T]$. Define $\tilde{Y} = V(\tilde{f}) \subset \mathbb{A}^{d+1}$. This is what we wanted.

(1) $\tilde{Y}$ is an irreducible hypersurface.

(2) $\tilde{Y}$ is birational to $Y \iff K(\tilde{Y}) = K(Y)$

Step 1: Need $\tilde{f}_1 \in K[X_1, ..., X_d, T]$ irreducible. Suppose $\tilde{f} = \tilde{f}_1 \tilde{f}_2, \tilde{f}_i \in A[T] \implies E \ni f = \frac{\tilde{f}_1}{\prod c_i} \tilde{f}_2$ factors in $E[T]$, since f is irreducible in $E[T]$, one of $\deg(\tilde{f}_1)$ or $\deg(\tilde{f}_2)$ is zero

$\implies \tilde{f}$ is irreducible.

Step (2): $\mathcal{O}(\tilde{Y}) = K[X, T]/(\tilde{f})$. We have an injective morphism

$$\begin{cases} \mathcal{O}(\tilde{Y}) \longrightarrow K(Y) = E(\alpha) \\ \quad X_i \longmapsto X_i \\ \quad T \longmapsto \alpha \end{cases}$$

so the fraction field $K(\tilde{Y})$ injects into $K(Y)$. The image of $K(\tilde{Y})$ contains $X_1, ..., X_d$ and α hence it contains $E(\alpha)$, i.e., $K(\tilde{Y}) = K(Y)$ □

Nonsingular varieties

Concrete geometric definition:

Definition 1.39. $Y \subset \mathbb{A}^n$ affine variety $\dim Y = d$, $x \in Y$. We say Y is **nonsingular** at x if for any generating set $\underline{f} := (f_1, ..., f_m)$ of $I(Y)$, the Jacobian matrix at x

$$J_{\underline{f}}(x) = \left(\frac{\partial f_i(x)}{\partial x_j} \right)_{1 \le i \le m, 1 \le j \le n} \in M_{m \times n}(K)$$

has rank $n - d$. If this holds for all x, then we say Y is nonsingular.

Key fact: It suffices to check the rank of $J_F(x)$ for some generating set.
Indeed suppose $\underline{h} = (h_1, .., h_k)$ also generate $I(Y)$ so

$$f_i = \sum_{\ell=1}^{k} g_{i\ell} h_\ell,$$

where $g_{i\ell} \in \mathcal{O}(\mathbb{A}^n)$, $\frac{\partial f_i}{\partial x_j} = \sum_{\ell=1}^{k} \frac{\partial g_{i\ell}}{\partial x_j} h_\ell + \sum_{\ell=1}^{k} g_{i\ell} \frac{h_\ell}{x_j}$
At x where $h_\ell(x) = 0$, we get

$$\frac{\partial f_i}{x_j}(x) = \sum_{\ell=1}^{k} \frac{\partial g_{i\ell}}{\partial x_j} h_\ell$$

$$\implies J_{\underline{f}}(x) = M J_{\underline{h}}(x)$$

so rank $J_{\underline{f}}(x) \leq$ rank $J_{\underline{h}}(x)$. Exchanging $\underline{f}, \underline{h}$, we get the equality.

Example 1.40.

(1) If $K = \mathbb{C}$, the implicit function theorem says that around a point where $J_{\underline{f}}(x)$ has rank $n - d$, then $V(f_1, ..., f_m)$ is diffeomorphic to $\mathbb{C}^d$

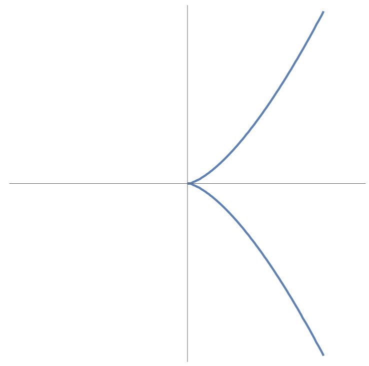
(2) Let $Y = V(f)$, f irreducible in $\mathbb{A}^n$. Then $x \in V(f)$ is nonsingular $\iff$ $(\partial f(x)/\partial x_1, ..., \partial f(x)/\partial x_n) \neq 0$

We have a singular point $\iff$ the system of $n+1$ equations

$$\begin{cases} f(x) = 0 \\ \dfrac{\partial f}{\partial x_1}(x) = 0 \\ \vdots \\ \dfrac{\partial f}{\partial x_n}(x) = 0 \end{cases}$$

has a solution. For instance

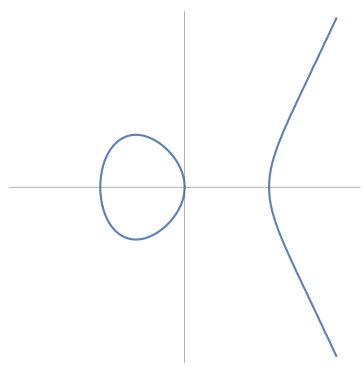
$$Y^2 = X^3$$



$$\begin{cases} f = Y^2 - X^3 \\ \dfrac{\partial f}{\partial X} = -3X^2 \\ \dfrac{\partial f}{\partial Y} = 2Y \end{cases}$$

so $X = Y = 0$ is the only singular point.

$$Y^2 = X^3 - X$$



$$\begin{cases} f = Y^2 - X^3 + X \\ \dfrac{\partial f}{\partial X} = -3X^2 + 1 = 0 \\ \dfrac{\partial f}{\partial Y} = 2Y = 0 \end{cases}$$

If char $k \neq 2$, $\implies Y = 0$, $X^3 - X = 0$ $X = 0, -1, 1$ do not satisfy the system of solutions. In the case char $= 2$, $(1, 0) \in Y$ is singular.

The intrinsic characterization was found by Zariski.

Definition 1.41. $x \in Y$ variety

(1) The **local ring** of Y at x

$$\begin{aligned}\mathcal{O}_{Y,x} &= \{f \in K(Y) | f \text{ defined at } x\}\\ &= \{\text{ regular functions on some } U \ni x\}/(f_1 \sim f_2 \text{ if they coincide on } U_{f_1} \cap U_{f_2})\end{aligned}$$

if Y is affine, then $\mathcal{O}_{Y,x} = \{f_1/f_2 \in K(Y) \mid f_i \in \mathcal{O}(Y), f_2(x) \neq 0\} = \mathcal{O}(Y)_{\mathfrak{m}_x}$, where $\mathfrak{m}_x = \{f \in \mathcal{O}(Y) | f(x) = 0\}$ is the maximal ideal corresponding to x.

$$\mathcal{O}(Y) \subset \mathcal{O}_{Y,x} \subset K(Y)$$

Definition 1.42. $Y \subset \mathbb{A}^n$ affine $x \in Y$. The (Zariski) cotangent spaces of Y at x is the K-vector space

$$\mathfrak{m}_{Y,x}/\mathfrak{m}_{Y,x}^2,$$

where $\mathfrak{m}_{Y,x} \subset \mathcal{O}_{Y,x}$ is the maximal ideal

Remark 1.43. $\mathcal{O}_{Y,x}$ is a local ring, it has a unique maximal ideal $\mathfrak{m}$ which is $\mathcal{O}_x\mathcal{O}_{Y,x}$ in the affine case. Moreover $\mathcal{O}_{Y,x}/\mathfrak{m} = K$ by $f \mapsto f(x)$.

N.B. Intuitively, the Taylor expansion of $f \in \mathcal{O}_{Y,x}$ about $x \in \mathfrak{m}_{Y,x}$ is

$$f(X) = f(x) + \sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(x)(X - x_j) + \dots$$

if $f \in \mathfrak{m}_{Y,x}$ then $f(x) = 0$ and terms of order ≥ 2 belongs to $\mathfrak{m}_{Y,x}^2$, so f has image

$$\sum \frac{\partial f}{\partial x_j} dX_j \in \mathfrak{m}_{Y,x}/\mathfrak{m}_{Y,x}^2$$

where $dX_j = X - x_j$.

Definition 1.44. A local ring $\mathcal{O}$ with maximal ideal $\mathfrak{m}$ is callled **regular** if

$$\dim \mathcal{O} = \dim_k \mathfrak{m}/\mathfrak{m}^2$$

where $k = \mathcal{O}/\mathfrak{m}$ is the residue field.

1.6 Mar 13th-A: Continue and proofs

Theorem 1.45. (Zariski) For $x \in Y \subset \mathbb{A}^n$ the following are equivalent:

(1) Y is non-singular at x

(2) $\dim(Y) = \dim_K(\mathfrak{m}_{Y,x}/\mathfrak{m}_{Y,x}^2)$, where $\mathfrak{m}_{Y,x}$ is the maximal ideal in the local ring $\mathcal{O}_{Y,x} := \mathcal{O}(Y)_{\tilde{\mathfrak{m}}_{Y,x}}$ with $\tilde{\mathfrak{m}}_{Y,x} = \{f \in \mathcal{O}(Y) \mid f(x) = 0\}$.

Remark 1.46. One can show $\dim_K \mathfrak{m}_{Y,x}/\mathfrak{m}_{Y,x}^2 \geq \dim(Y)$ so the question is whether it is larger or not.

Proof. Denote $I := I(Y)$, $d = \dim Y$ and $x := (x_1, ..., x_n) \in \mathbb{A}^n$. Let $I_x := (X_1 - x_1, ..., X_n - x_n) \subset \mathcal{O}(\mathbb{A}^n)$ so that $\tilde{\mathfrak{m}}_{Y,x} = I_x/I$. There is an isomorphism of K-vector spaces

$$\theta : \begin{cases} I_x/I_x^2 \longrightarrow K^n \\ \quad f \longmapsto \left(\dfrac{\partial f}{\partial X_j}(x)\right)_{1\leq j\leq n} \end{cases}.$$

To see this, note that $f \in I_x^2$ iff $f = \sum_{i,j} h_{ij}(X_i - x_i)(X_j - x_j)$ and thus each $f \in I_x/I_x^2$ can be expressed as

$$f = \sum_i^n (X_i - x_i)\frac{\partial f}{\partial X_i}(x) + I_x^2.$$

That means each f is uniquely defined by its derivatives and this preserves scalar multiplication.

Let $(f_1, ..., f_m)$ be a generating set of I. Then $(\theta(f_1), ..., \theta(f_m))$ are the columns of $J_{\underline{f}}(x)$ and for any $f \in I$ we can write

$$f = \sum_j g_j f_j$$

for some $g_j \in K[X]$. Thus

$$\frac{\partial f}{\partial X_i}(x) = \sum_{j=1}^n g_j(x)\frac{\partial f_j}{\partial X_i}(x).$$

In vector notation this is

$$\theta(f)_i = \sum_{j=1}^n g_j(x)\theta(f_j)_i.$$

We conclude that the span of the $\theta(f_j)$ is $\theta((I+I_x^2)/I_x^2)$, so

$$\mathit{rank}\ J_{\underline{f}}(x) = \dim_K \theta((I+I_x^2)/I_x^2) = \dim_K (I+I_x^2)/I_x^2.$$

Consider the short exact sequence

$$0 \longrightarrow (I+I_x^2)/I_x^2 \longrightarrow I_x/I_x^2 \longrightarrow I_x/(I+I_x^2) \longrightarrow 0.$$

From this we see that

$$\mathit{rank}\ J_{\underline{f}}(x) + \dim_K I_x/(I+I_x^2) = \dim_K I_x/I_x^2.$$

We already established that the RHS is n hence x is non-singular iff $d = \dim_K I_x/(I+I_x^2)$.

Consider

$$\begin{tikzcd} I_x \arrow[r] \arrow[rr, bend right, "\varphi"'] & \tilde{\mathfrak{m}}_{Y,x} \subset \mathfrak{m}_{Y,x} \arrow[r] & \mathfrak{m}_{Y,x}/\mathfrak{m}_{Y,x}^2 \end{tikzcd}$$

Note $\varphi(I+I_x^2) = 0$ so we get a K-linear map

$$I_x/(I+I_x^2) \longrightarrow \mathfrak{m}_{Y,x}/\mathfrak{m}_{Y,x}^2$$

<u>Claim</u>: This is an isomorphism [$\Longrightarrow$ the theorem]. (a) φ is surjective: $h \in \mathfrak{m}_{Y,x} \subset \mathcal{O}_{Y,x} \subset K(Y)$, $\Longrightarrow h = \frac{h_1}{h_2}$, with $h_1, h_2 \in \mathcal{O}(Y)$ and $h_2(x) \neq 0, h_1(x) = 0$. Then

$$h - \frac{h_1}{h_2(x)} = h_1 \left(\frac{h_2(x) - h_2}{h_2(x) h_2} \right) \in \mathfrak{m}_{Y,x}^2$$

$$\Longrightarrow [h] = \varphi\left(\frac{h_1}{h_2(x)}\right),$$

where $\frac{h_1}{h_2(x)} \in I_x$, so φ is surjective.

(b) $\ker(\varphi) = I + I_x^2 \subset I_x$ (Intuitively, the restriction of f on Y vanishes to order 2 ar x).

<u>Precisely</u>:

$$\mathcal{O}_{Y,x} = (\mathcal{O}(\mathbb{A}^n)/I)_{I_x/I} = \mathcal{O}(\mathbb{A}^n)_{I_x}/I\mathcal{O}(\mathbb{A}^n)_{I_x}$$

the last equality from commutative algebra. $\varphi(f) = 0$ means that $f \mod I$ belongs to $(I_x^2)_{I_x}$ which is an ideal in $\mathcal{O}(\mathbb{A}^n)_{I_x}$ generated by I_x^2

$$f \mod I = \sum_{i,j} (X_i - x_i)(X_j - x_j) h_{ij}$$

$\theta(f \mod I) = 0 \Longrightarrow f \in I + I_x^2$. $\square$

Theorem 1.47. Let $Y \subset \mathbb{A}^n$ affine variety. Then $Y^\circ = \{x \in Y \mid Y \text{ non-singular at } x\}$ is dense open subset.

Corollary 1.48. Any variety Y is birational to a non-singular variety.

Proof. (of theorem)
Let $S = Y - Y^\circ = \{$ singular points $\}$. Then we know

(1) S is closed in Y, indeed fixing $(f_1, ..., f_m)$ generating $I(Y)$

$$S = \{x \mid rank\ J_{\underline{f}}(x) \neq n - d\}$$

One can show that $rank\ J_{\underline{f}}(x \leq n - d)$. So

$$\begin{aligned} S &= \{x \mid rank\ J_{\underline{f}}(x) < n - d\} \\ &= \{x \in Y \mid \text{ for all minors } M \text{ of } J_{\underline{f}} \text{ of size } n-d \text{ are degenerate } \det(M) = 0.\} \end{aligned}$$

is a closed algebraic set in $\mathbb{A}^n$.

(b), $S \neq Y (\Longrightarrow Y^\circ \neq \emptyset$ and open, so is dense).

If $S = Y$, then by the theorem of Zariski, the set of non-singular points in an open set of a hypersurface birational to Y would be empty. This means that we may assume $Y = V(f) \subset \mathbb{A}^{d+1}$ with f non-zero irreducible. Then

$$V(f) \supset S = \left\{ x \in \mathbb{A}^{d+1} | 0 = f(x = \frac{\partial f}{x_1}(x) = ... = \frac{\partial f}{x_d}(x) \right\}$$

so if $S = V(f)$, $\frac{\partial f}{\partial x_1} \in I(V(f)) = f\mathcal{O}(\mathbb{A}^{d+1}) = fK[X_1, .., X_{d+1}]$

$$\Longrightarrow \text{ in char } = 0, \text{ comparing degrees, we have contradiction}$$

$\Longrightarrow$ in chat $p \neq 0$, we get $\frac{\partial f}{\partial x_i} = 0$ for $1 \leq i \leq d$, $\Longrightarrow f \in K[x_1^p, .., X_d^p] \Longrightarrow f = g^p$, contradicting the irreducibility. □

2 Schemes

In this chapter we will mainly follow chap 2 of Hartshorne and chap 1 of Eisenbud-Harris.

2.1 Mar 13th-B: Affine schemes

2.1.1 Motivations

Serious problems with classical approach occurred in late 1950's

(1) Intrinsic definitions (Without embeddings in $\mathbb{A}^n$ or $\mathbb{P}^n$)

(2) Construction of various algebraic varieties especially Jacobian variety of a curve, especially w.r.t. base field (is the Jacobian of a curve given by equation with coefficients in the same field?)

(3) Reduction modulo p of a variety given by equation in $\mathbb{Z}[X_1, .., X_n]$

To attack (1), Serre started from

$$\{\text{alg. set } Y \subset \mathbb{A}^n\} \longleftrightarrow \{\text{fin.gen. reduced } K\text{-algebra}\}$$
$$Y \mapsto \mathcal{O}(Y)$$
$$\{\text{maximal ideals in } A\} \leftarrow\!\shortmid A.$$

Grothendieck tried to remove the restriction on the algebras and managed to interpret it geometrically.

$$\{\text{affine schemes }\} \longleftrightarrow \{\text{all commutative rings.}\}$$

To each ring A, we will associate a geometric object called its **spectrum** denoted $\operatorname{Spec}(A)$.

(1) $\operatorname{Spec} A$ is a set. $\operatorname{Spec} A \neq \{$ maximal ideals $\}$ because this choice is not functorial. If $A_1 \xrightarrow{f} A_2$, we want $\operatorname{Spec}(A_2) \xrightarrow{f^*} \operatorname{Spec}(A_1)$ which would have to be $f^*(\mathfrak{m}) = f^{-1}(\mathfrak{m}) \subset A_1$. But $f^{-1}(\mathfrak{m})$ is <u>NOT</u> necessarily maximal.

Example 2.1. A is an integral domain

$$\{0\} \subset A \hookrightarrow Frac(A) \supset \{0\} \text{ maximal}$$

Definition 2.2. $\operatorname{Spec} A := \{$ prime ideals $\mathfrak{p} \subset A$ $\}$

<u>Fact</u>: If $f : A_1 \longrightarrow A_2$ is a ring morphism then $\mathfrak{p} \mapsto f^{-1}\mathfrak{p}$ gives map of sets

$$\operatorname{Spec} A_2 \longrightarrow \operatorname{Spec} A_1$$

Proof.

$$A_1 \xrightarrow{f} A_2/\mathfrak{p}$$
$$f^{-1}\mathfrak{p} \mapsto 0$$

leads to an injective map

$$A_1/f^{-1}\mathfrak{p} \hookrightarrow A_2/\mathfrak{p},$$

then $A/f^{-1}\mathfrak{p}$ is an integral domain and $f^*(\mathfrak{p})$ is therefore a prime ideal. □

Definition 2.3. If $\mathfrak{p} \in \operatorname{Spec} A$. the fraction field of $A/\mathfrak{p}$ is called the residue field at $\mathfrak{p}$, denoted $\kappa(\mathfrak{p})$.

If $a \in A$, then a defines a function $\tilde{a} : \operatorname{Spec} A \longrightarrow \coprod_{\mathfrak{p}\in \operatorname{Spec}(A)} \kappa(\mathfrak{p})$, $\mathfrak{p} \mapsto a \bmod \mathfrak{p}$

2.1.2 Spec A as a topological space

Definition 2.4. For any set $S \subset A$, let $V(S) = \{\mathfrak{p} \in \operatorname{Spec}(A) | S \subset \mathfrak{p}\}$:

Note:

(1) $V(S) = V($ ideals generated by S $)$

(2) Not always true that $V(S) = V($ finitely many elements$)$

(3) $V(S) = \{\mathfrak{p} \in \operatorname{Spec} A | \forall x \in S, \tilde{x}(\mathfrak{p}) = 0 \in \kappa(\mathfrak{p})\}$

Lemma 2.5.

(1) The sets $V(I)$, I ideal in A, from the closed set s of a topology on $\operatorname{Spec} A$ (called the **Zariski topology**).

(2) $V(I) \subset V(J) \iff \sqrt{J} \subset \sqrt{I}$

(3) If $f : A_1 \longrightarrow A_2$ is a ring morphism, then

$$f^* : \operatorname{Spec}(A_2) \longrightarrow \operatorname{Spec}(A_1)$$

is continuous.

Proof. (1) $\emptyset = V(A) = V(\{1\})$ $\operatorname{Spec} A = V(\{0\})$.

$$\begin{aligned}\cap_{i\in X} V(I_i) &= \{\mathfrak{p} \in \operatorname{Spec}(A) | I_i \subset \mathfrak{p} \text{ for every } i\} \\ &= \{\mathfrak{p} \in \operatorname{Spec}(A) | \sum I_i \subset \mathfrak{p}\} \\ &= V\left(\sum_{i\in X} I_i\right)\end{aligned}$$

$$\begin{aligned}V(I)\cup V(J) &= \{\mathfrak{p} \in \operatorname{Spec}(A) | I \subset \mathfrak{p} \text{ or } J \subset \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} A | IJ \subset \mathfrak{p}\}(\text{because } \mathfrak{p} \text{ prime}) \\ &= V(IJ)\end{aligned}$$

(2) recall the definition of radicals of an ideal

$$\begin{aligned}\sqrt{I} := \{x \in A | \exists k \geq 0, x^k \in I\} \quad &= \cap_{I\subset \mathfrak{p}, \mathfrak{p}\in \operatorname{Spec} A} \mathfrak{p} \\ = \cap_{\mathfrak{p}\in V(I)} \mathfrak{p}\end{aligned}$$

then if $V(J) \subset V(I)$, we get $\sqrt{I} \subset \sqrt{J}$.

Conversely, if $\sqrt{I} \subset \sqrt{J}$ then for $\mathfrak{p} \in V(J)$, then $I \subset \sqrt{I} \subset \sqrt{J} \subset \mathfrak{p} \Longrightarrow \mathfrak{p} \in V(I)$.

(3) □

2.2 Mar 16th: Affine schemes, examples and properties.

Recall

A is a ring with unity $\operatorname{Spec} A = \{$ prime ideals in $A\}$

closed sets: for a subset $S \subset A$, $V(S) = V(I :=$ ideal generated by $S)$ $= \{\mathfrak{p} | I \subset \mathfrak{p}\}$

If $A \xrightarrow{f} B$ is a ring morphism, then $f^* : \operatorname{Spec}(B) \longrightarrow \operatorname{Spec}(A)$: $\mathfrak{p} \mapsto f^{-1}(\mathfrak{p})$ is continuous.

Indeed, let $V(I) \subset \operatorname{Spec} A$ be closed,, then $(f^*)^{-1}(V(I)) = \{\mathfrak{p} \in \operatorname{Spec}(B) | f^*(\mathfrak{p}) \in V(I)\} = \{\mathfrak{p} \in \operatorname{Spec} B | I \subset f^{-1}\mathfrak{p}\} = \{\mathfrak{p} \in \operatorname{Spec} B \mid f(I) \subset \mathfrak{p}\}$, therefore

$$(f^*)^{-1} V_A(I) = V_B(f(I))$$

2.2.1 Examples of Spec A

Example 2.6. $\operatorname{Spec}(\{0\}) = \emptyset$

By definition, this is the only ring with $\operatorname{Spec} A$ empty.

Example 2.7. K algebraically closed field, $\emptyset \neq Y \subset K^n$ affine algebraic set. The corresponding affine scheme is

$$Y^{sc} = \text{ Spec}\,(\mathcal{O}(Y))$$

in other words

$$Y^{sc} = \text{ Spec}\,(K[X_1, ..., X_n]/I(Y) =: A).$$

Maximal ideals of $\mathcal{O}(Y)$ are in bijection with points of Y by

$$x \mapsto \mathfrak{m}_x = \{f \in \mathcal{O}(Y|f(x) = 0\}$$

so we get an injective map

$$\begin{aligned} Y &\xrightarrow{\varphi} Y^{sc} \\ x &\longmapsto \mathfrak{m}_x \end{aligned}$$

This map φ is continuous, when both Y and Y^{sc} are endowed with Zariski topologies.

Let $V(I) \subset Y^{sc}$ be closed and $I \subset \mathcal{O}(Y)$.

$$\begin{aligned} &\varphi^{-1}(V(I)) \\ &= \{x \in Y \mid \mathfrak{m}_x \in V(I)\} \\ &= \{x \in Y \mid I \subset \mathfrak{m}_x\} \\ &= \{x \in Y \mid \forall f \in I, f(x) = 0\} \end{aligned}$$

is a closed algebraic set in K^n.

Observe: for every $x \in Y$, the residue field of $\mathfrak{m}_x$ is $A/\mathfrak{m}_x \cong K$ where the function associated to $f \in A$ is given by

$$\tilde{f}(\mathfrak{m}_x) = f(x).$$

The following are equivalent

1. $Y \xrightarrow{\varphi} Y^{sc}$ is surjective
2. every prime ideal in $\mathcal{O}(Y)$ is maximal
3. $\dim \mathcal{O}(Y) = 0$.

Consider the case $Y = K$ and $Y^{sc} = \operatorname{Spec}(K[X])$ with $\dim Y = 1$. $K[X]$ is a principal ideal domain and K is algebraically closed.

$$Y^{sc} = \{(X - x) | x \in K\} \cup \{0\}$$

where $\eta := \{0\}$ is called the generic point of Y^{sc}.

Claim: $\{\eta\}$ is not closed in Y^{sc}, in fact it is dense

$$\overline{\{\eta\}} = Y^{sc}.$$

Example 2.8. More generally, Let A be an integral domain and $\eta = \eta_A = \{0\} \in \operatorname{Spec} A$.

Claim:

$$\overline{\{\eta\}} = \operatorname{Spec} A$$

Let $\mathfrak{p} \in \operatorname{Spec} A$.

$$\begin{aligned}\overline{\{\mathfrak{p}\}} &= \bigcap_{\mathfrak{p} \in V(I)} V(I) \\ &= \bigcap_{I \subset \mathfrak{p}} V(I) \\ &= V(\sum_{I \subset \mathfrak{p}} I) = V(\mathfrak{p})\end{aligned}$$

$$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}) = \{Q \in \operatorname{Spec}(A) | \mathfrak{p} \in Q\}$$

So:

1. $\overline{\{\eta_A\}} = \operatorname{Spec} A$ if A is an integral domain.
2. $\{\mathfrak{p}\}$ is closed iff $\mathfrak{p}$ is maximal.

Definition 2.9. If $\mathfrak{p} \in \overline{\{Q\}}$, we say that $\mathfrak{p}$ is a **specialization** of Q, and that Q **specializes to** $\mathfrak{p}$.

Example 2.10. Any point is a specialization of η_A if A is integral domain. What is $\kappa(\eta_A)$?

$$A/\{0\} = A$$

so $\kappa(\eta_A) = Frac(A)$.

Back to the Example 2.7

$Y = K$, $Y^{sc} = \operatorname{Spec}(K[X])$, $\eta = \{0\}$ is dense in Y^{sc}, its residue field is $K(X)$.

Remark 2.11. If $f_1, f_2 \in K[X]$ are such that they coincide at η;

$$\tilde{f}_1(\eta) = \tilde{f}_2(\eta)$$

then in fact $f_1 = f_2$ in $K[X]$.

We will often encounter situations like "A property holds at $\eta \implies$ it holds at for all x in an open set"

Example 2.12. A is an integral domain. Any $\emptyset \neq U$ open set in Spec A is dense:

$$U \cap \{\eta\} \neq \emptyset$$

so $\eta \in U, \implies \overline{\{\eta\}} = \overline{U}$

Example 2.13. The Zariski topology is **quasi-compact**: any open covering has a finite subcover. Indeed, suppose

$$\begin{aligned}
&\bigcap_\alpha V(I_\alpha) = \emptyset \\
\iff & V(\sum_\alpha I_\alpha) = \emptyset = V(A) \\
\iff & 1 \in \sum_\alpha I_\alpha \\
\iff & 1 = \sum_{j=1}^m f_{\alpha_j}, f_{\alpha_j} \in I_{\alpha_j} \\
\iff & V(\sum_j I_{\alpha_j}) = \emptyset \\
\iff & \bigcap_j V(I_{\alpha_j}) = \emptyset
\end{aligned}$$

Example 2.14. For any $I \subset A$, $A \xrightarrow{\pi} A/I$ induces

$$\operatorname{Spec}(A/I) \xrightarrow{\pi^*} \operatorname{Spec} A$$

which gives homeomorphism

$$\operatorname{Spec}(A/I) \cong V(I).$$

Example 2.15. K is a field, not necessarily algebraically closed. Let $J \subset K[X_1, .., X_n]$ be an ideal and $Y = \operatorname{Spec}(K[X_1, ..., X_n]/J)$. (Want to understand in particular the relation with the case K is algebraically closed.) Fix $L \supset K$ where L is algebraically closed Then we get an injective ring morphism

$$K[X]/J \longrightarrow L[X]/JL[X]$$

hence a map

$$Y_L := \operatorname{Spec}(L[X]/JL[X]) \longrightarrow Y,$$

where $\operatorname{Spec}(L[X]/JL[X])$ is a classical algebraic set (if J is prime).

Take $Y = \operatorname{Spec}(KX) = \mathbb{A}^1_K$.

Definition 2.16. Let A be any ring. The **affine n-space** $\mathbb{A}^n_A$ over A is $\operatorname{Spec} A[X_1, ..., X_n]$.

What is $\mathbb{A}^1_L \longrightarrow \mathbb{A}^1_K$?

$$\begin{aligned} \mathbb{A}^1_K &= \{\mathfrak{p} \subset K[X] \text{ prime}\} \\ &= \{0\} \cup \{fK[X] \mid f \text{ irreducible and monic}\} \end{aligned}$$

Check: the Zariski topology has closed sets $\emptyset$, $\mathbb{A}^1_K$, finite sets of closed points. Given $i : K[X] \hookrightarrow L[X]$, what is $\mathbb{A}^1_L \xrightarrow{i^*} \mathbb{A}^1_K$? We have that

$$\begin{aligned} i^*(\eta_L) &= i^{-1}(\{0\}) \\ &= \eta_K \end{aligned}$$

which means the image of i^* us dense.

Let $x \in L$

$$\begin{aligned} & i^*(X-x)L[X] \\ &= i^{-1}((X-x)L[X]) \\ &= \{f \in K[X] \mid (X-x)|f \text{ in } L[X]\} \\ &= \{f \in K[X] \mid f(x) = 0\} \end{aligned}$$

Case 1: x is transcendental over K

$$\Longleftrightarrow i^*(x) = \{0\} = \eta_K$$

Case 2: x is algebraic over K

$$i^*(x) = f_x$$

where f_x is the minimal polynomial x over K.

Observe that i^* is not injective more precisely,

$$(i^*)^{-1}(f) = \{\text{ roots of } f \text{ in } L\}$$

where f is irreducible monic.

Example 2.17. Given A, B integral domain $A \xrightarrow{f} B$ is injective iff

$$f^*(\text{ Spec } B) \subset \text{ Spec } A$$

is dense. The proof is left as an exercise.

Example 2.18. $K = \overline{K}$,

Y^{sc} for $Y = \{(x, y) \in K^2 \mid (xy) = 0\}$. ($Y$ is not a variety in this case.)

$$\mathbb{A}^2_K \supset V(xy) \cong Y^{sc} = \text{ Spec } (K[X, Y]/(XY))$$

Check the points of Y^{sc} are

$$\begin{aligned} h_x &= \langle (X - x), Y \rangle \subset K[X, Y]/(XY) \\ v_y &= \langle X, (Y - y) \rangle \end{aligned}$$

because $XY = (X - x)Y + xY$. h_x and v_y are closed points with residue field K. Let

$$\begin{aligned} \eta_1 &= XK[X, Y]/(XY) \\ \eta_2 &= YK[X, Y]/(XY). \end{aligned}$$

We have $\{0\} \notin \text{ Spec } (K[X, Y]/(XY))$ because the ring is not an integral domain.

$$\begin{aligned} \overline{\{\eta_1\}} &= \{\eta_1\} \cup \{\mathfrak{m} \text{ maximal s.t. } X \subset \mathfrak{m}\} \\ &= \{\eta_1\} \cup \{v_y \mid y \in K\}. \end{aligned}$$

Similarly, we have

$$\overline{\{\eta_2\}} = \{\eta_2\} \cup \{h_x \mid x \in K\}.$$

Note $v_0 = h_0$ is a specialization of both η_1 and η_2.

Example 2.19. For $K = \overline{K}$ consider

$$\mathbb{A}^2_K = \{(x, y) \mid (x, y) \in K^2\} \cup \{\eta\} \cup \{fK[X, Y] \mid f \text{ irreducible monic}\}$$

where we identify the maximal ideals $(X - x, Y - y)$ in $K[X, Y]$ with points (x, y). Note that prime ideals of height 1 are principal in a UFD.

$$\overline{\{fK[X, Y]\}} = \{fK[X, Y]\} \cup \{(x, y) \in K^2 | f(x, y) = 0\}$$

For this reason, we denote $\{fK[X, Y]\}$ by η_f because it is the generic point of $V(f)$.

$$\begin{aligned} \overline{\{\eta_f\}} &= \eta_f \cup \text{ classical points on } C_f \\ \kappa(\eta_f) &= K[X, Y]/fK[X, Y] = \kappa(C_f) \end{aligned}$$

where C_f is the classical curve. η_f specializes to the point (x, y) on C_f.

2.3 Mar 20th:

Example 2.20. $A = \mathbb{Z}$, $\operatorname{Spec} A = \{0\} \cup \{p\mathbb{Z} | p \text{ prime number}\}$. Recall $\dim(\mathbb{Z}) = 1$, with residue fields

$$\begin{cases} K(\eta) = \mathbb{Q} \\ K(p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p, \text{ finite field} \end{cases}$$

A statement like " property P is true at η" $\implies$" It is true on any open set" means "a property P true for $\mathbb{Q}$ is also true for mod p for p large enough."

(Topology has closed sets $\emptyset$, $\operatorname{Spec}\mathbb{Z}, V(n\mathbb{Z}) = \{p\mathbb{Z} : p$ **divides** $n\}$, where $V(n\mathbb{Z})$ is a finite set of closed points.)

$$\mathbb{Z} \longrightarrow \mathbb{F}_p \longleftrightarrow \begin{array}{c} \operatorname{Spec}(\mathbb{F}_p) \hookrightarrow \operatorname{Spec}(\mathbb{Z}) \\ \{0\} \in \mathbb{F}_p \mapsto p\mathbb{Z} \end{array}$$

$$\mathbb{Z} \overset{i}{\hookrightarrow} \mathbb{Q} \longleftrightarrow \begin{array}{c} \operatorname{Spec}(\mathbb{F}_p) \xrightarrow{i^*} \operatorname{Spec}(\mathbb{Z}) \\ \{0\} \in \mathbb{F}_p \mapsto \eta \end{array}.$$

In particular, the image of i^* is dense in $\operatorname{Spec}\mathbb{Z}$.

structure sheaf

Note recall we want

$$\{\text{affine schemes}\} \longleftrightarrow \{\text{ commutative rings}\}$$

$$\operatorname{Spec} A \leftarrow\!\shortmid A$$

$$f^* \leftarrow\!\shortmid f$$

This is functorial but cannot capture the whole category of rings because for instance all rings

$$A = K[X]/(X^n), n \geq 1$$

(K is a field). We have $\operatorname{Spec} A = \{XK[X]\}$, independent of K and n. We need to remember what is K and what is n.

We deal with that by defining "regular functions"

Definition 2.21. A is a ring. For $U \subset \operatorname{Spec} A$ open, we define the ring $\mathcal{O}(U)$ of "regular functions on U" by

$$\mathcal{O}(U) = \left\{ s : U \longrightarrow \bigsqcup_{\mathfrak{p} \in U} A_{\mathfrak{p}} \;\middle|\; \begin{array}{l} (1)\ s(\mathfrak{p}) \in A_{\mathfrak{p}} \text{ for } \mathfrak{p} \in U \\ (2) \forall \mathfrak{p} \in U, \exists V \text{ open nbhd of } \mathfrak{p} \text{ in } U \\ \text{ and } a \in A, f \in A, \\ \text{ s.t.} \forall \mathfrak{q} \in V, f \notin \mathfrak{q} \text{ and } s(\mathfrak{q}) = a/f \in A_{\mathfrak{q}} \end{array} \right\}$$

Note: if $V \subset U$ open then $s \mapsto s|_V$ is a ring morphism $res_V^U : \mathcal{O}(U) \longrightarrow \mathcal{O}(V)$ and $res_V^U = id_{\mathcal{O}(U)}$. Then the pair $\left((\mathcal{O}(U))_{U \in \operatorname{Spec} A}, (res_V^U)_{U,V \in \operatorname{Spec} A}\right)$ is a **sheaf of rings** on $\operatorname{Spec} A$.

Definition 2.22. X is a topological space, $\mathcal{C}$ a category,

(1) A $\mathcal{C}$**-presheaf** is sthe data of

  (a) For every open set $U \subset X$, an object $\mathcal{F}(U) = \Gamma(U, \mathcal{F})$ in $\mathcal{C}$.
  (b) For every $V \subset U$ opens in X, a $\mathcal{C}$-morphism $res_V^U : \mathcal{F}(U) \longrightarrow \mathcal{F}(V)$

  such that given U opens in X.

  (i) $res_U^U = id_{\mathcal{F}(U)}$
  (ii) Given $W \subset V \subset\subset U$ opens in X

$$res_W^U = res_W^V \circ res_V^U$$

  <u>Notation:</u> $res_V^U(s) = s|_V$

(2) A $\mathcal{C}$-presheaf is a $\mathcal{C}$**-sheaf** if: for any $U \subset X$ open, for every open covering $U = \cup_\alpha V_\alpha$, for any family $(s_\alpha)_\alpha$ with $s_\alpha \in \mathcal{F}(V_\alpha)$ such that $s_\alpha|_{V_\alpha \cap V_\beta} = s_\beta|_{V_\alpha \cap V_\beta}$, there is a unique $s \in \mathcal{F}(U)$ with $s|_{V_\alpha} = s_\alpha$.

Exercise 2.23. Check that the sheaf of regular functions is indeed a sheaf.

Definition 2.24. A a ring. The **affine scheme** associated to A is $(\operatorname{Spec} A, \mathcal{O})$ where the first data is endowed with Zariski's topology and the $\mathcal{O}$ is the structure sheaf.

Example 2.25. K a field, $\operatorname{Spec} K = \{\eta\}$

$$\begin{cases} \mathcal{O}(\operatorname{Spec} K) = \{s : \eta \longrightarrow K_{\{0\}} = K, \text{ (i.e. } s(\eta) \in K)\} \\ \mathcal{O}(\emptyset) = \{0\} \end{cases}$$

Different K gives different affine schemes.

Proposition 2.26. For $f \in A$, define $U_f = \{\mathfrak{p} \in \operatorname{Spec} A | f \notin \mathfrak{p}\}$

(1) U_f is a open "basic open sets"

(2) We have a canonical isomorphism

$$\begin{cases} A_f \xrightarrow{\psi} \mathcal{O}(U_f) \\ a/f^m \longmapsto (s : \mathfrak{p} \in U_f \mapsto \dfrac{a}{f^m} \in A_{\mathfrak{p}}) \end{cases}$$

In particular, for $f = 1$, we get a canonical isomorphism

$$A = A_1 \xrightarrow{\sim} \Gamma(\operatorname{Spec} A, \mathcal{O})$$

$\Longrightarrow$ the affine scheme of A allows you to recover A.

Proof. (injectivity)

Suppose $\psi\left(\frac{a}{f^m}\right) = 0$. This means that

$$\forall \mathfrak{p} \in U_f, \frac{a}{f^m} = \frac{0}{1} \in A_{\mathfrak{p}}$$

$\Longleftrightarrow \forall \mathfrak{p} \in U_f, \exists h_{\mathfrak{p}} \notin \mathfrak{p}, ha = 0$. Let $I = \{x \in A | xa = 0\}$. I is an ideal and $I \not\subset \mathfrak{p}$ for any $\mathfrak{p} \in U_f$

$\Longrightarrow V(I) \cap U_f = \emptyset$

$\Longrightarrow V(I) \subset V(f)$

$\sqrt{(f)} \subset \sqrt{I}$

$f \in \sqrt{(f)} \in \sqrt{I}$

$\exists k \geq 0, f^k a = 0 \Longrightarrow a/f^m = 0 \in A_f$

(Surjectivity): We need the following lemma

Lemma 2.27.

(1) $U_{f_1} \cap U_{f_2} = U_{f_1 f_2}$

(2) $U_{f^n} = U_f, V(f^n) = V(f)$

(3) U_f is quasicompact

(4) The open sets U_f forms a basis of the Zariski topology.

Consider $\psi : A_f \longrightarrow \mathcal{O}(U_f)$, let $s \in \mathcal{O}(U_f)$.

By definition there exists an open covering of U_f, $U_f = \bigcup_\alpha V_\alpha$, and elements a_α, g_α such that $\forall \mathfrak{p} \in V_\alpha$, $s(\mathfrak{p}) = \frac{a_\alpha}{g_\alpha}, g_\alpha \notin \mathfrak{p}$.

Using the above lemma, we may assume there are finitely many V_α and $V_\alpha = U_{h_\alpha}$.

Observe: $\forall \mathfrak{p} \in U_{h_\alpha} = V_\alpha$, $g_\alpha \notin \mathfrak{p} \Longleftrightarrow \mathfrak{p} \in U_{g_\alpha}$

$$\begin{aligned} & U_{h_\alpha} \subset V_{g_\alpha} \\ & \Longrightarrow V(g_\alpha) \subset V(h_\alpha) \\ & \Longrightarrow \sqrt{(h_\alpha)} \subset \sqrt{(g_\alpha)} \\ & \Longrightarrow \exists n_\alpha, h_\alpha^{n_\alpha} \in (g_\alpha) \end{aligned}$$

So $h_\alpha^{n_\alpha} = c_\alpha g_\alpha$, Now for $\mathfrak{p} \in U_{h_\alpha}$

$$\frac{a_\alpha}{g_\alpha} = \frac{a_\alpha c_\alpha}{g_\alpha c_\alpha} = \frac{a_\alpha c_\alpha}{h_\alpha^{n_\alpha}} \in A_\mathfrak{p}$$

Replacing a_α by $a_\alpha c_\alpha$, g_α by $h^{n_\alpha}\alpha$, Using $U_{h_\alpha^{n_\alpha}} = U_{h_\alpha}$, we reduce to the case where $g_\alpha = h_\alpha$ for all α.

On $U_{h_\alpha} \cap U_{h_\beta} = U_{h_\alpha h_\beta}$, we have

$$\forall \mathfrak{p} \in U_{h_\alpha h_\beta}, \frac{a_\alpha}{h_\alpha} = \frac{a_\beta}{h_\beta} \text{ in } A_\mathfrak{p}$$

$$\Longrightarrow \exists n(\alpha, \beta), (h_\alpha h_\beta)^{n(\alpha,\beta)}(a_\alpha h_\beta - h_\alpha a_\beta) = 0$$

Take n to be the largest of the finite many $n(\alpha, \beta)$

$$\Longrightarrow (h_\alpha h_\beta)^n (a_\alpha h_\beta - h_\alpha a_\beta) = 0$$

$$a'_\alpha h'_\beta - a'_\beta h'_\alpha = 0$$

where $a'_\alpha = a_\alpha h_\alpha^n$ and $h'_\alpha = h_\alpha^{n+1}$

Note $\frac{a'_\alpha}{h'_\alpha} = \frac{a_\alpha}{h_\alpha}$ in $A_\mathfrak{p}$ for all $\mathfrak{p} \in U_{h'_\alpha} = U_{h_\alpha}$.

Now

$$\begin{aligned} & \bigcup_\alpha U_{h'_\alpha} = U_f \\ & V(f) = V(\textstyle\sum(h'_\alpha)) \\ & \Longrightarrow \sqrt{f} = \sqrt{\textstyle\sum(h'_\alpha)} \\ & \Longrightarrow f^k = \sum_\alpha h'_\alpha c_\alpha \quad \text{for some } k \end{aligned}$$

Define

$$a = \sum_\alpha c_\alpha a'_\alpha \in A$$

Fix β,

$$ah'_\beta = \sum_\alpha c_\alpha a'_\alpha h'_\alpha = \sum_\alpha c_\alpha a'_\beta h'_\alpha = a'_\beta f^k$$

$$\implies s(\mathfrak{p}) = \frac{a_\beta}{h_\beta} = \frac{a'_\beta}{h'_\beta} = \frac{a}{f^k}$$

in $A_\mathfrak{p}$ for any $\mathfrak{p} \in U_{h_\beta} = V_\beta$.

So $\psi(\frac{a}{f^k})|_{V_\beta} = s|_{V_\beta}$ for any β. So $\psi(a/f^k)$ and s are elements of $\mathcal{O}(U_f)$ with restrictions equal on open sets forming a covering of U_f, by the uniqueness condition in the definition of sheaf, it follows that $\psi(a/f^k) = s$. □

Proof. (of the lemma)

(1) $U_{f_1} \cap U_{f_2} \stackrel{?}{=} U_{f_1 f_2}$

$$\begin{aligned} V(f_1) \cup V(f_2) &= \{\mathfrak{p} \in \operatorname{Spec} A | f_1 \in \mathfrak{p} \text{ or } f_2 \in \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} A | f_1 f_2 \in \mathfrak{p}\} \end{aligned}$$

(2) $f^n \in \mathfrak{p} \iff f \in \mathfrak{p}, n \geq 1$

(3) Suppose $V(f) \subset \cap_\alpha V(I_\alpha) \implies V(\sum I_\alpha) \supset V(f) \implies \sqrt{(f)} \subset \sqrt{\sum I_\alpha}$

□

2.4 Mar 23th: Sheaves and stalks

Example 2.28. (1) Let X be a topological space. Then

$$\underline{C}(U) = \{f : U \longrightarrow \mathbb{C} \text{ continuous}\}$$

for $U \subset X$ open is a sheaf. For X a manifold we also have that

$$\underline{C}^\infty(U) = \{f : U \longrightarrow \mathbb{C} \text{ smooth}\}$$

is a sheaf and lastly for X a complex manifold the following is a sheaf:

$$\mathcal{H}(U) = \{f : U \longrightarrow U \text{ holomorphic}\}.$$

(2) Let $X = \mathbb{C}^\times$. Then

$$\mathcal{F}(U) = \{f : U \longrightarrow \mathbb{C} \text{ holomorphic and } f = g^2 \text{ for some } g \text{ holomorphic}\}$$

is a pre-sheaf but not a sheaf. A holomorphic function might have a square root locally but not on all of U.

Definition 2.29. Let $\mathcal{F}_1, \mathcal{F}_2$ be $\mathcal{C}$-pre-sheaves on X. A **morphism** $\mathcal{C} : \mathcal{F}_1 \longrightarrow \mathcal{F}_2$ is a collection of morphisms $\varphi_U : \mathcal{F}_1(U) \longrightarrow \mathcal{F}_2(U)$ such that for any $V \subset U$ open we have a commutative square

$$\begin{tikzcd} \mathcal{F}_1(U) \arrow[r, "\varphi_U"] \arrow[d, "res^U_V \text{ for } \mathcal{F}_1"'] & \mathcal{F}_2(U) \arrow[d, "res^U_V \text{ for } \mathcal{F}_1"] \\ \mathcal{F}_1(V) \arrow[r, "\varphi_V"] & \mathcal{F}_2(V) \end{tikzcd}$$

A morphism of sheaves we define to be the same as a morphism of pre-sheaves.

Note that $\mathrm{Id}_{\mathcal{F}(U)} : \mathcal{F}(U) \longrightarrow \mathcal{F}(U)$ gives a morphism and that composition makes sense, i.e. we have that

$$(\varphi \circ \psi)_U = \varphi_U \circ \psi_U.$$

Thus we have now defined the category of $\mathcal{C}$-pre-sheaves and sheaves.

Example 2.30. (1) If X is a complex manifold, there are morphisms

$$\mathcal{H} \longrightarrow \underline{C}^\infty \longrightarrow \underline{C}$$

(2) If $X \subset \mathbb{R}^n$ is a manifold, then

$$\begin{cases} \underline{C}^\infty(U) \longrightarrow \underline{C}^\infty(U) \\ \qquad f \longmapsto \partial f / \partial x_1 \end{cases}$$

is a morphism of sheaves from $\underline{C}^\infty \longrightarrow \underline{C}^\infty$.

Proposition 2.31. Suppose $\mathcal{F}$ is a $\mathcal{C}$-pre-sheaf on X. Then there is a unique, up to unique isomorphism, morphism $\sigma : \mathcal{F} \longrightarrow \mathcal{F}^\sigma$, (the "sheafification" of $\mathcal{F}$) such that for any morphism of presheaves $\varphi : \mathcal{F} \longrightarrow \mathcal{Y}$ there is a unique φ^σ such that $\varphi = \varphi^\sigma \circ \sigma$. In particular $\mathrm{Hom}(\mathcal{F}, \mathcal{Y}) = \mathrm{Hom}(\mathcal{F}^\sigma, \mathcal{Y})$.

$$\begin{tikzcd} \mathcal{F} \arrow[r, "\varphi"] \arrow[d, "\sigma"'] & \mathcal{Y} \\ \mathcal{F}^\sigma \arrow[ur, "\varphi^\sigma"'] & \end{tikzcd}$$

If $\mathcal{F}$ is a sheaf then σ is an isomorphism.

$\mathcal{F}^\sigma$ is called the sheaf associated to $\mathcal{F}$. In order to prove the statement, we need another definition.

Definition 2.32. Suppose $\mathcal{F}$ is a $\mathcal{C}$-presheaf on X. The **stalk** of $\mathcal{F}$ at $x \in X$ is

$$\mathcal{F}_x := \{(U, s) \mid x \in U \subset X \text{ open}, s \in \mathcal{F}(U)\} / \sim$$

with

$$(U_1, s_1) \sim (U_2, s_2) \quad \Longleftrightarrow \quad \exists V \subset U_1 \cap U_2 \text{ s.t. } s_1|_V = s_2|_V \text{ and } x \in V.$$

This is also called the "germs of sections of $\mathcal{F}$ at x".

Proposition 2.33. Let A be a ring and consider $\mathcal{O}_A$ on $\operatorname{Spec} A$. Then the following morphism is an isomorphism:

$$\varphi \begin{cases} \mathcal{O}_{A,p} \longrightarrow A_p \\ (U, s) \longmapsto s(p) \end{cases}$$

Proof. It follows easily from the definitions that φ is well defined. For surjectivity, let $a/f \in A_p$, $f \notin p$. Then we can construct s defined on U_f such that $s(q) = a/f$ in A_q for all $q \in U_f$.

Next, suppose that $s(p) = 0$ for some section (U, s). Then we can write $s(q) = a/f$ for any $q \in V$ where V is an open neighbourhood of p in V. Since $s(p) = 0$, we get $ha = 0$ for some $h \notin p$. But then on $V \cap U_h$, $s \equiv 0$. $\square$

Now we get back to the construction of $\mathcal{F}^\sigma$. Define

$$\mathcal{F}^\sigma(U) := \left\{ s : U \longrightarrow \bigsqcup_{x \in U} \mathcal{F}_x \;\middle|\; \begin{array}{l} \forall x \in U, s(x) \in \mathcal{F}_x \text{ and} \\ \forall x \in U, \exists V \subset U \text{ open, s.t. } x \in V, \\ \exists t \in \mathcal{F}(V) \text{ s.t. } \forall y \in V, s(y) = t_y \end{array} \right\}$$

where t_y denotes the equivalence class $[(V, t)] \in \mathcal{F}_y$. Moreover, define $\varphi^\sigma : \mathcal{F} \longrightarrow \mathcal{F}^\sigma$ by

$$\varphi_U^\sigma(t) = (x \longmapsto t_x)$$

and for $s \in \mathcal{F}^\sigma(U)$, $V \subset U$ let

$$\operatorname{res}_V^U(s)(y) = s(y)$$

for $y \in V$. Finally for a given sheaf $\mathcal{Y}$, let $\varphi_U^\sigma : \mathcal{F}^\sigma(U) \longrightarrow \mathcal{Y}(U)$, such that s maps to the unique $\tilde{s} \in \mathcal{Y}(U)$ such that for all $a \in U$, $V \subset U$ and $t \in \mathcal{F}(V)$ such that $s(y) = t_y$ on V, we have $\tilde{s}|_V = \varphi_V(t)$. Using the sheaf property of $\mathcal{Y}$, we see that such an $\tilde{s} \in \mathcal{Y}(U)$ does exist.

Then $\mathcal{F}^\sigma$ is a presheaf and σ is a morphism. One checks that $\mathcal{F}^\sigma$ is a sheaf (because it is defined by local conditions) and that the universal property holds.

Given $\mathcal{F}$ and $\mathcal{F}^\sigma$, we obtain an isomorphism for all x, $\sigma : \mathcal{F}_x \longrightarrow \mathcal{F}^\sigma_x$ by

$$[(U,x)] \longmapsto [(U, \varphi^\sigma_U(s))].$$

Proposition 2.34. Given sheaves $\mathcal{F}_1$, $\mathcal{F}_2$ on X and a morphism $\varphi : \mathcal{F}_1 \longrightarrow \mathcal{F}_2$, φ is an isomorphism if and only if for every $x \in X$ the induced $\varphi_x : \mathcal{F}_{1,x} \longrightarrow \mathcal{F}_{2,x}$, $[(U,s)] \longmapsto [(U, \varphi_U(s))]$ is an isomorphism.

We omit the proof, it can be found in Hartshorne or Eisenbud.

Remark 2.35. (1) This only holds for sheaves not presheaves.

(2) The ismorphism φ_x need to come from a "global" map $\varphi : \mathcal{F}_1 \longrightarrow \mathcal{F}_2$.

(3) One checks that $\varphi : \mathcal{F}_1 \longrightarrow \mathcal{F}_2$ is and isomorphism iff $\varphi_U : \mathcal{F}_1(U) \longrightarrow \mathcal{F}_2(U)$ are all isomorphisms. One can define φ to be injective if φ_U is injective for all U. However, the correct definition of surjectivity for φ is not equivalent to saying that φ_U is surjective for all U.

Definition/Theorem 2.36. Let X, Y be topological spaces and $f_X \longrightarrow Y$ be continuous, $\mathcal{C}$ be a category and $\mathcal{F}$ be a $\mathcal{C}$-presheaf on X. Define $(f_*\mathcal{F})(U) = \mathcal{F}(f^{-1}(U))$ and $\operatorname{res}^U_V = \operatorname{res}^{f^{-1}(U)}_{f^{-1}(V)}$. Then $f_*\mathcal{F}$ is a $\mathcal{C}$-presheaf and is a sheaf is $\mathcal{F}$ is one. $f_*\mathcal{F}$ is called the **direct image of $\mathcal{F}$ on Y**.

Proof. We check that $f_*\mathcal{F}$ is a sheaf. Let $U \subset Y$ be open, $U \bigcup U_\alpha$ be and open cover for U and let $s_\alpha \in (f_*\mathcal{F})(U_\alpha)$ be such that

$$s_\alpha | U_\alpha \cap U_\beta = s_\beta | U_\alpha \cap U_\beta.$$

Then $s_\alpha \in \mathcal{F}(f^{-1}(U_\alpha))$ and

$$s_\alpha | f^{-1}(U_\alpha) \cap f^{-1}(U_\beta) = s_\beta | f^{-1}(U_\alpha) \cap f^{-1}(U_\beta).$$

Since $f^{-1}(U) = \bigcup f^{-1}(U_\alpha)$ and $\mathcal{F}$ is a sheaf, there is a unique $s \in \mathcal{F}(f^{-1}(U))$ such that $s | f^{-1}(U_\alpha) = s_\alpha$. Hence $s \in (f_*\mathcal{F})(U)$, $s | U_\alpha = s_\alpha$. The uniqueness follows from the same kind reasoning. $\square$

2.5 Mar 27th: Morphism of schemes

Recall: Spec A, Zariski topology $\mathcal{O}_A$ structure sheaf.

Observe: $f : A \longrightarrow B$ ring morphism and

$$\begin{aligned} \tilde{f} : \operatorname{Spec} B &\longrightarrow \operatorname{Spec} A \\ \mathfrak{p} &\longmapsto f^{-1}(\mathfrak{p}) \end{aligned}$$

we also get, (Recall $f_*\mathcal{F}(U) = \mathcal{F}(f^{-1}(U))$)

$$\mathcal{O}(A) \xrightarrow{f^*} \tilde{f}_*\mathcal{O}_B$$

$$\forall U \subset \operatorname{Spec} A, \mathcal{O}_A(U) \longrightarrow \tilde{f}_*\mathcal{O}_B(U) = \mathcal{O}_B(f^{-1}(U))$$

is defined as follows:

To $s \in \mathcal{O}_A(U), s : U \longrightarrow \sqcup_{\mathfrak{p}\in U} A_{\mathfrak{p}}$, such that....
we associated $t : f^{-1}(U) \longrightarrow \sqcup_{Q \in \tilde{f}^{-1}(U)} B_Q$ such that ...
defined

$$t(Q) = f(s(\tilde{f}(Q))), \;\; s(\tilde{f}(Q)) \in A_{\tilde{f}(Q)}$$

where $f(a/b) = f(a)/f(b)$.

$$\begin{aligned} f : A_{f^{-1}(Q)} &\longrightarrow B_Q \\ \frac{a}{b} &\longmapsto \frac{f(a)}{f(b)} \end{aligned}$$

One checks that $t \in \mathcal{O}_B(f^{-1}(U))$ if $s \in \mathcal{O}_A(U)$. IN other words: $f : A \longrightarrow B$ gives

$$(\tilde{f}, f^*) : (\operatorname{Spec} B, \mathcal{O}_B) \longrightarrow (\operatorname{Spec} A, \mathcal{O}_A)$$

Definition 2.37. A **ringed space** is $(X\mathcal{O}_X)$, where X is a topological space and $\mathcal{O}_X$ is a sheaf of rings on X. A **locally ringed space** is a ringed space where $\mathcal{O}_{X,x}$ is a local ring for all $x \in X$. (e.g. $\mathcal{O}_{A,\mathfrak{p}} = A_{\mathfrak{p}}$, where $A_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$).

A morphism of ringed space $f : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ is a pair

$$(f, f^*) : \begin{cases} f : X \longrightarrow Y & \text{morphism of topological spaces} \\ f^* : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X & \text{morphism of sheaves} \end{cases}$$

Ringed space form a category $Id_{(X,\mathcal{O}_X)} = (Id_X, Id_{\mathcal{O}_x})$ and

$$\begin{cases} X \xrightarrow{f} & Y \xrightarrow{g} Z \\ \mathcal{O}_Y \xrightarrow{f^*} f_*\mathcal{O}_X & \\ & \mathcal{O}_Z \xrightarrow{g^*} g_*\mathcal{O}_Y, \end{cases}$$

has composition

$$(g \circ g, g_*(f^*) \circ g^*)$$

where $g_*(f^*)$ is the direct image $\mathcal{F} \longrightarrow g_*\mathcal{F}$ is a functor from (pre)sheaves on Y to sheaves on Z . (Any morphism of sheaves $\varphi : \mathcal{F}_1 \longrightarrow \mathcal{F}_2$ gives a morphism $g_*\mathcal{F}_1 \longrightarrow g_*\mathcal{F}_2$)

A morphism of locally ringed space $(X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ is (f, f^*) $f : X \longrightarrow Y$ is continuous and $\mathcal{O}_Y \xrightarrow{f^*} f_*\mathcal{O}_X$ such that f^* induces for each $x \in X$ a <u>local</u> morphism $\mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$.

Recall that A, B are local rings. $f : A \longrightarrow B$ is <u>local</u> iff $f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$.

<u>Note</u>: $f^{-1}(\mathfrak{m}_B) \subset \mathfrak{m}_A$ because if $f(a) \in \mathfrak{m}_B$ $a \notin A^\times \implies a \in \mathfrak{m}_A$. So the condition to be local is

$$\mathfrak{m}_A \subset f^{-1}(\mathfrak{m}_B) \Longleftrightarrow f(\mathfrak{m}_A) \subset \mathfrak{m}_B$$

Definition 2.38. If $\mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$ f^* gives morphisms

$$\mathcal{O}_Y(U) \xrightarrow{f_U^*} \mathcal{O}_X(f^{-1}(U))$$

for every $y \in Y$

$$\mathcal{O}_{Y,y} \longrightarrow (f_*\mathcal{O}_X)_y$$
$$[(U,s)] \longmapsto [(U, f_U^*(s))].$$

Take $y = f(x)$:

$$\mathcal{O}_{Y,f(x)} \longrightarrow (f_*\mathcal{O}_X)_{f(x)} \longrightarrow \mathcal{O}_{X,x}$$
$$[(U,s)] \longmapsto [(U, f_U^*(s))] \longmapsto [f^{-1}(U), f_U^*(s)]$$

is the desired morphism.

Theorem 2.39. (1) For any $f : A \longrightarrow B$ the pair $(\tilde{f}, \tilde{f}^*)$ is a morphism of locally ringed spaces $(\operatorname{Spec} B, \mathcal{O}_B) \longrightarrow (\operatorname{Spec} A, \mathcal{O}_A)$

(2) Conversely, any morphism of locally ringed spaces $(\operatorname{Spec} B, \mathcal{O}_B) \longrightarrow (\operatorname{Spec} A, \mathcal{O}_A)$ is induced by a morphism of rings.

(3) This gives a equivalence of categories

(commutative rings with unity) $\overset{\simeq}{\longleftrightarrow}$ (affine schemes as locally ringed spaces)

$$\mathrm{Hom}_{rings}(A, B) = \mathrm{Hom}_{loc.r.sp}(\operatorname{Spec} B, \operatorname{Spec} A)$$

Proof. Recall $\mathcal{O}_{A,\mathfrak{p}} = A_{\mathfrak{p}}$ and recall $f : A_{f^{-1}(\mathfrak{q})} \longrightarrow B_{\mathfrak{q}}$ i.e.

$$\mathcal{O}_{A,\tilde{f}(\mathfrak{q})} \longrightarrow \mathcal{O}_{B,\mathfrak{q}}$$

Claim: This is exactly the morphism $\mathcal{O}_{A,\tilde{\mathfrak{q}}} \longrightarrow \mathcal{O}_{B,\mathfrak{q}}$ induced by $\tilde{f}^* : \mathcal{O}_A \longrightarrow \tilde{f}^*\mathcal{O}_B$

Claim2: For every $\mathfrak{q} \in \operatorname{Spec} B$,

$$\begin{aligned} A_{f^{-1}(\mathfrak{q})} &\longrightarrow B_{\mathfrak{q}} \\ a/b &\longmapsto f(a)/f(b) \end{aligned}$$

is a local morphism.

We first prove Claim2, it suffices to check $f(\mathfrak{m}_{A_{f^{-1}(\mathfrak{q})}}) \subset \mathfrak{m}_{B_{\mathfrak{q}}}$

$$f(a/b) = \frac{f(a)}{f(b)} \in \mathfrak{q}$$

$$\begin{tikzcd}
\mathcal{O}_{A,\tilde{f}(\mathfrak{q})} \arrow[rr] \arrow[ddd, "\simeq"'] & & (\tilde{f}^*_*\mathcal{O}_B)_{\tilde{f}(\mathfrak{q})} \arrow[rr] & & \mathcal{O}_{B,\mathfrak{q}} \arrow[ddd, "\simeq"] \\
& (U,s) \arrow[r, mapsto] \arrow[d, mapsto] & (U,\tilde{f}^*_*(s)) \arrow[r, mapsto] & (\tilde{f}^{-1}(U),\tilde{f}^*_*(s)) \arrow[d, mapsto] & \\
& s(f^{-1}(\mathfrak{q})) = s(\tilde{f}(\mathfrak{q})) \arrow[rr, mapsto] & & f(s(\tilde{f}(\mathfrak{q}))) = \tilde{f}^*_*(s)(\mathfrak{q}) & \\
A_{f^{-1}(\mathfrak{q})} \arrow[rrrr, "f"] & & & & B_{\mathfrak{q}},
\end{tikzcd}$$

so this indeed works,

(2) Let $(f,f^*) : (\operatorname{Spec} B, \mathcal{O}_B) \longrightarrow (\operatorname{Spec} A, \mathcal{O}_A)$ be a morphism of locally ringed space/

$$f^* : \mathcal{O}_A \longrightarrow f_*\mathcal{O}_B$$

$$\begin{tikzcd}
\mathcal{O}_A(\operatorname{Spec} A) \arrow[r, "f^*_{\operatorname{Spec} A}"] \arrow[dd, equal] & \mathcal{O}_B(f^{-1}(\operatorname{Spec} A)) \arrow[d, equal] \\
& \mathcal{O}_B(\operatorname{Spec} B) \arrow[d, equal] \\
A \arrow[r] & B.
\end{tikzcd}$$

Let $\varphi = f^*_{\operatorname{Spec} A}$.

<u>Claim</u>: The locally ringed morphism induced by φ is (f, f^*).

To finish the proof of (2), we need to check that the two constructions are reciprocal bijections.

To check the claim, let $\mathfrak{q} \in \operatorname{Spec}(B)$, we have

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d] & B \arrow[d] \\ \mathcal{O}_{A,f(\mathfrak{q})} \arrow[r, "f*_{\mathfrak{q}}"] & B_{\mathfrak{q}} = \mathcal{O}_{B,\mathfrak{q}} \end{tikzcd}$$

We know:

(1) $f^*_{\mathfrak{q}}$ is local

$$\Longleftrightarrow (f^*_{\mathfrak{q}})^{01}(\mathfrak{m}_{B_{\mathfrak{q}}}) = \mathfrak{m}_{A_{f(\mathfrak{q})}}$$

(2) The diagram commutes, because f^* is a morphism of sheaves so compatible with restriction. This implies $f(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q}) = \tilde{\varphi}(\mathfrak{q})$. (Indeed. let $\alpha \in \varphi^{-1}(\mathfrak{q}), \beta = \varphi(\alpha) \in \mathfrak{q} \Longrightarrow \alpha \in f(\mathfrak{q}) \Longrightarrow \varphi^{-1}(\mathfrak{q}) \subset f(\mathfrak{q})$).

$$\begin{tikzcd} \alpha \arrow[r, mapsto] \arrow[d, mapsto] & \beta \arrow[d, mapsto] \\ (*) \arrow[r, mapsto] & (\bullet \in \mathfrak{m}_{B_{\mathfrak{q}}}), \end{tikzcd}$$

where $(*)$ belongs to $\mathfrak{m}_{A_{f(\mathfrak{q})}}$ (because the morphism is local)

Conversely, let $\alpha \in F(\mathfrak{q})$

$$\begin{tikzcd} \alpha \arrow[r, mapsto] \arrow[d, mapsto] & \beta = \varphi(\alpha) \arrow[d, mapsto] \\ (\bullet \in \mathfrak{m}_{A_{f(\mathfrak{q})}}) \arrow[r, mapsto] & (* \in \mathfrak{m}_{B_{\mathfrak{q}}}) \end{tikzcd}$$

since β maps to an element in $\mathfrak{m}_{B_{\mathfrak{q}}}$, we have $\beta \in \mathfrak{q}$, so $\varphi(f(\mathfrak{q})) \subset \mathfrak{q} \Longleftrightarrow f(\mathfrak{q}) \subset \varphi^{-1}(\mathfrak{q})$

Proof of part (3) is left as an exercise. $\square$

Definition 2.40. $(X, \mathcal{O}_X)$ (locally)-ringed space. $U \subset X$ open set. Define $\mathcal{O}_U(V) = \mathcal{O}_X(V)$ for $V \subset U$ open. Then $(U, \mathcal{O}_U)$ is a (locally) ringed space. (in fact $\forall x \in U$, $\mathcal{O}_{U,x} = \mathcal{O}_{X,x}$)

Definition 2.41. A **scheme** S is a locally ringed space $(S, \mathcal{O}_S)$ which is locally isomorphic to affine schemes, i.e. $\forall x \in S \exists U \subset S$ open, $x \in U$, and a ring A such that $(U, \mathcal{O}_U)$ is isomorphic as locally ringed spaces to $(\operatorname{Spec} A, \mathcal{O}_A)$. We view category of schemes as a subcategory of locally ringed spaces.

Examples of schemes/morphisms

Let K be a field. Let S be a scheme with morphism $f : S \longrightarrow \operatorname{Spec} K$.

Affine case: $S = \operatorname{Spec} A$

$$f \longleftrightarrow (K \longrightarrow A)$$

i.e. $f \longleftrightarrow$ structure of K-algebra on A

Example 2.42. $A = K[X_1, ..., X_m]/I$ has morphism $\operatorname{Spec} A \longrightarrow K$.

Global case:

$$f \longleftrightarrow \begin{cases} S \overset{continuous}{\longrightarrow} \operatorname{Spec}(K) = \eta = \{0\} \\ \mathcal{O}_{\operatorname{Spec} K} \longrightarrow f_*\mathcal{O}_S \end{cases}$$

where $\mathcal{O}_{\operatorname{Spec} K}$ consists of

$$\emptyset : \mathcal{O}_K(\emptyset) = \{0\} \longrightarrow \{0\}$$

$$\{\eta\} : \mathcal{O}_K(\eta) = K \longrightarrow (f_*\mathcal{O}_S)(\{\eta\}) = \mathcal{O}_S(S)$$

therefore

$$\{S \longrightarrow \operatorname{Spec} K\} \longleftrightarrow \{K \longrightarrow \mathcal{O}_S(S)\}.$$

Definition 2.43. Let B be a scheme, a scheme **over** B is

$$f : S \longrightarrow B$$

a morphism of schemes.

A morphism of schemes over B is

$$\begin{tikzcd} S_1 \arrow[rr, "g"] \arrow[dr, "f_1"'] & & S_2 \arrow[dl, "f_2"] \\ & B & \end{tikzcd}$$

so that $f_2 \circ g = f_1$.

Global case2: K is a field , $f : \operatorname{Spec} K \longrightarrow S$ corresponds to a point $x = f(\eta) \in S$, $\mathcal{O}_S \longrightarrow f_*\mathcal{O}_{\operatorname{Spec} K}$:

$$\forall U, \mathcal{O}_S(U) \longrightarrow \mathcal{O}_{\operatorname{Spec} K}(f^{-1}(U)) = \begin{cases} \{0\} \text{ if } x \notin U \\ K \text{ if } x \in U. \end{cases}$$

Compatibility with restrictions show that this is equivalent to

$$\mathcal{O}_{S,f(\eta)} = \mathcal{O}_{S,x} \xrightarrow{g} \mathcal{O}_{K,\eta} = K$$

such that $g^{-1}(\{0\}) = \mathfrak{m}_{\mathcal{O}_{S,x}}$, i.e. g passes to the quotient

$$K_S(x) \longrightarrow K.$$

Concretely, "the coordinates of x are in K^n"

2.6 Apr 10th:

Recall: A scheme S is a locally ringed space $(S, \mathcal{O}_S)$, $(\mathcal{O}_{S,x})$ are local rings. s.t. $\forall x \in S$, exists an open set $U \in S$ $x \in U$ and a ring A s.t. $(U, \mathcal{O}_S|_U) \simeq \operatorname{Spec} A$.

We will give some examples of morphism of schemes.

Example 2.44.

(1) A, B are rings.

$$\operatorname{Hom}_{Sch}(\operatorname{Spec} A, \operatorname{Spec} B) = \operatorname{Hom}_{Rings}(B, A)$$

(2) K is a field.

$$[X \longrightarrow \operatorname{Spec} K = \{\eta\}] \Longleftrightarrow [K \longrightarrow \Gamma(X, \mathcal{O}_X)]$$

(also for any $x \in X$, we get $\mathcal{O}_{K,\eta} = K \longrightarrow \mathcal{O}_{X,x} \longrightarrow \kappa(x)$) so every residue field is an extension of K.

(3)

$$[\operatorname{Spec}(K) \xrightarrow{f} X] \Longleftrightarrow [\text{a point } x = f(\eta) \text{ and } \mathcal{O}_{X,x} \xrightarrow{f^*} K]$$

s.t. $\ker(f^*) = \mathfrak{m}_{X,x}$ i.e. $\kappa(x) \hookrightarrow K$.

I.e. $\operatorname{Hom}_{Sch}(\operatorname{Spec}(K), X) \cong \{(x, i) | x \in X, i : \kappa(x) \hookrightarrow K\}$.

In particular, take $X = \operatorname{Spec}(K[X_1, ..., X_n]/(f_1, ..., f_m))$ then using (1), we get

$$\mathrm{Hom}_{Sch}(\operatorname{Spec} K, X) \simeq \mathrm{Hom}_{Rings}(K[X]/I, K).$$

If we only consider morphism over $\operatorname{Spec} K$,

$$\begin{tikzcd}
\operatorname{Spec} K \arrow[rr] \arrow[dr, "id"'] & & X \arrow[dl] \\
& \operatorname{Spec} K &
\end{tikzcd},$$

we look ar $\mathrm{Hom}_{K-alg}(K[X]/I, K)$

K-linear $K[X]/I \longrightarrow K \iff$ giving $x = (x_1, ..., x_n) \in K^n$ s.t. $f_1(x) = ... = f_m(x) = 0$ so

$$\mathrm{Hom}_{Sch\ over\ K}(\operatorname{Spec} K, X)$$

are the K-valued solutions of the equation defining X.

Notation: Any $S \xrightarrow{f} X$ is called an S-valued point of X.

(4) (restriction of morphisms)

$$U \subset X \xrightarrow{f} Y$$

where U is open. We want to restrict f to U, first $(U, \mathcal{O}_X|_U)$ is a locally ringed space. (We will see that it is a scheme.)

Let $f|U : (U, \mathcal{O}_X \mid U) \longrightarrow X$ be defined by

$$(f|U)(x) = f(x) \forall x \in U$$

so $f|U$ is continuous and $\mathcal{O}_Y \xrightarrow{f|_U^*} (f|U)_*(\mathcal{O}_X|U)$ defined by $\forall V \in Y,$ open

$$\mathcal{O}_Y(V) \longrightarrow (\mathcal{O}_X|U)((f|U)^{-1}(V)) = \mathcal{O}_X(U \cap f^{-1}(V))$$

obtained by

$$\mathcal{O}_Y(V) \longrightarrow \mathcal{O}_X(f^{-1}(V)) \xrightarrow{\text{res}} \mathcal{O}_X(f^{-1}(U) \cap V).$$

This is a morphism of ringed spaces. Moreover, we can check that it is a morphism of schemes. On the stalks, the induced morphisms

$$\mathcal{O}_{Y,(f|U)(x)=f(x)} \longrightarrow \mathcal{O}_{X,x}$$

are the same as those from f it self.

Check $V \subset U \subset X \Longrightarrow f|V = (f|U)|V$.

Proposition 2.45. Any $U \subset X$, where X is a scheme, U open , is a scheme.

Note: in general, U is not an affine scheme even if X is affine.

E.g. Let $X = \mathbb{A}^2_{\mathbb{C}} = \operatorname{Spec}(\mathbb{C}[X_1, X_2])$, $U = X - \{(0,0)\}$ open, where the point $(0,0)$ corresponds to the maximal ideal (X_1, X_2). U is not an affine scheme because one can check that

$$\begin{array}{ccc}
\Gamma(U, \mathcal{O}_U) & \xrightarrow{\simeq} & \mathbb{C}[X_1, X_2] \\
\| & & \| \\
\Gamma(U, \mathcal{O}_X|_U) & & \Gamma(X, \mathcal{O}_X) \\
\| & & \\
\Gamma(U, \mathcal{O}_X) & &
\end{array}$$

This phenomenon is an analogy **Hartog's Lemma** in complex geometry, which states that we can extend a holomorphic function defined on the complement of a set of codimension at least two on a complex manifold over the missing set [1].

If U was affine, we would get $U \simeq X$ which is absurd.

Proof of Prop 2.45. $x \in U$, X is a scheme, $\Longrightarrow \exists x \in V \subset X$ open s.t. $V = \operatorname{Spec} A$ is affine. Then $V \cap U$ is an open neighborhood of $x \in U$, and is open in $V = \operatorname{Spec} A$ so it it suffices to check that an open subset of $\operatorname{Spec}(A)$ is a scheme. Recall that the basic open subsets $U_f = \{\mathfrak{p} \in \operatorname{Spec} A | f \notin \mathfrak{p}\}$ form a basis of the topology. So we reduces to showing that U_f is affine. Precisely, U_f is canonically isomorphic to $\operatorname{Spec}(A_f)$. (Topologically, we already constructed a homeomorphism $U_f \xrightarrow{i} \operatorname{Spec}(A_f) : \mathfrak{p} \mapsto \mathfrak{p}A_f$).

To deduce the Proposition, it suffices to have an isomorphism of sheaves

$$\mathcal{O}_{A_f} \xrightarrow{\simeq} i_* \mathcal{O}_{U_f}$$

i.e. for all $V \subset \operatorname{Spec}(A_f)$ open an isomorphism

$$\mathcal{O}_{A_f}(V) \xrightarrow{\simeq} \mathcal{O}_{U_f}(i^{-1}(V))$$

and compatible with restrictions.

Recall: $\mathcal{O}_{A_f}(U) = \left\{ g : U \longrightarrow \sqcup_{Q \in U} (A_f)_Q | g \text{ “locally” } \frac{a}{b}, a, b \in A_f \right\}$

[1]This will work more generally in the algebraic setting: you can extend over points in codimension at least 2 not only if they are “smooth manifold”, but also if they are mildly singular what we will call normal and is called $\boxed{\textit{Hartog's phenomenon}}$ in general.

$$\mathcal{O}_{U_f}(i^{-1}(V)) = \mathcal{O}_A(i^{-1}(V)) = \left\{ \tilde{g} : i^{-1}(V) \longrightarrow \sqcup_{\mathfrak{p}\in A_\mathfrak{p}} \middle| \tilde{g} = \frac{\tilde{a}}{\tilde{b}}, \tilde{a}, \tilde{b} \in A \right\}$$

The morphism $g \mapsto \tilde{g}$ is given by $\tilde{g}(\mathfrak{p}) = g(\mathfrak{p}A_f) = g(i(\mathfrak{p}))$. This works because $a = \tilde{a}/f^n$ and $b = \tilde{b}/f^m$ so $a.b = f^m\tilde{a}/f^n\tilde{b}$ □

Example 2.46. A discrete valuation ring (DVR) is a local ring A with maximal ideal $\mathfrak{m}_A \subset A$ being a principal ideal generated by $\varpi \in A$ ("uniformizer")[2] $A/\mathfrak{m}_A = k$ is the residue field. (Exercise. $A = \{a/b \in \mathbb{Q} | p \nmid b, a \in \mathbb{Z}\}$, $\mathfrak{m}_A = (p), \varpi = p$ is an example of DVR)

Consider a DVR A, $\operatorname{Spec} A = \{\eta = \{0\}, s\}$, where s is the "special point" $s = (\varpi) = \mathfrak{m}_A$. The open sets are $\emptyset$, $\operatorname{Spec} A, \{\eta\}$, $\{\eta\}$ is open because $\{s\}$ is closed. Structure sheaf

$$\mathcal{O}_A(\emptyset) = 0, \mathcal{O}_A(\operatorname{Spec} A) = A, \mathcal{O}_A(\{\eta\}) \simeq A_\varpi = K = Frac(A)$$

(since $A_\varpi = \{\frac{a}{\varpi^n} | a \in A, n \geq 0\}$ and any $b \notin (\varpi)$ is invertible)

$$\kappa(s) = A/\mathfrak{m}_A = k$$

$$\kappa(\eta) = Frac(A/\{0\}) = K$$

$$\operatorname{res}^{\operatorname{Spec} A}_{\{\eta\}} : A \longrightarrow A_\varpi = K$$

is the inclusion. What is the nature of schemes over A?

$$f : X \longrightarrow \operatorname{Spec}(A)$$

<u>Topologically</u>: $X = X_s \sqcup X_\eta$,

$$f(x) = \begin{cases} s, x \in X_s \\ \eta, x \in X_\eta \end{cases}$$

s.t. $f^{-1}(\{\eta\}) = X_\eta$ is open in X. (topology is determined by an open set $X_\eta \subset X$),

<u>sheaf-theoretical point</u>

$$\mathcal{O}_A \longrightarrow f_*\mathcal{O}_X \Longleftrightarrow \begin{tikzcd} A = \mathcal{O}_A(\operatorname{Spec} A) \arrow[r, "f_A^*"] \arrow[d, "\operatorname{res}"'] & \mathcal{O}_X(X) \arrow[d] \\ K = \mathcal{O}_A(\{\eta\}) \arrow[r, "f_\eta^*"'] & \mathcal{O}_X(X_\eta) \end{tikzcd}$$

[2] A is a the local ring at a closed point of a non-singular point of a curve

such that
$$\mathrm{res}^X_{X_\eta}(f_A^*(a)) = f_\eta^*(a)(\text{ viewed a elements of } K).$$
It is locally ringed $\forall x, \mathcal{O}_{A,f(x)} \longrightarrow \mathcal{O}_{X,x}$ local $\Longleftrightarrow \forall x \in X_\eta$, $\mathcal{O}_{A,\eta} = A_\eta = K \longrightarrow \mathcal{O}_{X,x}$ (always local) and $\forall s \in X_s$, $\mathcal{O}_A(\operatorname{Spec} A) = A = \mathcal{O}_{A,s} \longrightarrow \mathcal{O}_{X,x}$, where the equality holds because $\operatorname{Spec} A$ is the only open set that contains s.

Lemma 2.47. For any scheme X, there is a unique morphism $X \longrightarrow \operatorname{Spec}(\mathbb{Z})$. recall $\dim(\mathbb{Z}) = 1$.

Proof. adsfd If $X = \operatorname{Spec} A$, then
$$\mathrm{Hom}_{Sch}(\operatorname{Spec} A, \operatorname{Spec} \mathbb{Z}) = \mathrm{Hom}_{Rings}(\mathbb{Z}, A) = \{1 \mapsto 1\}$$
has a unique element. If X is arbitrary, $X = \cup_i \operatorname{Spec} A_i$ for every i, there is a unique $f_i : \operatorname{Spec}(A_i) \longrightarrow \operatorname{Spec} \mathbb{Z}$. Intuitively, this implies uniqueness $(f, \tilde{f} : X \longrightarrow \operatorname{Spec} \mathbb{Z}) \Longrightarrow f|_{\operatorname{Spec}(A_i)} = f_i = \tilde{f}|_{\operatorname{Spec}(A_i)}$ and thus implies $f = \tilde{f}$.

The existence comes from
$$f_i|_{\operatorname{Spec}(A_i) \cap \operatorname{Spec}(A_j)} = f_j|_{\operatorname{Spec}(A_i) \cap \operatorname{Spec}(A_j)}.$$

Indeed

Proposition 2.48. Given X, Y schemes, $X = \cup_i U_i$ open covering. To give $f : X \longrightarrow Y$ is "the same" as giving $f_i|_{U \longrightarrow Y}$ s.t. $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$.

I.e. $f \mapsto (f|_{U_i})_i$ gives a bijection the set of morphisms $\mathrm{Hom}(X, Y)$ and the set of compatible local morphisms on the open sets

Proof of 2.48. Surjectivity: Given $(f_i)_i$,$f_i : U_i \longrightarrow Y$ satisfying the cocycle relation, construct f?
$$X \xrightarrow{f} Y$$

Topologically: $f(x) = f_i(x)$ if $x \in U_i$ is well-defined since $f_i(x) = f_j(x)$ if $x \in U_i \cap U_j$. f thus defined is continuous (exercise)

Sheaf-theoretically: we need $\mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$: $\forall V \subset Y, \mathcal{O}_Y(V) \xrightarrow{?} \mathcal{O}_X(f^{-1}(V))$. Given $s \in \mathcal{O}_Y(V)$, we get $s_i \in \mathcal{O}_{U_i}(f_i^{-1}(V)) = \mathcal{O}_X(f_i^{-1}(V))$ and $f^{-1}(V) = \cup_i f_i^{-1}(V)$ and $s_i|_{f_i^{-1}(V) \cap f_j^{-1}(V)} = s_j|_{f_i^{-1}(V) \cap f_j^{-1}(V)}$. By the sheaf condition on $\mathcal{O}_X$, there exists a unique $\tilde{s} \in \mathcal{O}_X(f^{-1}(V))$ s.t.
$$\tilde{s}|_{f^{-1}(V_i)} = s_i, \forall i.$$

The map $s \mapsto \tilde{s}$ is the required $\mathcal{O}_Y(V) \longrightarrow \mathcal{O}_X(f^{-1}(V)) \Longrightarrow$ get $\mathcal{O}_Y \xrightarrow{f^*} f_*\mathcal{O}_X$. It is local because if $x \in U_i \subset X$ the induced morphism satisfies

$$\begin{array}{ccc} \mathcal{O}_{Y,f(x)} & \xrightarrow{f^*} & \mathcal{O}_{X,x} \\ \| & & \| \\ \mathcal{O}_{Y,f_i(x)} & \xrightarrow{f_i^*} & \mathcal{O}_{U_i,x}. \end{array}$$

f is local because f_i^* is local. □

□

2.7 Apr 13th-A: Continue, morphism to affine schemes

Example 2.49.

Proposition 2.50. For any scheme X and any ring A, there is a bijection

$$\mathrm{Hom}_{Sch}(X, \operatorname{Spec} A) \simeq \mathrm{Hom}_{Rings}(A, \mathcal{O}_X(X))$$

given by

$$X \xrightarrow{f} \operatorname{Spec} A$$

$$\Longrightarrow \mathcal{O}_A \xrightarrow{f^*} f_*\mathcal{O}_X \Longrightarrow A = \mathcal{O}_{\operatorname{Spec} A}(\operatorname{Spec} A) \longrightarrow \mathcal{O}_X(f^{-1} \operatorname{Spec} A) = \mathcal{O}_X(X)$$

Ex.

(1) $\mathrm{Hom}_{Sch}(X, \operatorname{Spec} K) \longleftrightarrow K \hookrightarrow c\mathcal{O}_X(X)$

(2) $\mathrm{Hom}_{Sch}(X, \operatorname{Spec} \mathbb{Z}) \simeq \mathrm{Hom}(\mathbb{Z}, \mathcal{O}_X(X))$ has a unique element. ($\operatorname{Spec} \mathbb{Z}$ is the final object in Sch)

(3) $\mathrm{Hom}_{Sch}(X, \mathbb{A}^1_{\mathbb{Z}}) \simeq \mathrm{Hom}(\mathbb{Z}[T], \mathcal{O}_X(X))$

Proof.

$$X = \cup_i U_i, U_i \cong \operatorname{Spec}(A_i) \text{ open in } X$$

$$\begin{aligned} \mathrm{Hom}_{Sch}(X, \operatorname{Spec} A) &= \{(f_i) \mid f_i : U_i \longrightarrow \operatorname{Spec} A \text{ s.t. } f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}\} \\ &\cong \{(g_i) \mid g_i : A \longrightarrow A_i, \text{ which are compatible on intersections}\} \\ &= \{(g_i) \mid g_i : A \longrightarrow \Gamma(U_i, \mathcal{O}_X), \forall a \in A, g_i(a)|_{U_i \cap U_j} = g_j(a)|_{U_i \cap U_j}\} \\ &\simeq \{g | g : A \longrightarrow \mathcal{O}_X(X)\} \text{ by sheaf condition} \\ &= \mathrm{Hom}_{Rings}(A, \mathcal{O}_X(X)) \end{aligned}$$

□

Note in general the dual statement is not true:

$$\mathrm{Hom}_{Sch}(\,\mathrm{Spec}\,A, X) \neq \mathrm{Hom}_{Rings}(\mathcal{O}_X(X), A)$$

Ex. $X = \mathbb{P}^1_K$, $\implies \mathcal{O}_X(X) = K$. If $A = K$, then $\mathrm{Hom}_{rings}(K,K) = \{id\}$ but $\mathrm{Hom}(\,\mathrm{Spec}\,\mathbb{Q}, \mathbb{P}^1_{\mathbb{Q}})$ has infinitely many elements.

3 Fibred product

3.1 Apr 13th-B: Categorical introduction of Fibred product

This is a notion that makes sense in any category. (Though a specific fibred product may not exist)

Definition 3.1. $\mathcal{C}$ a category, X, Y objects of $\mathcal{C}$, S an object of $\mathcal{C}$. Assume given

$$\begin{tikzcd} & Y \arrow[d, "f_2"'] \\ X \arrow[r, "f_1"] & S \end{tikzcd}$$

We say that an object Z of $\mathcal{C}$ with morphisms

$$\begin{tikzcd} Z \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & Y \arrow[d, "f_2"'] \\ X \arrow[r, "f_1"] & S \end{tikzcd}$$

makes the diagram commutes is a **fibred product** of X, Y over S if it has the universal property

$$\begin{tikzcd} T \arrow[dr, dashed, "\exists!"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\ & Z \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & Y \arrow[d, "f_2"'] \\ & X \arrow[r, "f_1"] & S \end{tikzcd}$$

Notation: $Z = X \times_S Y$

N.B. This notation is ambiguous because the fibred product depends on f_1, f_2. The fibred product is only suitably unique when it is specified with its two projections π_1, π_2.

Example 3.2. In Sets fibred products exist and

$$X \times_S Y = \{(x,y) \in X \times Y | f_1(x) = f_2(y)\}$$

with $\pi_1(x,y) = x$ and $\pi_2(x,y) = y$

Proof.

(1) $f_2 \circ \pi_2(x,y) = f_2(y) = f_1(x) = f_1 \circ \pi_1(x,y)$ for $(x,y) \in Z$.

(2) Let T be a set with $p_1 : T \longrightarrow X$ and $p_2 : T \longrightarrow Y$ s.t.

$$\begin{tikzcd}
T \arrow[dr, "f"] \arrow[drr, bend left, "p_2"] \arrow[ddr, bend right, "p_1"'] & & \\
& Z \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & Y \arrow[d, "f_2"] \\
& X \arrow[r, "f_1"] & S
\end{tikzcd}$$

define $f(t) = (p_1(t), p_2(t))$, $f_1(p_1(t)) = f_2(p_2(t))$, therefore $f(t) \in Z$. So f is a map makes the above diagram commute. Uniqueness of f is obvious. If there is another $\tilde{f}(t) = (\tilde{f}_1(t), \tilde{f}_2(t))$ making the above diagram commute, then $\tilde{f}_1(t) = \pi_1 \circ \tilde{f}(t) = p_1(t)$ and $\tilde{f}_2(t) = \pi \circ \tilde{f}(t) = p_2(t)$.

<u>Note</u>: This construction/definition is a an example of "universal" object in the categorical sense. It is universal in the following sense.

Given $X \xleftarrow{\pi_1} Z_1 \xrightarrow{\pi_2} Y$, $X \xleftarrow{\tilde{\pi}_1} Z_2 \xrightarrow{\tilde{\pi}_2} Y$ both fibred products over S there is a unique isomorphism $j : Z_1 \longrightarrow Z_2$, s.t. $\tilde{\pi}_1 = \pi_1 \circ j^{-1}$ and $\tilde{\pi}_2 = \pi_2 \circ j^{-1}$. $\square$

Example 3.3. If $\mathcal{C} =$ Sets, $S = \{*\}$ any 1 element set, the fibred product over S is just the Cartesian product

$$X \times_S Y = \{(x,y) \in X \times Y | f_1(x) = f_2(y)\}$$

But the restriction on f_i is just vacuous, the fibred product contains the usual Cartesian product.

(2) Let $X \overset{f_1}{\hookrightarrow} S \overset{f_2}{\hookleftarrow} Y$ (inclusion of subsets) We can see that the fibred product is isomorphic to the intersection of X, Y

$$\begin{tikzcd}
X \cap Y \arrow[r, hook] \arrow[d, hook] & Y \arrow[d, hook] \\
X \arrow[r, hook] & S
\end{tikzcd}$$

(3)

$$\begin{tikzcd} f_2^{-1}(X) \arrow[r, hook] \arrow[d, "f_2|_{f_2^{-1}(X)}"'] & Y \arrow[d, "f_2"] \\ X \arrow[r, hook, "f_1"] & S \end{tikzcd}$$

Theorem 3.4. In the category Sch of schemes, arbitrary fibred product exists.

Note This is false in the category of affine algebraic sets over K, with K algebraically closed.

Proof of theorem. Step 1 We prove this for affine schemes.

Assume $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, $S = \operatorname{Spec} R$. Given a diagram

$$\begin{tikzcd} X \arrow[r] & S \\ & Y \arrow[u] \end{tikzcd}$$

in AffnSch, we have a reversed diagram in Rings

$$\begin{tikzcd} A & \\ R \arrow[u] \arrow[r] & B \end{tikzcd}$$

Define $Z = \operatorname{Spec}(A \otimes_R B)$, and set $A \otimes_R B =: C$. We have

$$\begin{tikzcd} A \arrow[r] & C & & 1 \otimes b \\ & a \mapsto a \otimes 1 & & b \arrow[u, mapsto] \\ R \arrow[uu] \arrow[r] & B \arrow[uu] & & \end{tikzcd}$$

This diagram is commutative, which guarantees a diagram in AffSch

$$\begin{tikzcd} Z \arrow[r] \arrow[d] & Y \arrow[d] \\ X \arrow[r] & S \end{tikzcd}$$

$$\begin{tikzcd} T \arrow[drr] \arrow[ddr] & & \\ & Z \arrow[r] \arrow[d] & Y \arrow[d] \\ & X \arrow[r] & S \end{tikzcd}$$

N.B. Spec $(A \otimes_R B)$ is not easy to describe as a set.

Step 2 Uniqueness of $X \times_S Y$, when it exists, is formal.

Step 3. If $X \times_S Y$ exists, for any open subset $U \subset X$, $U \times_S Y$ exists and is $\pi_1^{-1}(U)$

$$\begin{tikzcd} \pi_1^{-1}(U) \arrow[r] \arrow[d] & X \times_S Y \arrow[r] \arrow[d, "\pi_1"] & Y \arrow[d] \\ U \arrow[r, hook] & X \arrow[r] & S \end{tikzcd}$$

Step 4 U_i affine. If for each i, $U - i \times_S Y$ exists, then so does $X \times_S Y$

$$\begin{tikzcd} & Y \arrow[d, "f_2"] \\ \cup_i U_i = X \arrow[r, "f_1"] & S \end{tikzcd}$$

If for each i, $U_i \times_S Y$ exists, then so does $X \times_S Y$.

Define $V_{i,j} = \pi_{1,i}^{-1}(U_i \cap U_j) \subset U_i \times_S Y$ open. Check that $V_{i,j} = (U_i \cap U_j) \times_S Y$ »»»»>2

One can glue the $U_i \times_S Y$ along the isomorphisms.

Check This scheme is $X \times_S Y$

Step 5.

step 1+ step 4.

Y, S affine $\Longrightarrow X \times_S Y$ exists. $\square$

3.2 Apr 17th: Examples and Applications of the Fibred Product

Recall. If we have maps $X \longrightarrow S$, $Y \longrightarrow S$, a space Z with maps $Z \longrightarrow X, Z \longrightarrow Y$ if the fibred product of $X \longrightarrow S \longleftarrow Y$ if it has the universal property

$$\begin{tikzcd} T \arrow[dr, dashed, "\exists!"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\ & Z \arrow[r] \arrow[d] & Y \arrow[d] \\ & X \arrow[r] & S \end{tikzcd}$$

$X = \operatorname{Spec} A, Y = \operatorname{Spec} B, S = \operatorname{Spec} R$. The contravariant functor Spec would invert the fiber coproduct of rings to fibred product of schemes.

$$X \times_S Y = \operatorname{Spec}(A \otimes_R B)$$

Define: $X \times_R Y := X \times_{\operatorname{Spec} R} Y$.

Example 3.5. Why not product? For X, Y and schemes, each have a unique map to $\operatorname{Spec} \mathbb{Z}$. The fibred product $X \times_{\mathbb{Z}} Y$ depends only on X and Y. ($\operatorname{Spec} \mathbb{Z}$ is the final object in Schemes)

$X = \operatorname{Spec} \mathbb{Z}[T]$, Krull dimension 2, $Y = \operatorname{Spec} \mathbb{Z}[V]$, dimension 2. $X \times_{\mathbb{Z}} Y \neq \operatorname{Spec} \mathbb{Z}[T, V]$ Krull dimension 3.

$$\dim X \times_{\mathbb{Z}} Y \neq \dim X + \dim Y.$$

Example 3.6. K a field, X, Y schemes over K $\dim X \times_K Y = \dim X + \dim Y$. But hte set of points of $X \times_K Y$ is not simply a topological product. For example, $X = \mathbb{A}^1_K, Y = \mathbb{A}^1_K$, $X \times_K Y = \mathbb{A}^2_K$, but it true that $X(K) = \operatorname{Hom}(\operatorname{Spec} K, X)$

$$X \times_K Y(K) = X(K) \times Y(K)$$

$$\operatorname{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} K, X \times_K Y) = \operatorname{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} K, X) \times \operatorname{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} K, Y)$$

by the universal product of fibred products.

If X is a scheme over S, T is a scheme over S. We can define $X(T)$ as $\operatorname{Hom}_S(T, X)$ and call it the T-valued points of X.

$$T = \operatorname{Spec} R, X(R)$$

$$X \times_S Y(T) = X(T) \times Y(T).$$

If we have the following morphism of schemes

$$\begin{tikzcd} X \arrow[dr] & & Y \arrow[dl] \\ & S' \arrow[d] & \\ & S & \end{tikzcd},$$

we have

$$X \times_{S'} Y(T) = X(T) \times_{S'(T)} Y(T).$$

$\operatorname{Hom}_S(T, X \times_{S'} Y)$ ={ pair (f_1, f_2) of elements $f_1 \in \operatorname{Hom}_S(T, X)$ and $f_2 \in \operatorname{Hom}_S(T, Y)$ such that $p_1 \circ f_1 = p_2 \circ f_2$}={ pair of elements $f_1 \in X(T)$ and $f_2 \in Y(T)$, $p_1 \circ f_1 = p_2 \circ f_2 \in S'(T)$}

$$\begin{tikzcd} T \arrow[dr] \arrow[drr, "f_2"] \arrow[ddr, "f_1"'] \arrow[dddrrr, dashed, bend right] & & & \\ & X \times_{S'} Y \arrow[r] \arrow[d] & Y \arrow[d, "p_2"] & \\ & X \arrow[r, "p_1"] & S' \arrow[dr] & \\ & & & S \end{tikzcd}$$

Example 3.7. Consider $GL_n(K)$. There exists a scheme $\mathcal{GL}_n$ with $\mathcal{GL}_n(K) = GL_n(K)$. $\mathbb{A}^{n^2} \supset V(det)$, $\mathcal{GL}_n$ gives the "open complement of $V(det)$". What are the R-valued points of $\mathcal{GL}_n$?

$$\mathcal{GL}_n(R) \neq \{n \times n \text{ matrices over } R \text{ with } det \neq 0\}$$

But

$$\begin{aligned} \mathcal{GL}_n(R) &= \{n \times n \text{ matrices over } R \text{ s.t. } \operatorname{Spec} R \longrightarrow \mathbb{A}^{n^2} \text{ does not intersect } V(det)\} \\ &= \{n \times n \text{ matrices } M \text{ over } R \text{ s.t.} det(M) \notin \text{ any prime ideal of } R\} \\ &= \{n \times n \text{ matrices } M \text{ over } R \text{ where } det(M) \text{ is invertible}\} \end{aligned}$$

Example 3.8. Equation

$$x^3 + y^3 + z^2 = 0,$$

find all solutions in $\mathbb{Z}$. $X = \operatorname{Spec} \mathbb{Z}[x, y, z]/(x^3 + y^3 + z^2)$. The set of solutions is $X(\mathbb{Z})$

Example 3.9. $f : X \longrightarrow S$, $\mathfrak{p}$ a point of S $K(\mathfrak{p})$ residue field of $\mathfrak{p}$. $\operatorname{Spec} K(\mathfrak{p}) \longrightarrow S$. Define$K(\mathfrak{p}) \times_S X$ as the fiber of f over $\mathfrak{p}$

$$\begin{tikzcd} & X \arrow[d] \\ \operatorname{Spec} K(\mathfrak{p}) \arrow[r] & S \end{tikzcd}$$

Lemma 3.10. The set of points of the fiber is the inverse image of $\mathfrak{p}$ where f is the set of points of X. The underlying set of $K(\mathfrak{p}) \times_S X$ maps to the underlying set of X.

The relative point of view "A parametrized family of varieties" $y^2 = x^3 - 3x - t$ viewed as a family of algebraic sets in $\mathbb{A}^2$ with coordinates X, Y parameter t. For each , we get an equation in X, Y, this defines a curve in $\mathbb{A}^2$. Consider the morphism

$$f : \operatorname{Spec} k[x, y, t]/(y^2 - x^3 - 3x + t) \longrightarrow \operatorname{Spec} K[t].$$

The fibers of f over closed points are curves in the family.

Idea from Grothendieck: view any morphism as a family where elements are the fiber. $\mathbb{A}^3 \cup pt \Longrightarrow \mathbb{A}^1$, $\mathbb{A}^3$ to 0 pt to 1. Not all maps make nice families but this point of view is helpfull in general, why?

- Fibers of a family are often simper (e.g.)
- Full family are simpler than individual fibers.

Example 3.11. Reduction $\mod p$. X is a scheme over $\mathbb{Z}$. $X \times_{\mathbb{Z}} \operatorname{Spec} \mathbb{F}_p$ is a scheme over $\mathbb{F}_p$. "reduction $\mod p$" of X $X = \operatorname{Spec} \mathbb{Z}[x_1, ..., x_n]/(f_1, ..., f_m)$ $X \times_{\mathbb{Z}} \operatorname{Spec} \mathbb{F}_p = \operatorname{Spec} \mathbb{F}_p[x_1, ..., x_n]/(f_1, .., f_m)$. This can be tricky, for example $\operatorname{Spec} \mathbb{Z}[T]/T(T+2)$ has no nilpotents (is "reduced" scheme) but $\operatorname{Spec} \mathbb{F}_2[T]/Y(T+2) = \operatorname{Spec} \mathbb{F}_2[T]/T^2$ has nilpotent.

Example 3.12. X a scheme over $\mathbb{Z}$ $X \times_{\mathbb{Z}} \operatorname{Spec} \mathbb{Q}$ (or $X \times_{\mathbb{Z}} \operatorname{Spec} \overline{\mathbb{Q}}$). Given Y over $\operatorname{Spec} \mathbb{Q}$, can we find X over $\operatorname{Spec} \mathbb{Z}$ with $X \otimes_{\mathbb{Z}} \operatorname{Spec} \mathbb{Q} = Y$? If so $X \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{F}_p$ will give some perspective on Y.

Lemma 3.13. If Y in $\mathbb{F}^n_{\mathbb{Q}}$ is the vanishing scheme of $f_1, .., f_m$ then this is possible.

Proof. $Y = \operatorname{Spec} \mathbb{Q}[T_1, .., T_n]/(f_1, .., f_m)$, where f_i are polynomials with rational coefficients. We can find $c_1, .., c_m$ positive integes where $c_i f_i$ has integer coefficients for all i. $X = \operatorname{Spec} \mathbb{Z}[T_1, ..., T_n]/(c_1 f_1, ..., c_m f_m)$. Because c_i^{-1} exists in $\mathbb{Q}$, it produces the same scheme over $\mathbb{Q}$. $\square$

However, this is not unique. For example, $Y = \operatorname{Spec} \mathbb{Q}[T]/(T^2/2+1)$. We can take $c = 2$ to get $\mathbb{Z}[T]/T^2 + 2$ and $c = 4$ to get $\mathbb{Z}[T]/2T^2 + 4$. These are not isomorphic fibers over 2, in fact, they are distinct $\mathbb{F}_2[T]/T^2$ v.s. $\mathbb{F}_2[T]$. Worse $T = 2U$, $Y = \operatorname{Spec} \mathbb{Q}[U]/(2U^2+1), X = \operatorname{Spec} \mathbb{Z}[U]/(2U^2+1)$. Reducetion over 2 gives $\operatorname{Spec} \mathbb{F}_2[U]/1 = \emptyset$

Example 3.14. (Base change) $f : X \longrightarrow S$ a morphism, family of schemes.

$$\begin{tikzcd} X \times_S T \arrow[r] \arrow[d, "f'"'] & X \arrow[d, "f"] \\ T \arrow[r] & S \end{tikzcd}$$

we can think of $f' : X \times_S T \longrightarrow T$as some family with different parameter space/ base/ This process is known as base change. $a \in T$ a point which mapsto $p \in S$

3.3 Apr 20th: absent

4 Elementary geometry of schemes

4.1 Apr 23rd: Some basics of schemes

Definition 4.1. X is a scheme. It is called **connected** if it is connected as a topological space. It is **irreducible** if it is irreducible as a topological space (it can not be expressed as union of two closed non empty set.)

Warning: spearated does not mean X is separated (Hausdorff) as topological space.

Definition 4.2. The dimension of X, denoted $\dim(X)$ is the max number n s.t. there is a chain of closed subsets

$$Y_0 \subsetneq Y_1 \subsetneq ... \subsetneq Y_n \subset X.$$

with each $Y_i$irreducible (with induced topology from X).

$$\dim \operatorname{Spec}(A) = \text{Krull dimsnion of } A$$

[check that $V(I) \subset \operatorname{Spec} R$ is irreducible $\iff I$ is prime]

Definition 4.3. A scheme X is reduced if $\forall U \subset X$ open, $\mathcal{O}_X(U)$ is reduced (no nilpotents)

And this is equivalent to

$$\forall x \in X, \quad \mathcal{O}_{X,x} \text{ is reduced.}$$

Definition 4.4. A scheme X is called **integral** if for all $U \subset X$ open, $\mathcal{O}(U)$ is an integral domain.

Note that being integral scheme $\not\Longleftarrow \forall x \in X, \mathcal{O}_{X,x}$ is integral domain.

Lemma 4.5. X integral $\Longleftrightarrow X$ is reduced and irreducible.

Proof.
- In a scheme X is integral, $\mathcal{O}_X(U)$ is integral for all open subsets, hence $\mathcal{O}_X(U)$ is also reduced because integral domain has no nonzero zero divisors.
- An integral scheme should be irreducible. Assume contrarily X is reducible, and can be written as union of two closed subsets $X = Y \cup Z$. Define the complements $U := X - Y$ and $V = X - Z$, we know U, V are nonempty opens and their have empty intersection. The structure sheaf $\mathcal{O}_X(U \cup V) = \mathcal{O}_X(U) \times \mathcal{O}_X(V)$ which is not integral in general.
- Conversely: X reduced + irreducible. Let $U \subset X$ be a open, and assume $\mathcal{O}_X(U)$ is not integral. (exists $s, tin\mathcal{O}_X(U)$ such that $st = 0$.)

  Let $Z_s = \{x \in U | s(x) \in \mathfrak{m}_{X,x} \subset \mathcal{O}_{X,x}\}$, $Z_t = \{X \in U | t(x$
  $in\mathfrak{m}_{X,x} \subset \mathcal{O}_{X,x}$

  Claim: Z_t, Z_s are closed in X. (If $U = \operatorname{Spec} A$ is affine, then s corresponds to an element $a \in A$ and

  $$\begin{aligned} Z_s &= \{\mathfrak{p} \in \operatorname{Spec} A | a \in \mathfrak{p}A_\mathfrak{p}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} A | a \in \mathfrak{p}\} \\ &= V(aA) \text{ is closed} \end{aligned}$$

  In the general case, it follows that $Z_s \cap \operatorname{Spec} A$ is closed for any $\operatorname{Spec} A \subset U$ open affine $\Longrightarrow Z_s$ is closed.)

  Since $st = 0$, we have $s(x)t(x) \in \mathfrak{m}_{X,x}$ for every x, so $x \in Z_s \cup Z_t$ for every x. $Z_t \cup Z_s = U$.

  Since X is irreducible $\Longrightarrow Z_s = U$ or $Z_t = U$. For instance, if $Z_s = U$, then $s|V = 0$ nilpotent for every affine $\operatorname{Spec} B = V \subset U$ (because $s|V$

corresponds to $a \in A$ which has $U_a = V - V(a)$ is empty set $\Longrightarrow \sqrt{(a)} = \{0\} \Longrightarrow a$ is nilpotent). Since X (hence U) is reduced, we get $s|V = 0$ for every $V \subset U$ open affine, so by the (sheaf condition) we have $s = 0$.

$\square$

Definition 4.6. A scheme X is **locally Noetherian** if there exists an affine open cover of X $\cup_{i \in I} U_i = X$, $\operatorname{Spec} A_i = U_i$, with A_i Noetherian. X is **Noetherian** if there is a finite such cover.

Fact: Hartshone. prop II 3.2

$$\text{locally Noetherian} \Longleftrightarrow \forall \operatorname{Spec}(A) \subset X \text{ open, } A \text{ Noetherian}$$

This implies that an affine scheme $\operatorname{Spec} A$ is locally Noetherian iff A is Noetherian.

Definition 4.7. $X \xrightarrow{f} Y$ (scheme over Y) is a morphism **locally of finite type** $\Longleftrightarrow \exists Y = \cup_i U_i, U_i = \operatorname{Spec} A_i$, such that $\forall i, \exists f^{-1}(U_i) = \cup_i \operatorname{Spec}(B_{ij})$ s.t.

$$\operatorname{Spec}(B_{ij}) \longrightarrow \operatorname{Spec}(A_i)$$

corresponds to

$$A_i \longrightarrow B_{ij}$$

which makes B_{ij} an A_i-algebra of finite type.

$X \longrightarrow Y$ is of finite type if for every i as above, there is a covering with only finitely many j.

Example 4.8.

(1) K a field, $\operatorname{Spec} K[X_1, .., X_n]/I$ is Noetherian, of finite type over K

$$\Longrightarrow \operatorname{Spec}(K[X]/I) \longrightarrow \operatorname{Spec}(K) isoffinitetype.$$

(2) $\sqcup_{n \geq 0} \mathbb{A}_K^n \longrightarrow \operatorname{Spec} K$ is locally of finite type, not of finite type(over K)

(3) $\operatorname{Spec}(\mathbb{Z}[X_1, .., X_n]/I) \longrightarrow \operatorname{Spec} \mathbb{Z}$ is of finite type and Noetherian.

(4) $\operatorname{Spec}(\mathbb{Q}) \longrightarrow \operatorname{Spec} \mathbb{Z}$ if **not** of finite type.

Open and closed subschemes

Definition 4.9. X a scheme $U \subset X$ open $(U, \mathcal{O}_X|U)$ is called an **open subscheme** of X, $j : U \hookrightarrow X$ is called an **open immersion**.

Definition 4.10. (Hartshorne p85) A morphism $Y \xrightarrow{f} X$ is a called a **closed morphism** if

(1) f induces a homeomorphism $Y \longrightarrow f(Y) \subset X$ where $f(Y)$ is closed.

(2) $f^* : \mathcal{O}_X \to f_*\mathcal{O}_Y$ is surjective (surjective at the level of stalks)

Intuitively,

$$\mathcal{O}_X(U) \longrightarrow \mathcal{O}_Y(f^{-1}(U))$$

are not surjective in general, but if $s \in (f_*\mathcal{O}_Y)(U)$, we can find locally for each $x \in U$ a section on some open set $V \subset U$ containing x which maps to the restriction of s to V.

Definition 4.11. A **closed subscheme** of X is an equivalence class of closed immersions modulo

$$\begin{tikzcd} Y \arrow[rr, "f"] \arrow[dr, "g"'] & & X \\ & Y' \arrow[ur, "f'"'] & \end{tikzcd} \qquad \begin{array}{c} f \sim f' \\ \iff \exists g : Y \xrightarrow{\sim} Y' \end{array}$$

Example 4.12. Let $X = \operatorname{Spec}(A)$ let $I \subset A$ be an ideal and $\operatorname{Spec}(A/I) \xrightarrow{f} \operatorname{Spec} A$ the canonical morphism. Then it is a closed immersion:

We saw that $\operatorname{Spec} A/I \xrightarrow{\sim} V(I) \subset \operatorname{Spec}(A)$ is a homeomorphism. $\forall \mathfrak{p} \in V(I)$ the morphism $\mathcal{O}_{A,\mathfrak{p}} \longrightarrow \mathcal{O}_{A/I,\mathfrak{p}/I}$ is $A_\mathfrak{p} \longrightarrow (A/I)_{\mathfrak{p}/I}$ which is surjective by elementary localization.

Proposition 4.13. (1) A is a ring. If

$$Y \xrightarrow{f} \operatorname{Spec} A$$

is a closed immersion, there exists an ideal $I \subset A$ such that f is equivalent to $\operatorname{Spec}(A/I) \longrightarrow \operatorname{Spec}(A)$: There is a commutative diagram where the lower map is the canonical closed immersion.

$$\begin{tikzcd} Y \arrow[r, "f"] \arrow[d, "\sim"] & \mathrm{Spec}\,(A) \\ \mathrm{Spec}\,(A/I) \arrow[ur] & \end{tikzcd}$$

(elementary proof in Wedhorn, best proof is to use coherent sheaves)

(2) Consider

$$\begin{tikzcd} Z \times_X Y \arrow[r, "\tilde{j}"] \arrow[d] & Y \arrow[d] \\ Z \arrow[r, "j"] & X, \end{tikzcd}$$

where j is closed immersion. Then $\tilde{j}$ is a closed immersion. (e.g. $Z = \mathrm{Spec}\,\kappa(x)$ where $x \in X$ is a closed point, then $Z \longrightarrow X$ is a closed immersion and hence also f $\mathrm{Spec}\,\kappa(x) \times_X Y \longrightarrow Y$ is a closed immersion)

(3) Note that a closed subscheme of X is not determined by its image in X.

e.g. $\mathrm{Spec}\,(A/I)$"=" $\mathrm{Spec}\,(A/J)$ iff $\sqrt{I} = \sqrt{J}$ which may give infinitely many J for a given I. $n \geq 1$, $\mathrm{Spec}\,K[X]/(X^n) \hookrightarrow \mathrm{Spec}\,(K[X])$ all have the same image $XK[X]$. Intuitively, it is they are both the point 0 but "memorize" different information of derivatives.

Proposition 4.14. »»»>1

If $V(I) = Y \subset X = \mathrm{Spec}\,A$, take $\mathrm{Spec}\,A/\sqrt{I}$ which is a reduced closed subscheme with image $V(I)$. [This is called the reduced induced scheme structure on Y.]

4.2 Apr 27th: Projective space and schemes

Definition 4.15. S is a scheme, $n \geq 1$ $\mathbb{P}^n_S = \mathbb{P}^n_{\mathbb{Z}} \times_{\mathrm{Spec}\,\mathbb{Z}} S$

Two standard constructions of $\mathbb{P}^n_{\mathbb{Z}}$

(1) Proj of a graded ring (hartshorne p 76)

$$A = \oplus_{d \geq 0} A_d,\ A_d A_e \subset A_{d+e}$$

A_0 is a ring and each A_d is an A_0-module.

<u>Ex</u> $A = B[X_1, .., X_n], A_0 = B$

To each such A, one can associate a scheme Proj(A) which generalizes classical projective algebraic sets. For $\mathbb{P}^n_{\mathbb{Z}}$ we take $A = \mathbb{Z}[X_0, ..., X_n]$. Let $A^+ := (X_0, .., X_n)$. The definition of Proj$(A) = \mathbb{P}^n_{\mathbb{Z}}$ is

$$\mathbb{P}^n_{\mathbb{Z}} = \{P \subset A \mid \text{prime and homogeneous ideal in } A \text{ such that} P \not\supset A^+\}.$$

Topologically, the closed sets $V^p(I) = \{P \in \mathbb{P}^n_{\mathbb{Z}} | I \subset P\}$ homogeneous and for $U \subset \mathbb{P}^n_{\mathbb{Z}}$ open

$$\mathcal{O}_{\mathbb{P}^n_{\mathbb{Z}}}(U) = \left\{ s : U \longrightarrow \sqcup_{P \in U} A_{(P)} \middle| \begin{array}{l} \forall P, s(P) \in A_{(P)}, \\ \text{and locally } s(P) = a/b, \\ \text{where } a, b \text{ homogeneous of same degree} \end{array} \right\},$$

where $A_{(P)} = \{$degree 0 elements in localization of A w.r.t. $S - P$, homogeneous$\}$

<u>FACTS</u>:

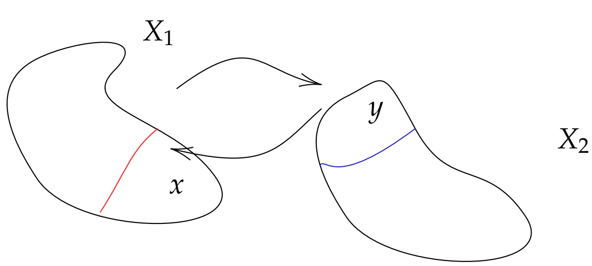
(a) $\mathbb{P}^n_{\mathbb{Z}}$ is a locally-ringed space

(b) $\mathbb{P}^n_{\mathbb{Z}}$ is a scheme, more precisely, for each $i \in \{0, ..., n\}$, let $U_i = \{P \in \mathbb{P}^n_{\mathbb{Z}} | X_i \notin P\}$, then U_i is open and $\cup_i U_i = \mathbb{P}^n_{\mathbb{Z}}$(because $P \in \mathbb{P}^n_{\mathbb{Z}}$ does not contain A^+).

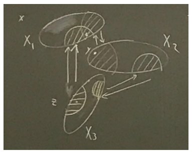
By "dehomogeneousation" one has an isomorphism

$$U_i \tilde{\longrightarrow} \text{ Spec}\,(\mathbb{Z}[Y_1, ..., Y_n]) \simeq \mathbb{A}^n_{\mathbb{Z}}$$

(2) "Glueing"



Glueing constructs "$X_1 \cup X_2$ where each point x is "identified" with the corresponding point y in X_2. More generally: we need to take care of intersections »»»»»1



Proposition 4.16. Given the glueing datum on $(X_i)_{i\in I}$, there is a scheme X obtained by "glueing the X_i's along the U_{ij} using φ_{ij}'s " given by

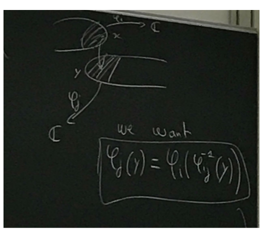
$$X = (\sqcup_{i\in I} X_i) \;/\; \sim,$$

where the equivalence relation is each $x \in X_i$ is identified with $\varphi_{ij}(x) \in X_j$ for $j \neq i$ if $x \in U_{ij}$, with the quotient topology. The quotient map $\sqcup X_i \xrightarrow{f} X$ is open, in particular $f(X_i) \subset X$ is open).

Note: $\sim$ is an equivalence relation because of the cocycle relation: if $y = \varphi_{ij}(x)$, then $x = \varphi_{ij}^{-1}(y) = \varphi_{ji}(y)$. If $y = \varphi_{ij}(x), x \in U_{ij}, z = \varphi_{jk}(y), y \in U_{jk}$ and $x \in U_{ik}$, then $\varphi_{ik}(x) = \varphi_{jk} \circ \varphi_{ij}(y)$ so $x \sim y \sim z \Longrightarrow X \sim z$ and with structure sheaf

$$\mathcal{O}_X(U) = \{(s_i)_{i\in I} | s_i \in \mathcal{O}_{X_i}(U \cap X_i) \text{ s.t. } \varphi_{ij}^{\alpha}(s_j|U \cap U_{ji} = s_i|U \cap U_{ij}\},$$

we want $\varphi_j(y) = \varphi_i(\varphi_{ij}^{-1}(y))$



Note that the projection

$$f : \sqcup X_i \longrightarrow X$$

induces a homomorphism $X_i \xrightarrow{\sim} f(X_i) \subset X$ with open image [$f|X_i$ is injective.]

We identify X_i with $f(X_i) \subset X$ to write $U \cap X_i$ for instance (really it is $f^{-1}(U) \cap X_i$). Then $(X, \mathcal{O}_X)$ is a ringed space and there is an isomorphism $X_i \longrightarrow f(X_i)$ of ringed spaces, it follows that(since $f(X_i)$ is open) that X is a scheme.

Here we fix j,

$$\mathcal{O}_{f(X_j)} \longrightarrow f_* \mathcal{O}_{X_j}$$

is given by

$(s_i) \mapsto$ the unique s section of $\mathcal{O}_{X_j}$ that coincides with s_i on$X_i \cap X_j = U_{ij} \subset X_i$

Application to $\mathbb{P}^n_{\mathbb{Z}}$. Let $A = \mathbb{Z}[X_0, ..., X_n, X_0^{-1}, ..., X_n^{-1}]$. In A, we have subrings $A_i = \mathbb{Z}[\frac{X_0}{X_i}, ..., \frac{X_n}{X_i}]$. Note $A_i \simeq \mathbb{Z}[Y_1, .., Y_n]$ by

$$\frac{X_0}{X_i} \mapsto Y_1$$
$$\frac{X_{i-1}}{X_i} \mapsto Y_i$$
$$\frac{X_{i+1}}{X_i} \mapsto Y_{i+1}$$
$$\frac{X_n}{X_i} \mapsto Y_n$$

Let $X_i = \operatorname{Spec}(A_i)$ ($\simeq \mathbb{A}^n_{\mathbb{Z}}$), $(0 \leq i \leq n)$. Let $U_{ij} \subset X_i$ be $\operatorname{Spec}(A_i, \frac{X_j}{X_j}) = \operatorname{Spec}(\mathbb{Z}[\frac{X_0}{X_i}, ..., \frac{X_n}{X_i}, \frac{X_i}{X_j})$ is an open subset in X_i.

Note that $B_{ij} = B_{ji}$, the identity $B_{ij} \longrightarrow B_{ji}$ corresponds to an isomorphism

$$\varphi_{ij} : U_{ij} \longrightarrow U_{ji}.$$

Since the ring part is identity, the cocycle condition holds.

Definition 4.17. $\mathbb{P}^n_{\mathbb{Z}}$ is the glued scheme in that case i.e. covered by $n+1$ open subschemes $\simeq \mathbb{A}^n_{\mathbb{Z}}$, it is of finite type, Noetherian, integral ...

Definition 4.18. S is a scheme, A projective $S-$scheme

$$X \xrightarrow{f} S$$

is a morphism such that there is a factorization

$$X \overset{\text{closed immersion}}{\hookrightarrow} \mathbb{P}^n_S \longrightarrow S$$

for some integer $n \geq 1$.

How to concretely construct projective scheme over K? Let K be a field,. Let $f \in K[X_0, ..., X_n]$ homogeneous. Goal: Define the zero set Y of f as a closed subscheme of $\mathbb{P}^n_K$. We are going to do it by glueing up the corresponding intersection

$$Y \cap U_i$$

We define the dehomogeneousation

$$f_i := f\left(\frac{X_0}{X_i}, .., 1, .., \frac{X_n}{X_i}\right) \in K[\frac{X_0}{X_i}, ..., \frac{X_n}{X_i}] = A_i$$

for $0 \leq i \leq n$. So we get closed immersions

$$Y_i = \operatorname{Spec}(A_i / f_i A_i) \hookrightarrow U_i$$

Idea: Y is obtained by glueing the Y_i by identify $Y_i \cap U_{ji}$ with $Y_j \cap U_{ji}$ along φ_{ij}.

Precisely: Let $B_{ij} = K[\frac{X_0}{X_i}, ..., \frac{X_n}{X_i}, \frac{X_i}{X_j}]$,

$$Y_i \cap U_{ij} = \operatorname{Spec}(B_{ij} / f_i B_{ij})$$

and

$$Y_i \cap U_{ij} = \operatorname{Spec}(B_{ji} / f_j B_{ji})$$

$$\begin{array}{ccc} B_{ij} & \longrightarrow & B_{ij}/f_iB_{ij} \\ \| & & \downarrow \sim \\ B_{ji} & \longrightarrow & B_{ji}/f_jB_{ji} \end{array}$$

commutative because f_i and f_j generate the same ideal ub $B_{ij} = B_{ji}$, since

$$\begin{aligned} f_j &= \sum_J \alpha_J \left(\frac{X_0}{X_j}\right)^{d_0} \cdots \left(\frac{X_i}{X_j}\right)^{d_i} \cdots \left(\frac{X_n}{X_j}\right)^{d_n} \\ &= \sum_J \alpha_J \left(\frac{X_0}{X_i}\right)^{d_0} \cdots \left(\frac{X_i}{X_i}\right)^{d_i} \cdots \left(\frac{X_n}{X_i}\right)^{d_n} \cdot \left(\frac{X_j}{X_i}\right)^{d_0 + \cdots d_n} \\ &= f_i \cdot \left(\frac{X_j}{X_i}\right)^{d_0 + \cdots d_n} \end{aligned}$$

4.3 May 4th-A: Projective schemes continued

Recall: $\mathbb{P}^n_{\mathbb{Z}}$ =“glueing” $U_i := \operatorname{Spec}(\mathbb{Z}[X_0/X_i, ..., X_n/X_i])$ along open subsets $U_{ij} = \operatorname{Spec}(\mathbb{Z}[...]_{X_j/X_i})$

$f \in K[X_0, ..., X_n]$ is non-constant homogeneous polynomial, $\rightsquigarrow$“vanishing scheme Z_f” by glueing the closed subschemes of $U_{i,K} = U_i \times_{\operatorname{Spec}(\mathbb{Z})} \operatorname{Spec}(K)$ defined by $f_i = f(X_0/X_i, ..., X_n/X_i)$. WE can do this with $f^{(1)}, f^{(2)}, ..., f^{(m)}$ homogeneous of some degrees $\rightsquigarrow$ vanishing sets of finitely many homogeneous polynomials.

Fact: These "vanishing sets " are closed subscheme of $\mathbb{P}^n_K$ all closed subscheme of $\mathbb{P}^n_K$ arise in this way.

Reason: let Y be this vanishing scheme; it is defined by glueing closed subschemes.

$$Y_i \overset{\varphi_i}{\hookrightarrow} U_{i,K} = \mathbb{A}^n_K$$

where

$$Y_i = \operatorname{Spec}\left(K[X_0/X_i, ..., X_n/X_i]\right)/(f_i^{(1)}, ..., f_i^{(m)}).$$

One checks that there is a unique morphism

$$\varphi : Y \longrightarrow \mathbb{P}^n_K$$

such that $\varphi|Y_i = \varphi_i$. and that φ is a closed immersion. (Because every point has one Y_i as an open neighbourhood and φ_i is a closed immersion.)

Example 4.19. In $\mathbb{P}^2_{\mathbb{Z}}$, we have a closed subscheme defined by

$$Y^2Z - X^3 - XZ^2$$

and on $U_2 = \operatorname{Spec}(\mathbb{Z}[X/Z, Y/Z, 1])$ it is isomorphic to the closed subscheme of $\mathbb{A}^2_n = \operatorname{Spec}(\mathbb{Z}[U, V])$

$$\left(\frac{Y}{Z}\right)^2 - \left(\frac{X}{Z}\right)^3 - \left(\frac{X}{Z}\right) = V^2 - U^3 - U.$$

5 Divisors

5.1 May 4th-B: Weil divisors

Divisors are the first non-trivial geometric invariants of the schemes and have many applications and forms.

- classification of "hypersurfaces" in a scheme X. (Weil divisors.)
- certain sheaves (invertible sheaves of $\mathcal{O}_X$-modules)
- Picard groups $\rightsquigarrow$ morphisms of projective spaces.

In order to define Weil divisors, the scheme is required to be Noetherian and integral. We usually look at those schemes with nice enough properties so that we don't have to worry about Cartier divisors

Definition 5.1. Let X be scheme. X is **regular in codimension one** if for any $x \in X$ where $\dim(\mathcal{O}_{X,x}) = 1$, the local ring $\mathcal{O}_{X,x}$ is regular ($\dim \mathfrak{m}/\mathfrak{m}^2 = 1$). i.e. each local ring $\mathcal{O}_{X,x}$ of dimension one is regular.

In this section, we require the scheme to be Noetherian integral, separated scheme which is regular in codimension one. (In general a Noetherian local ring $(A, \mathfrak{m})$, with $k = A/\mathfrak{m}$ is called regular if the dimension of A is equal to the $\dim_k \mathfrak{m}/\mathfrak{m}^2$ this means X has some minimal "smoothness")

Example 5.2.

(1) Assume, a scheme X if of finite type over a filed K, then X is regular in codimension one if X is "non-singular" in the sense analogue of definition of non-singular varieties.

(2) $X = \mathbb{A}^n_K = \operatorname{Spec}(K[X_1, .., X_n])$. To say that $\mathfrak{p} \in X$ has dimension one means $\dim \mathcal{O}_{X,\mathfrak{p}} = 1 \iff$ height of $\mathfrak{p}$ is equal to 1. Because
$$\mathcal{O}_{X,\mathfrak{p}} = K[X_1, ..., X_m]_{\mathfrak{p}}$$
in which prime ideals are exactly in bijection with prime ideals $\mathfrak{q} \subset \mathfrak{p}$. In $K[X_1, .., X_n]$ a prime ideal of height 1 is principal ideal generated by f irreducible. We also know that in that case $K[X_1, .., X_n]_{(f)}$ is regular.

(3) $\mathbb{P}^n_K$ is also regular in codimension 1, because it is a local condition, and we apply (2).

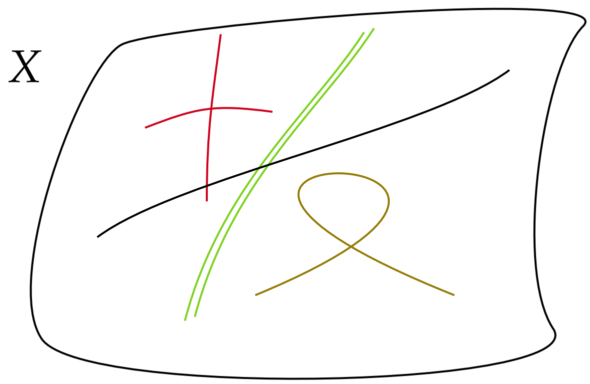
(4) Any smooth curve over a field (points of dimension 1 are closed points.)

(5) If X is a singular curve, it is not regular in codimension 1.

(6) $\operatorname{Spec}(\mathbb{Z})$ is also regular in codimension 1. (the points of dimension 1 are $p\mathbb{Z}$ and local ring at $p\mathbb{Z}$ is
$$\mathcal{O}_{\mathbb{Z},p} = \left\{ \frac{a}{b} \in \mathbb{Q} | a, b \text{ coprime } and p \nmid b \right\}$$
which is a regular local ring.

Convention: Below in this section, X is Noetherian, integral, regular in codimension 1. (quasiprojective over affine base)
$$X \underset{\hookrightarrow}{\text{open}} Y \underset{\hookrightarrow}{\text{closed}} \mathbb{P}^n_S \longrightarrow S$$
In particular, X is of finite type over S.

We look at closed subschemes of codimension 1 in X.



Regular codimension 1 $\Longrightarrow$ any such subscheme is a union of irreducible pieces, each of which is of the form $f^n = 0$, $(n \geq 1)$ with $\{f = 0\}$ being integral.

Definition 5.3.

(1) A **prime (Weil) divisor** D in X is an integral closed subscheme of codimension 1. (there is no intermediate closed subscheme between D and X)

(2) The **group of Weil divisors** on X is the free abelian group generated by prime divisors.

$$\sum_{i \in I, finite} n_i D_i, n_i \in \mathbb{Z} \text{ and } D_i \text{ prime divisors}$$

It is denoted $\mathrm{Div}(X)$. A divisor $D = \sum_i n_i D_i$ is effective if all $n_i \geq 0$. Intuitively, effective divisor $\sum_i n_i D_i$ corresponds to the closed subscheme union of the D_i's with multiplicity n_i.

Definition 5.4. The **function field** of X is the residue field/local ring at the generic point η of X. An element f of $K(X)$ is therefore the equivalence class of (U, s) where U is an open set $\emptyset \neq U \subset X$ and $s \in \Gamma(U, \mathcal{O}_X)$.

Example 5.5. $K(\mathbb{A}^n_K) = K(X_1, ..., X_n) = K(\mathbb{P}^n_K)$

Lemma 5.6. Let D be a prime divisor, and η_D its generic point. Let $\tilde{\eta}_D$ be the image of η_D in X. The ring $\mathcal{O}_{X,\tilde{\eta}_D}$ is a DVR with fraction field $K(X)$

Proof. Affine Case: $D = \operatorname{Spec}(A/\mathfrak{p})$ with $\mathfrak{p}$ prime ideal so that $A/\mathfrak{p}$ is integral. $\eta_D = \{0\} \subset A/\mathfrak{p}$ and $\tilde{\eta}_D = \mathfrak{p} \in \operatorname{Spec}(A)$.

D has codimension 1, $\iff \mathrm{ht}(\mathfrak{p}) = 1 \iff \dim \mathcal{O}_{X,\tilde{\eta}_D} = \dim A_{\mathfrak{p}} = 1$ so by regularity in codimension 1, $A_{\mathfrak{p}}$ is a regular local ring of dimension 1, Noetherian, i.e. it is a DVR $\iff$ [maximal ideal is principal.] Then $K(X) = Frac(A) = Frac(A_{\mathfrak{p}})$. $\square$

Now given D a prime divisor, $f \in K(X)^{\times}$, we denote by $\nu_D(f)$ the valuation at D of f, $f \in Frac(\mathcal{O}_X, \tilde{\eta}_D)$. $(\mathfrak{m}_{X,\tilde{\eta}_D} = (\varpi))$ then $f \in Frac(\mathcal{O}_{X,\tilde{\eta}_D})$ is of the form $\frac{a}{b}$, a, b in $\mathcal{O}_{X,\tilde{\eta}_D}$, $a = \varpi^n u, n \geq 0, u \in \mathcal{O}^{\times}_{X,\tilde{\eta}_D}$ and $b = \varpi^m v, m \geq 0, v \in \mathcal{O}^{\times}_{X,\tilde{\eta}_D}$ and $\nu_D(f) = n - m$.

Intuitively: $d = \nu_D(f) \geq 1$ means f has a zero of order d along D (has degree of vanishing d along D). $d \geq -1$ means a pole of order $-d$ (a zero of order d of $1/f$)

Lemma 5.7 (Hartshorne II 6.1)**.** If $f \in K(X)^{\times}$ then $\nu_D(f) = 0$ for all but at most finitely many prime divisors D.

Definition 5.8. For $f \in K(X)^{\times}$,

$$\mathrm{div}(f) = \sum_{D \text{ prime}} \nu_D(f) D \in \mathrm{Div}(X)$$

$$div : K(X)^{\times} \longrightarrow \mathrm{Div}(X) \text{ group morphism}$$

The group of all $\mathrm{div}(f)$ is called the group of principal divisors. The quotient

$$\mathrm{Div}(X)/Im(div) = \mathrm{Cl}(X)$$

is the **divisor class group** of X

Proof of lemma immediately above. Let $f \in K(X)^{\times}$, view it as $f \in \Gamma(U, \mathcal{O}_X)$, where $\emptyset \neq U = \operatorname{Spec}(A)$ is affine. Let $Z = X - U$, closed in X, with reduced subscheme structure.

$\{D \text{ prime } \mid D \subset Z\}$ is finite because X (hence Z) is Noetherian.

Example. $f = X^2 + 3X^2Y + Y^3/(XY)$, $Z =$ union of coordinate axes, each is prime. If D is not in Z then $U \cap D = D_U$ is non-empty, and hence dense in D. Claim. $U \cap D$ is a prime divisor in U. Then $\nu_{D \cap U}(f)[= \nu_D(f)] \geq 0$ since $f \in \Gamma(U, \mathcal{O}_X) = A$ and to say that $\nu_{D\cap U}(f) \geq 1$ means $D \cap U \subset V(fA)$ proper closed in U. So again this happens for finitely many D.

WHy is $U \cap D$ a prime divisors in U?

$$\begin{tikzcd} D \arrow[r, "\text{closed}"] & X \\ \emptyset \neq D \cap U \arrow[u, phantom, "\text{open}\ \cup"] & \subset \quad U \arrow[u, phantom, "\cup\ \text{open}"] \end{tikzcd}$$

$D \cap U$ is an open subscheme of D then check that $D \cap U \simeq D \times_X U$, so $D \cap U \hookrightarrow U$ is a closed immersion. Moreover $D \cap U$ is integral because D is integral. One checks that $D \cap U$ is also of codimension 1

$$K(U) = k(X)$$

$$\Longrightarrow \nu_{D \cap U} = \nu_D$$

$\square$

5.2 May 8th-A: Divisors continued

Reminder: Let X be a scheme, which is integral regular in codimension one, Noetherian, quasi-projective.

We defined $\mathrm{Div}(X) :=$ free Abelian group with basis of the integral codimension 1 subschemes.

$f \in K(X)^\times$

$\Longrightarrow \mathrm{div}(f) = \sum_D \nu_D(f) D$

div gives a group morphism $K(X)^\times \longrightarrow \mathrm{Div}(X)$

Definition 5.9. $Cl(X) = \mathrm{Div}(X)/Imdiv$ is called the divisor class group.

Example 5.10. (1) Let X be a smooth curve over a field $K \Longrightarrow$ prime divisors are closed points of X, an $f \in K(X)^\times$ can be seen as a non-constant morphism

$$f : X \longrightarrow \mathbb{P}^1_K$$

and $\mathrm{div}(f)$ =zero of f with multiplicities or poles of f with multiplicities.

$Cl(X) \longleftrightarrow$ "given points $x_1, ..., x_m$ and$y_1, ..., y_n$ with specified integers of $\nu_1, .., \nu_m \geq 1$ and $\mu_1, ..., \mu_n \geq 1$". Is there an

$$f : X \longrightarrow \mathbb{P}^1_K$$

s.t. f has zeros at x_i with multiplicities ν_i and poles at y_j with multiplicities μ_j

$\rightsquigarrow$ **Riemann-Roch Theorem**

(2) $X = \mathbb{A}^1_K = \operatorname{Spec}(K[T])$. Prime divisors is in one to one correspondence with irreducible monic polynomials in $K[T]$ and divisor can be identifies to f_1/f_2, where f_1, f_2 are coprime monic polynomials. BY $\sum n_i D_i \mapsto \prod_i f_i^{n_i}$ (This is historically one of the motivating cases)

(3) $X = \mathbb{A}^n_K$ (or $\mathbb{A}^n_{\mathbb{Z}}$) Claim: $Cl(X) = 0$. (In fact: prop II 6.2 in Hartshorne If A is, integral domain and integrally closed , then A is $UFD \iff Cl(\operatorname{Spec}(A)) = 0$)

Any prime divisor D in $\mathbb{A}^n_K$ is of the form $V((f))$ for $f \in A$ irreducible, thus $D = \operatorname{Spec}(A/(f))$.

Let $D = \sum n_i D_i$ be a divisor with $n_{\geq}1$, D_i distinct. We can define f_i so that

$$D_i = \operatorname{Spec}(A/(f_i))$$

and let $f = \prod f_i^{n_i} \in K(T_1, ..., T_n)^\times = K(\mathbb{A}^n_K)$. Then recall how to compute $\operatorname{div}(f)$: D prime divisor, $D = \operatorname{Spec}(A/(g))$

$$\begin{aligned} \mathcal{O}_{\mathbb{A}^n_K, \tilde{\eta}_D} &= A_{(g)} \\ &= \{f_1/f_2 \in K(T_1, .., T_n)^\times : g \nmid f_2\} \end{aligned}$$

is indeed a DVR with maximal ideal generated by g, and $\nu_D(f_1/f_2) =$ the exponent of $g = k$ s.t. $f_1/f_2 = f^k u$, with $u \in A^\times_{(g)}$. So $\operatorname{div}(f) = \sum n_i D_i = D$ so any D is principal, therefore $Cl(\mathbb{A}^n_K) = 0$

(4) $Cl(\operatorname{Spec} K) = \{0\}$ has no prime divisors. Consider $L/\mathbb{Q}$ finite extension. Let $A \subset L$ be the integral closure of $\mathbb{Z}$. Then $\operatorname{Spec}(A)$ is regular of codimension one, so $Cl(\operatorname{Spec} A)$ is defined. This is isomorphic to the "ideal class group" $H(L)$ of L.

We sketch the reason here.

$$H(L) = \{\text{fractional ideals}\}/\{\text{ principal ideals}\}$$

where $\{\text{fractional ideals}\} \simeq$ free Abelian group generated by prime ideals and a fractional ideal is principal iff it is associated to a principal ideal.

There are still many open questions: are there infinitely many $L/\mathbb{Q}$ with $Cl(\operatorname{Spec} A) = 0$? (i.e. A UFD)

How are $Cl(\operatorname{Spec} A)$ distributed when $L/\mathbb{Q}$ varies? (Cohen-Lenstra Heuristics)

(5) $X = \mathbb{P}^n_K$ with K is a field.

Fact: the prime divisors are the closed subschemes associated to a single homogeneous irreducible polynomials $f \in K[X_0, .., X_n]$.

Theorem 5.11. (II 6.4) Define a group morphism from the $\underline{deg}$: $\mathrm{Div}(X) \longrightarrow \mathbb{Z}$

$$D \longmapsto \underline{deg}(f)$$

where D is the subscheme associated to homogeneous polynomial f.

(a) For all principal divisors $\mathrm{div}(f), f \in K(X)$, we have $\underline{deg}(f) = 0$.

(b) The induced morphism from class groups to $\mathbb{Z}$

$$Cl(X) \xrightarrow{\underline{deg}} \mathbb{Z}$$

is an isomorphism.

(c) $Cl(X)$ is isomorphic to $\mathbb{Z}$ with generator any

$$H_i = \mathbb{P}^n_K - U_i$$

where U_i is the canonical affine chart of $\mathbb{P}^n_K$ corresponding to X_i

Proof. (a) (A function on $\mathbb{P}^n_K$ has the same number of zeros and poles with multiplicities) We know

$$K(X)^\times = K(U_0)^\times$$

where $U_0 =$ Spec $(K[X_0/X_0, X_1/X_0, .., X_n/X_0])$. So $K(X) = K(X_0/X_0, ..., X_n/X_0)$ So $f \in K(X)^\times$ is of the form $f = f_1/f_2$ where $f_i \in K[X_0/X_0, .., X_n/X_0]$.

Key fact: f us also $f = g_1/g_2$ where g_i is homogeneous of degree $\underline{deg g_1} = deg g_2$ in $K[X_0, .., X_n]$. Then factor g_1, g_2 in irreducibles in $K[X_0, ..X_n]$, there are homogeneous, say

$$f = \prod_i h_i^{n_i} \prod_j k_j^{-m_j}$$

with $n_i \geq 1, m_j \geq 1$ Then

$$\mathrm{div}(f) = \sum n_i D_i - \sum m_j E_j$$

and D_i is the prime divisors of h_i, E_j is the prime divisors of k_j. (Intuitively, it is clear, but we need a proof)

$\Longrightarrow$
$$\begin{aligned}\underline{deg}(\mathrm{div}(f)) &= \sum n_i \underline{deg}(D_i - \sum m_j \underline{deg}(E_j) \\ &\quad (\underline{deg}(D_i) = deg(h_i), \underline{deg}(E_j) = deg(k_j)) \\ &= deg(g_1) - deg(g_2) = 0.\end{aligned}$$

Then we come back to prove the Key fact:

$$f_1 = \sum_{\underline{d}} \alpha_{\underline{d}} \left(\frac{X_0}{X_0}\right)^{d_0} \cdots \left(\frac{X_n}{X_0}\right)^{d_n}$$

e.g.

$$\begin{aligned}&\left(\frac{X_1}{X_0}\right)^2 + 37\left(\frac{X_1}{X_0}\right)^3\left(\frac{X_2}{X_0}\right) \\ &= \frac{X_0^2X_1^2 + 37X_1^3X_2}{X_0^4} \\ &= \frac{1}{X_0^{degf_1}} \sum_{\underline{d}} \alpha_{\underline{d}} X_0^{degf_1 - \sum_{i=1}^n d_i} X_1 d_1 \cdots X_n^{d_n} \\ &= \frac{\text{homogeneous degree } degf_1}{X_0^{degf_1}} \\ &\Longrightarrow f_2 = \frac{\text{homogeneous degree } degf_2}{X_0^{degf_2}}\end{aligned}$$

$$\Longrightarrow \frac{f_1}{f_2} = \frac{X_0^{degf_1}(degf_1)}{(degf_2)X_0^{degf_1}}$$

(b) $\underline{deg} : Cl(X) \longrightarrow \mathbb{Z}$ is surjective because $\underline{deg}(D_0) = 1$, D_0 associated to X_0 and injective because if $deg(D) = 0$ write $D = D_1 - D_2$ with D_1, D_2 effective then $\underline{deg}(D_1) = \underline{deg}(D_2)$. Write $D_1 = \sum n_i E_i$, where E_i is prime divisors associated to h_i. $D_2 = \sum m_j F_j$, where F_j is prime divisors associated to k_j.

Then let $f = \prod h_i^{n_i} \prod k_j^{-m_j} \in K(X)^\times$, and as shown above $dic(f) = D_1 - D_2 = D$ so D is 0 in $Cl(X)$.

(c) the proof can be found in Hartshorne

□

(6) Further examples:

(a) $X \subset \mathbb{P}^4_K$ cubic, where K is an algebraic closed field. X is a surface, smooth, then $Pic(X) \simeq \mathbb{Z}^7$

(b) $Y \subset \mathbb{P}^2_K$ curve of degree d. Let $U \subset \mathbb{P}^3_K - Y$ be the complements, then

$$CL(U) \simeq \mathbb{Z}/d\mathbb{Z}$$

generated by $U \cap H_0$

6 Picard group

6.1 May 8th-B: Picard group, definitions

Definition 6.1. Let $(X, \mathcal{O}_X)$ be a ringed space. A sheaf of $\mathcal{O}_X-$ modules is a sheaf $\mathcal{F}$ on X so that $\mathcal{F}(U)$ is a $\mathcal{O}_X(U)$-module for any open U and for $V \subset U$

$$\mathcal{F}(U) \xrightarrow{\text{res}} \mathcal{F}(V)$$

is linear i.e. given $f \in \mathcal{O}_X(U), s \in \mathcal{F}(U)$

$$\text{res}(fs) = \text{res}(f)\ \text{res}(s)$$

One defines in an obvious way $\mathcal{O}_X$-linear morphism of $\mathcal{O}_X$-modules [$\forall U, \mathcal{F}_1(U) \longrightarrow \mathcal{F}_2(U)$ is $\mathcal{O}_X(U)$-linear], so ther is a category of $\mathcal{O}_X$-modules

Example 6.2. $n \geq 1$, $\mathcal{O}_X^n : U \longrightarrow \mathcal{O}_X(U)^n$ is an $\mathcal{O}_X(U)$-module.

Definition 6.3. An $\mathcal{O}_X$-moduel $\mathcal{F}$ is locally free of rank $n \geq 1$ is $\forall x \in X, \exists U$ open nbhd of x s.t.

$$\mathcal{F}|_U \simeq \mathcal{O}_U^u$$

as $\mathcal{O}_U$-module.

If $\mathcal{L}$ is locally free of rank 1, it is called an invertible sheaf.

Proposition 6.4. The set $Pic(X)$ of isomorphism class of invertible sheaves on X form s an abelian group with operation induced by

$$(\mathcal{L}_1, \mathcal{L}_2) \longmapsto \mathcal{L}_1 \otimes_{\mathcal{O}_X} \mathcal{L}_2$$

$1 =$ class of $\mathcal{O}_X$

inverse

$$\mathcal{L} \longmapsto \text{Hom}_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X)$$

N.B for $\mathcal{F}_1, \mathcal{F}_2$ $\mathcal{O}_X$-modules, we define

$$\mathcal{F}_1 \otimes_{\mathcal{O}_X} \mathcal{F}_2 = \text{ sheaf associated to the presheaf } U \mapsto \mathcal{F}_1(U) \times_{\mathcal{O}_X(U)} \mathcal{F}_2(U)$$

and

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F}_1, \mathcal{F}_2) = \text{ sheaf associated to } U \mapsto \text{ } \mathrm{Hom}_{\mathcal{O}_X(U)}(\mathcal{F}_1(U), \mathcal{F}_2(U))$$

6.2 May 11th: The twisting invertible sheaf $\mathcal{O}(n)$ on $\mathbb{P}^n$

Recall: $\mathcal{O}_X$-modules, locally-free $\mathcal{O}_X$-modules,
rank 1 locally free $\Longrightarrow$ invertible sheaves.

Proposition 6.5. $\mathrm{Pic}(X) = \{\text{iso. class of invertible sheaves}\}$ is an abelian group with $\mathcal{L}_1 \otimes \mathcal{L}_2$ and $1 = \mathcal{O}_X$, $\mathcal{L}^{-1} = \mathcal{H}om\,(\mathcal{L}, \mathcal{O}_X)$.

Proof. What needs to be done (given commutativity/ Associativity of $\otimes$) is

(1) if $\mathcal{L}_1, \mathcal{L}_2$ are invertible, so is $\mathcal{L}_1 \otimes \mathcal{L}_2$

(2) $\mathcal{L} \otimes \mathcal{O}_X = \mathcal{L}$

(3) $\mathcal{L} \otimes \mathcal{L}^{-1} \cong \mathcal{O}_X$.

(1): If $\mathcal{L}_1|_U \simeq \mathcal{O}_X|_U$ and $\mathcal{L}_2|_U \simeq \mathcal{O}_X|_U$, $(\mathcal{L}_1 \otimes \mathcal{O}_X)|_U \simeq \mathcal{O}_X|_U \otimes \mathcal{O}_X|_U \simeq \mathcal{O}_X|_U$, where the LHS is sheaf associated to presheaf, (given $V \subset U$) $V \longmapsto \mathcal{L}_1(V) \otimes \mathcal{L}_2(V)$ and the $\mathcal{O}_X(V) \otimes \mathcal{O}_X(V) \simeq \mathcal{O}_X(V)$. So the LHS is the sheaf $V \longmapsto \mathcal{O}_X(V)$ and $\mathcal{L}_1|_U \otimes \mathcal{L}_2|_U \simeq \mathcal{O}|_U$ and therefore $\mathcal{L}_1 \otimes \mathcal{L}_2$ is invertible.

Warning! in general, $\mathcal{L}_1 \otimes \mathcal{L}_2(U) \neq \mathcal{L}_1(U) \otimes \mathcal{L}_2(U)$.

(2) For any $U \subset X$,

$$\mathcal{L}(U) \otimes \mathcal{O}_X(U) \xrightarrow{\sim} \mathcal{L}(U)$$

$$(s, a) \longmapsto as$$

$\Longrightarrow$ a morphism of presheaves

$$[U \mapsto \mathcal{L}(U) \otimes \mathcal{O}_X(U)] \longmapsto \mathcal{L}$$

$\Longrightarrow$ a canonical morphism

$$\mathcal{L} \otimes \mathcal{O}_X \longmapsto \mathcal{L}$$

and this is an isomorphism because on stalks it is

$$\mathcal{L}_x \otimes \mathcal{O}_{X,x} \simeq \mathcal{L}_x$$

$$(s,a) \longmapsto as$$

which is an isomorphism

(3) For any $U \subset X$ we have an isomorphism of modules

$$\mathcal{L}(u) \otimes \mathcal{L}^{-1}_{pre}(U) \xrightarrow{\sim} \mathcal{O}_X(U)$$

$$LHS = \mathcal{L}(U) \otimes \operatorname{Hom}_{\mathcal{O}_X(U)}(\mathcal{L}(U), \mathcal{O}_X(U))$$

$$(s,\lambda) \longmapsto \lambda(s).$$

After sheafification, we get a morphism

$$\mathcal{L} \otimes \mathcal{L}^{-1} \longrightarrow \mathcal{O}_X$$

which at stalks is an isomorphism. □

Example 6.6.

$\boxed{1}$ Affine case: $X = \operatorname{Spec} A$. Theory of (quasi)-coherent sheaves establishes a connection between A-modules and $\mathcal{O}_X$-modules.

Given an A-module M, we can construct a $\mathcal{O}_X$-module $\tilde{M}$ by

$$\tilde{M}(U) = \left\{ s : U \longrightarrow \sqcup_{x \in U} M_x \;\middle|\; \begin{array}{l} \forall x, s(x) \in M_x, \forall x \in U, \exists V \subset U, \\ \text{s.t. for } x \in V, \exists m \in M, \exists f \in A, \\ \text{s.t. } \forall y \in V f \notin y,\ s(y) = \dfrac{m}{f} \in M_y \end{array} \right\}$$

subexample: $\tilde{A} = \mathcal{O}_X$ and $\tilde{M}$ is an $\mathcal{O}_X$-module:

$$(a \cdot s)(x) = a(x)s(x)$$

for all $a \in \mathcal{O}_X(U), s \in \tilde{M}(U)$

Facts:

(a) $\Gamma(U_f, \tilde{M}) \simeq M_f \longrightarrow$"$f(x) \neq 0$"

(b) stalk $\tilde{M}_x = M_x$ localization

(c) $\widetilde{M_1 \otimes M_2} = \tilde{M}_1 \otimes \tilde{M}_2$

Serre-Swan Locally-free $\mathcal{O}_X$-modules is in bijection with vector bundle and projective A-modules.

In practice, $\tilde{M}$ is an invertible sheaf iff M is projective, locally of rank 1 $M_{\mathfrak{p}} \cong A_{\mathfrak{p}}$ (when viewed as $A_{\mathfrak{p}}$-module)

Cor: If A is a UFD, then $Pic(\operatorname{Spec} A) = \{0\}$

$\boxed{2}$ If X has the usual regularity properties, and D is a prime divisor, there is a naturally associated invertible sheaf $\mathcal{L}(D)$: Let $U \subset X$ open small enough, so that $D \cap U$ is given by $f = 0$ on U, then

$$\mathcal{L}(D)(U) = \{s \in Frac(\mathcal{O}_X(U)|s = f^{-1}t, t \in \Gamma(U, \mathcal{O}_X)\}$$

One checks that this is well-defined (it is independent on the choice of f)

Then $\mathcal{L}(D)$ is an invertible sheaf. This extends to a group morphism

$$\mathrm{Div}(X) \longrightarrow Pic(X).$$

$\boxed{3}$ The twisting sheaf on projective space. Let K be a field. We define an important non-trivial invertible sheaf on $\mathbb{P}^n_K$, $n \geq 1$, denoted

$$\mathcal{O}(1) = \mathcal{O}_{\mathbb{P}^n_K}(1).$$

From the Proj point of view, where $K[X_0, .., X_n] =: A$

$$\mathbb{P}^n_K = \mathsf{Proj}(A)$$

$$\begin{array}{ll} M & \text{graded } A\text{-module} \\ \rightsquigarrow & \\ \tilde{M} & \mathcal{O}_{\mathsf{Proj}(A)}\text{-module} \end{array}$$

Take:

$$M = \bigoplus_{k \geq 1} A_k,$$

where A_k is the homogeneous part of degree k. $\Longrightarrow \tilde{M} = \mathcal{O}(1)$.

Glueing: n,

$$\mathbb{P}^n_K = \cup_{i=0} U_i$$

where $U_i = \mathrm{Spec}\,(B_i)$, $B_i = K[X_0/X_i, ..., X_n/X_i] \subset B = [X_0^{\pm}, .., X_n^{\pm}]$ glued over $U_{ij} = \mathrm{Spec}\,(B_{ij})$, with $B_{ij} = (B_i)_{X_j/X_i}$ using the isomorphism

$$B_{ij} = B_{ji} \subset B.$$

To define a sheaf $\mathcal{F}$ on $\mathbb{P}^n_K$ it suffices to consider sheaves $\mathcal{F}_i$ on U_i, isomorphisms $\varphi_{i,j}\mathcal{F}_i|_{U_{ij}} \simeq \mathcal{F}_j|_{U_{ij}}$ with the cocycle condition on $\varphi_{i,j}$. We define $\mathcal{L}_i$ on U_i by

$$\mathcal{L}_i = \tilde{M}_i$$

where $M_i = X_i B_i \subset B_i$ as B_i-module. We have $M_i \simeq B_i$ as B_i-module so $\tilde{M}_i \simeq \mathcal{O}_{\mathbb{P}^n}|_{U_i}$ we glue the $\mathcal{L}_i$ over U_{ij} using the isomorphisms

$$B \supset M_{i,\left(\frac{X_j}{X_i}\right)} = M_{j,\left(\frac{X_i}{X_j}\right)}.$$

These identity morphisms glue to an ivertible sheaf $\mathcal{O}(1)$ on $\mathbb{P}^n_K$. By $\boxed{1}$, we have

$$\Gamma(U_i, \mathcal{O}(1)) \cong \Gamma(U_i, \tilde{M}_i) = M_i = X_i B_i.$$

Proposition 6.7. We have

$$\dim_K \Gamma(\mathbb{P}^n_K, \mathcal{O}(1) = n+1)$$

and $\dim_K \Gamma(\mathbb{P}^n_K, \mathcal{O}) = 1$. (A basis of $\Gamma(\mathbb{P}^n_K, \mathcal{O}(1))$ is given by the "homogeneous coordinates")

Proof. Using the glueing perspective $s \in \Gamma(\mathbb{P}^n_K, \mathcal{O}(1))$ is equivalent to $(s_i), s_i \in \Gamma(U_i, \mathcal{O}(1))$ with $s_i|_{U_{ij}} = s_j|_{U_{ji}}$ which means

$$s_i \in M_i = X_i B_i \subset B$$

and $s_i = s_j$ in B. $\Longrightarrow$

$$\Gamma(\mathbb{P}^n_K, \mathcal{O}(1)) = \bigcap_{i=0}^{n} X_i B_i \subset B.$$

Similarly,$\Gamma(\mathbb{P}^n_K, \mathcal{O}) = \bigcap_{i=0}^n B_i \subset B$. ($\bigcap B_i = K$ because only constant polynomial in $K[X_0/X_i, ..., X_n/X_i]$ are allowed.) Let $s \in \bigcap X_i B_i$,

$$\begin{aligned} \forall i, s &= X_i g_i(X_0/X_i, ..., X_n/X_i) \in A \\ &= \frac{f_i(X_0, ..., X_n)}{X_i^{d_i}} \end{aligned}$$

with $X_i \nmid f_i, d_i \geq 0$. Thus,

$$X_i^{-d_i} f_i = X_j^{-d_j} f_j$$

for all j, $x_j^{d_j} f_i = X_i^{d_i} f_j$, $\forall i, j$; since $X_k \nmid f_j, d_i = 0 \Longrightarrow i, j$ $f_i = f_j$ but f_i is homogeneous of degree $d_i + 1 = 1$, so $s \longleftrightarrow (f) \in$ homogeneous degree 1. Conversely, any f homogeneous of degree 1 is in $\bigcap X_i B_i$ $X_i = X_i \cdot 1 = X_j \cdot \frac{X_i}{X_j}$ so $\Gamma(\mathbb{P}^n_K, \mathcal{O}(1)) \xrightarrow{\sim} \{$ homogeneous polynomials of degree 1 in $A\}$ $\cong K^{n+1}$ as K-vector spaces. $\square$

Theorem 6.8. $Aut_{\mathsf{Sch}}(\mathbb{P}^n_K) \simeq PGL_{n+1}(K) = GL_{n+1}(K)/K^\times I_{n+1}$ given by

$$g \longmapsto ([x_0 : ... : x_n] \longrightarrow [\sum_j a_{0j}x_j : ... : \sum_j a_{nj}x_j])$$

with a_{ij} the entries of g.

This uses

Theorem 6.9 (Hartshorne II6.16)**.** X Noetherian, integral, quasi-projective, every local ring is regular $\Longrightarrow$ the map $D \longmapsto \mathcal{L}(D)$ gives an isomorphism

$$Cl(X) \xrightarrow{\simeq} Pic(X)$$

Proof of 6.8. We construct an inverse

$$Aut(\mathbb{P}^n_K) \longrightarrow PGL_{n+1}(K)$$

to the morphism in the statement of 6.9.

Idea: Any automorphism $\gamma : \mathbb{P}^n_K \xrightarrow{\sim} \mathbb{P}^n_K$ "acts linearly on $\Gamma(\mathbb{P}^n, \mathcal{O}(1)) \simeq K^{n+1}$". Precisely: As part of definition of morphism of scheme γ we get an morphism of sheaves

$$\gamma^* : \mathcal{F} \longrightarrow \gamma^*\mathcal{F}$$

where γ^* is pullback functor, see chap 16 of Vakil for a definition. In particular, we get

$$\mathcal{O}(1) \longrightarrow \gamma^*\mathcal{O}(1)$$

Key claim: $\gamma^*\mathcal{O}(1) \simeq \mathcal{O}(1)$. we can not simply argue that γ has an inverse δ^*, say δ would imply $\mathcal{F} \longrightarrow \gamma^*\mathcal{F}$ has an inverse. At best we can say $\delta^* \circ \gamma^*$ is naturally isomorphic to $id_{QCh_{\mathbb{P}^n_K}}$ as functors. This does not guarantee that $\mathcal{F} \longrightarrow \gamma^*\mathcal{F}$ is an isomorphism. We should be very lucky if it is true. However, by functorial property of γ^*, we know it induce well-defined morphism on the Picard group. When γ is an automorphism, it induce isomorphism on the Picard group, it send generators to generators.

Indeed, $\mathcal{O}(1) \in \operatorname{Pic}(\mathbb{P}^n_K) \simeq Cl(\mathbb{P}^n_K) \simeq \mathbb{Z}[H_0]$ corresponds to $[H_0]$, where H_0 means the hyperplane where $X_0 = 0$. $\gamma^*\mathcal{O}(1) \in \operatorname{Pic}(\mathbb{P}^n_K)$ is therefore also a generator of $\operatorname{Pic}(\mathbb{P}^n_K)$. $\gamma^*\mathcal{O}(1)$ can only be either $\mathcal{O}(1)$ or $\mathcal{O}(1)^{-1}$ However, one checks

$$\Gamma(\mathbb{P}^n_K, \mathcal{O}(1)^{-1}) = \{0\}$$

so that $\gamma^*\mathcal{O}(1) \neq \mathcal{O}(1)^{-1}$, hence the key claim is correct.

So we get

$$\mathcal{O}(1) \xrightarrow{\varphi} \gamma^*\mathcal{O}(1) \xrightarrow{\sim} \mathcal{O}(1)$$

$\Longrightarrow$ an isomorphism

$$K^{n+1} \simeq \Gamma(\mathbb{P}^n, \mathcal{O}(1)) \xrightarrow{\gamma\circ\varphi} \Gamma(\mathbb{P}^n, \mathcal{O}(1)) \simeq K^{n+1}$$

K-linear in $GL_{n+1}(K)$.

φ is only defined up to an automorphism of $\mathcal{O}(1)$: $\mathcal{O}(1) \simeq \mathcal{O}(1)$

Claim:

$$Aut_{\mathsf{Sheaves}}(\mathcal{O}(1)) \simeq K^\times$$

$$[s \mapsto \lambda s] \leftarrow\!\shortmid \lambda$$

$$\mathrm{Hom}_{\mathsf{Sheaves}}(\mathcal{O}(1), \mathcal{O}(1))$$

$$\mathcal{O}(1) \xrightarrow{f,\sim} \mathcal{O}(1)$$

$$\rightsquigarrow \mathcal{O}(1) \otimes \mathcal{O}(1)^{-1} \xrightarrow{\sim} \mathcal{O}(1) \otimes \mathcal{O}(1)^{-1}$$

$$\rightsquigarrow K \simeq \Gamma(\mathbb{P}^n, \mathcal{O}) \xrightarrow{\sim} \Gamma(\mathbb{P}^n, \mathcal{O}) \simeq K.$$

$\square$

6.3 May 15th-A: proof continued

Recall the theorem in last lecture:

$$Aut_{\mathsf{Sch}}(\mathbb{P}^n_K) \cong PGL_{n+1}(K)$$

$$\left[[x_0 : ... : x_n] \mapsto [\sum_j a_{0j}x_j : ... : \sum_j a_{nj}x_j] \right] \leftarrow\!\shortmid g = (a_{ij})$$

Proof. Construct an inverse, $Aut(\mathbb{P}^n_K) \longrightarrow PGL_{n+1}(K)$, by looking at the action of an automorphism γ on $\Gamma(\mathbb{P}^n_K, \mathcal{O}(1)) \cong K^{n+1}$.

Key Claim: let $\gamma^*\mathcal{O}(1)$ by $U \mapsto \Gamma(\gamma(U), \mathcal{O}(1))$, then $\gamma^*\mathcal{O}(1)$ is a sheaf, isomorphic to $\mathcal{O}(1)$

Proof of the key claim. $\gamma^*\mathcal{O}(1) \in \operatorname{Pic}(\mathbb{P}^n_K) \cong Cl(\mathbb{P}^n_K) \cong \mathbb{Z} \cdot [H_0]$, where $H_0 = \mathbb{P}^n_K - U_0$. Moreover, doing the same construction to other $\mathcal{L} \in \operatorname{Pic}(\mathbb{P}^n_K)$, we get that $\mathcal{L} \mapsto \gamma^*\mathcal{L}$ is a group isomorphism $\operatorname{Pic}(\mathbb{P}^n_K) \longrightarrow \operatorname{Pic}(\mathbb{P}^n_K)$, so $\gamma^*\mathcal{O}(1)$ is generator of $\operatorname{Pic}(\mathbb{P}^n_K) \cong \mathbb{Z}$, then we know $\gamma^*\mathcal{O}(1)$ is either isomorphic to $\mathcal{O}(1)$ or $\mathcal{O}(1)^{-1}$, but by definition

$$\Gamma(\mathbb{P}^n_K, \gamma^*\mathcal{O}(1)) := \Gamma(\mathbb{P}^n_K, \mathcal{O}(1)) \ncong \Gamma(\mathbb{P}^n_K, \mathcal{O}(1)^{-1}) = \{0\}$$

So the key claim must be correct. □

So we have an isomorphism $\sigma : \gamma^*\mathcal{O}(1) \longrightarrow \mathcal{O}(1)$, $\Longrightarrow \Gamma(\mathbb{P}^n_K, \mathcal{O}(1)) \xrightarrow{\sigma|_{\mathbb{P}^N_K}} \Gamma(\mathbb{P}^n_K, \mathcal{O}(1))$

i.e. $\sigma|_{\mathbb{P}^n_K} \in GL_{n+1}(K)$

Remark: this depends on the choice of σ, which may be changed to $\tau \circ \sigma$ where $\tau \in Aut_{\mathcal{O}-module}(\mathcal{O}(1))$

However, we have an isomorphism, $\operatorname{Hom}_{\mathcal{O}-mod}(\mathcal{O}(1), \mathcal{O}(1)) \cong \operatorname{Hom}_{\mathcal{O}-mod}(\mathcal{O}, \mathcal{O})$, $f \longmapsto f \otimes \mathcal{O}(1)^{-1}$, the later is an automorphism on $\mathcal{O}$.

An $f : \mathcal{O} \longrightarrow \mathcal{O}$, given $f|_{U_i} : \mathcal{O}(U_i) \longrightarrow \mathcal{O}(U_i)$ is an morphism of rings $B_i \longrightarrow B_i := K[X_0/X_i, ..., X_n/X_i]$ this has to be B_i-linear, determined by $b_i =$image of 1, compatible with restriction, $\Longrightarrow \forall i, jb_i = b_j \in B = K[X_k^{\pm 1}, 0 \leq k \leq n]$. f has to be a common element in $\cap_i B_i$, and the only choice is $f \in K$.

Therefore, we have $\operatorname{Hom}_{\mathcal{O}-mod}(\mathcal{O}(1), \mathcal{O}(1)) \cong K$, so σ is determined up to $K^\times$, so the image of γ in $PGL_{n+1}(K)$ is well-defined, one checks that is an inverse to the morphism $PGL_{n+1}(K) \longrightarrow Aut(\mathbb{P}^n_K)$. □

7 Algebraic Curves

7.1 May 15th-B: Preliminaries

Definition 7.1. An algebraic curve C over a field K, is an integral 1-dimensional scheme C/K

A non-singular C/K is a curve where every $\mathcal{O}_{C,x}$ is regular, for x being closed.

A non-singular projective curve C/K is a one dimensional K-subscheme of $\mathbb{P}^n_K$ and C is non-singular.

Warning: in general, smooth $\neq$non-singular. (NO problem if K is algebraic closed.)

Notation: $K(C)$ if the function field of C, and $K(C)/K$ is a field extension of transcendence degree 1.

Example 7.2. $C = \mathbb{P}^n_K$, non-singular projective curve, with $K(C) \cong K(T)$ moreover, any non-zero $f \in K(C)$ corresponds uniquely to a morphism $C \xrightarrow{\bar{f}} \mathbb{P}^n_K$ as follows:

if $f \in \Gamma(U, \mathcal{O}_C)$, where U is maximal open set (such that f is regular on U), then $f \longleftrightarrow f \in \Gamma(U, \mathcal{O}_C) \cong \text{Hom}_{\mathsf{Sch}}(U, \mathbb{A}^1_K))$. i.e.

$$f \longleftrightarrow p \mapsto [f(p), 1]$$

so $\tilde{f}|_U : U \longrightarrow \mathbb{A}^1_K$ and maps $C - U$ to the infinity point $\{\infty\} = \mathbb{P}^1_K - \mathbb{A}^1_K$

For detailed discussion, see Silverman II.2.2

Proposition 7.3. (1) $C_1 \xrightarrow{f} C_2$ a morphism of curves over K, then it is either constant or dominant ($f(C_1)$ dense)

(2) If C_1 and C_2 are both projective, f is either constant or surjective.

idea: (2) is a special case of

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr] & Y \arrow[d] \\ & \operatorname{Spec} K \end{tikzcd}$$

if both X, Y are projective $\Longrightarrow$ $f(X)$ is closed in Y. Because the only closed subset in a curve is either closed point or the whole set.

Example 7.4. (1) $\mathbb{P}^1_K, \mathbb{A}^1_K$

(2) $K = \mathbb{C}$, Riemann:

$\{$non-singular projective curvs $C/\mathbb{C}\} \longleftrightarrow \{$compact connected Riemann surfaces$\}$

e.g. if Γ is a discrete subgroup of $SL_2(\mathbb{R})$, torsion-free, then $\Gamma \backslash \mathbb{H}$ is a Riemann-surface, for any such Γ's, it is compact. Any "hyperbolic" compact Riemann surface has this form (Poincare-Koebe uniformization theorem)

Riemann "conjectured" that the "space" of compact Riemann surfaces is a disjoint union of spaces homeomorphic to $\mathbb{C}^{3g-3}$.

(3) K arbitrary, if $f \in K[X_1, X_2]$ is irreducible, non-constant, then $V(f) \subset \mathbb{A}^2_K$ is a curve. It is non-singular, provided for any closed point x, the partial derivative of f at x are not all zero.

7.1.1 Hyperelliptic curve

$f \in K[X,Y]$. with *Char* $K \neq 2$. Let $f(X,Y) = Y^2 - g(X)$ for $g \in K[X]$ and g is square free. Then f is irreducible in $K[X,Y]$, and $V(f)$ is non-singular. consider the point (x,y), solve $y^2 = g(x)$ then $\partial_X f(x,y) = -g'(x)$ and $\partial_Y f(x,y) = 2y$, if both are zero, then $y = 0$. then $g(x) = g'(x) = 0$, contradicts that g is square free.

If $\deg(g) = 3$, we get a so called elliptic curve.

Note: by varying g, we get many different hyperelliptic curves, in fact, if we fix $\deg(g) = d$, we have d parameters.

7.1.2 Artin-Schreier Curves

K is an algebraically closed field and $Char(K) = p > 0$, $f(X,Y) = Y^p - Y - g(X)$ Suppose, $\deg(g) < p$, then f is irreducible, and non-singular $V(f)$.

It is nonsingular because $K = \overline{K}$

$$\begin{cases} y^p - y = g(x) \\ \partial_X f(x,y) = -g'(x) \\ \partial_Y = py^p - 1 = -1 \neq 0 \end{cases}$$

It is irreducible because $p \neq 2$. Assume $Y^p - Y - g = g_1 g_2$ in $L[Y]$ where $L = K(X)$ assume that g_1, g_2 are monic, key observation: if $a \in \mathbb{F}_p \subset K$, $(y+a)^p - (y+a) - g = y^p + a^p - y - a - g = Y^p - Y - g = f$. By uniqueness of factorization either

$$g_1(Y+a) = \alpha g_1(Y)(**)$$

or

$$g_1(Y+a) = \alpha g_2(Y)(*)$$

where $\alpha = 1$ because g_i monic.

Assume $a = 1$ and $(*)$ occurs, then by iterating , $(**)$ happens for $a = 2$. Then get $(**)$ for $a = 1$ by iterating.

$$g_1(Y) = Y^{d_1} + a_1 Y^{d_1 - 1} + \cdots$$

$$\begin{aligned} g_1(Y) &= g_1(Y+1) = (Y+1)^{d_1} + a_1(Y+1)^{d_1-1} + \cdots \\ &= Y^{d_1} + (d_1 + a_1)Y^{d_1-1} + \cdots \end{aligned}$$

so $a_1 = a_1 + d_1 \iff d_1 = 0$. So $p \mid d_1 \leq \deg(f) = p$ so $d_1 = 0$ or $d_1 = p$.

In the case of $d_1 = 0$, we have g_1 is constant anf $g_2 = f$, in the other case we have $g_1 = f$ and g_2 is constant.

Remark 7.5. (1) If $\deg(g) \geq p$ the irreduciblility statement may fail. e.g. $y^p 0Y - (X^p - X) = (Y-X)^p - (Y-X) = (Y-X)((Y-X)^{p-1} - 1)$ is not irreducible.

(2) Consider $V(f)$, for $\deg(g) < p$.

We have a morphism $V(f) \longrightarrow \mathbb{A}^1_K$ corresponding to

$$(X,Y) \longmapsto X$$

$$K[X] \hookrightarrow K[X,Y]/(f)$$

which is a "covering": every $x \in \overline{K}$, has p distinct pre-image $y^p - y = g(x)$. it is connected $\partial_y = -1 \Longrightarrow$ no repeated roots.

in the case $\mathbb{C}$, $\mathbb{C} \longrightarrow \mathbb{C}$ is a unique connect covering.

In the case $p > 0$, $\mathbb{A}^1_K$(or $\mathbb{A}^n_K$) is very far from being simply connected.

7.2 May 18th-A:Non-singular curves

(3) If $0 \neq f \in K[X,Y,Z]$, homogeneous, non-constant, irreducible, then $V(f) \subset \mathbb{P}^2_K$ is an algebraic curve of K, integral.

E.g. (Hyperelliptic) $g \in K[X,Z]$, homogeneous degree $d \geq 3$, $f = Y^2 Z^{d-2} - g(X,Z)$, defines a plane projective hyperelliptic curve, if we look at the intersection with $\mathbb{A}^2_K$ = open pieces with $z \neq 0$ (= $\operatorname{Spec} K[X/Z, Y/Z]$), then we recover $C_f = Y^2 - g(X) = 0$, if g is square free and $CharK \neq 2$, C_f is non-singular. To see whether $V(f)$ is also non-singular, we compute the points at ∞ of $V(f)$ $[V(f) - C_f]$, we need to solve the equation.

$$Y^2 Z^{d-2} = g(X,Z) \text{ with } Z = 0$$

$g(X,Z) = a_d X^d + a_{d-1} X^{d-1} Z + \cdots$, then we get $0 = a_d X^d$ assume $a_d \neq 0$ then we get $X = 0$, $[0:1:0]$ at infinity on $V(f)$.

to check non-singularity:

$$\begin{cases} \dfrac{\partial f}{\partial X}(\infty) = 0 - 0 = 0 \\ \dfrac{\partial f}{\partial Y}(\infty) = Z/Z^{d-2}(\infty) = 0 \\ \dfrac{\partial f}{\partial Z}(\infty) = (d-2)Z^{d-3}Y^2(\infty) - 0 \quad = \begin{cases} 1, \ d = 3 \\ 0 \ d \geq 4 \end{cases} \end{cases}$$

Conclusion: (a) if $\deg_X g = 3 = \deg g$ and g is square free, $Y^2Z - g(X,Z) = 0$ defines a non-singular projective curve over K.

(b), if $\deg g \geq 4$, the point at ∞ is singular.

Artin-Schreier over finite field: $Char\ K = p \geq 2$, g homogensous polynomial of degree $d = \deg_X g = d \leq p$, $f = Y^p - YZ^{p-1} - Z^{p-d}g(X,Z)$. $V(f \cap \mathbb{A}^2_K)$ is the Artin-Schreier non-singular curve $Y^p - Y = \tilde{g}(X)$ with $\tilde{g}(X) = g(X,1)$, at ∞, we solve with $z = 0 : Y^p = 0, \Longrightarrow \infty = [1:0:0]$

• Moreover, $\frac{\partial f}{\partial X}(\infty) = 0$, $\partial f/\partial Y(\infty) = (pY^{p-1} - Z^{p-1} - 0)(\infty) = 0$,

$$\begin{aligned}\frac{\partial f}{\partial Z}(\infty) &= [-(p-1)YZ^{p-2} - (p-d)Z^{p-d-1}g(X,Z) - Z^{p-dg_Z(X,Z)}](\infty) \\ &= d_{neq0}Z^{0-d-1}g(1,0)\begin{cases} a_d d \text{ if } d = p-1 \\ 0 \text{ if } d < p-1 \end{cases}\end{aligned}$$

again, ∞ is often singular.

To understand the projective non-singular curves, one has the following theorem

Theorem 7.6. (Goertz-Wedhorn, 15.22), the functor $C \mapsto K(C)$, (non-constant $(f : C_1 \longrightarrow C_2) \longrightarrow (f^* : K(C_2) \longrightarrow K(C_1))$ is contravariant equivalence of categories between

$$\left\{\begin{array}{l}\text{normal proper integral curves over } K \\ \text{with non-constant morphisms}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Transcendental extension } L/K \\ \text{finitely generated} \\ \text{and of transcendence degree } 1\end{array}\right\}$$

• Interpretation: Any field L as in RHS is the function field of a unique (up to isomorphism) curve C/K projective and non-singular, in particular, if U/K is an integral geometric connected curve, then $K(U)$ is of this type, so ther eis a unique non-singular projective C with $K(C) = K(U)$

• Example: there are smooth projective C/K with the same function field as non-singular, hyperelliptic (Or Artin-Schreier) affine curves.

• A generic construction: $U \supset U_i = \operatorname{Spec} A_i$ dense, let $B_i \subset K(U_i) = K(U)$, s.t. f satisfies a monic polynomial equation with coefficients in A_i.

$B_i \supset A_i$, using the algebraic properties of integral closure, we get a scheme C by glueing the $\operatorname{Spec} B_i$ and a morphism $C \longrightarrow U$. One shows (1) C is a curve because $K(C) = K(U)$, (2) C is non-singular because local rings are integral, Noetherian, dimension 1 and integrally closed.

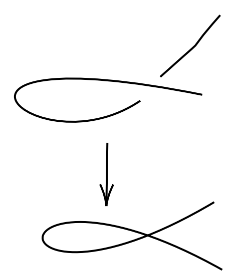
One shows that C is quasi-projective and is projective if U is.
In the general picture: $\overline{C}$:

$$\begin{tikzcd}
& \overline{C} \arrow[r] \arrow[d] & \text{non-singular, projective} \\
U \arrow[r, hook, "open"] & \overline{U} & K(\overline{C}) = K(\overline{U}) = K(U) \\
\cap & \cap & \\
\mathbb{A}^n_K & \mathbb{P}^n_K &
\end{tikzcd}$$

If U is non-singular, we have

$$\begin{tikzcd}
\pi^{-1}(U) \arrow[r] \arrow[d, "\pi"] & \overline{C} \arrow[d, "\pi\text{--desingularization of } \overline{U}"] \\
U \arrow[r] & \overline{U}
\end{tikzcd}$$

$\pi|_{\pi^{-1}(U)}$ is an isomorphism over x singular, there are usually ≥ 2 (non-singular) points of $\overline{C}$



$\subset \mathbb{A}^3_K$

$\subset \mathbb{A}^2_K$

• Definition: $C_1 \xrightarrow{f} C_2$, morphism of curves, if f is non-constant, then it is associated to a unique $f^* : K(C_2) \hookrightarrow K(C_1)$ an dit is a finite extension, one denotes $\deg(f) = [K(C_1) : K(C_2)]$

• Example: $C_g : Y^2 = g(X)$, then $K(C_g) = K(X)(\sqrt{g})$, where $K(X)$ is the base field and $K(X)\sqrt{g}/K(X)$ is of transcendence degree 2 if g is square free.

$$\begin{tikzcd}
C_g \arrow[d, "\pi"] & (x,g) \arrow[r] \arrow[d, mapsto] & K(X) \hookrightarrow K(C_g) \\
\mathbb{A}^1 & x & \deg(\pi) = 2
\end{tikzcd}$$

7.3 May 18th-B: Riemann-Roch Theorem

• History: late 19th century, and generalized by Serre Hirzebruch, Grothendieck. in 1960s.

• This theorem computes dimensions of global sections of invertible sheaves on C, a non-singular projective curve.

• Convnetion: curve=nonsingular projective curve (in this section)

Definition 7.7. C/K curve $D = \sum_i n_i[x_i], n_i \geq 1$, x_i closed point, a Weil divisor. $\mathcal{L}(D)$ invertible sheaf, and $\mathcal{L}(D)$ is defined as follows: $U \subset C$ open dense, if $U \cap \{x_i\} = \emptyset$, then $\Gamma(U, \mathcal{L}(D)) = \Gamma(U, \mathcal{O}_C)$ if $U \cap \{x_i\} = \{x_0\}$ then let $\pi_0 \in K(C)$ be a uniformizer of C at x_0. (π_0 has zero of order 1 at x_0), then $\Gamma(U, \mathcal{L}(D)) = \pi_0^{-n_0}(\Gamma(U, \mathcal{O}_C))$ where n_0 is the coefficient of x_0 in D.

Interpretation: section of $\mathcal{L}(D)$ on U has

$$\begin{cases} \bullet \text{ at most a pole of order } n_i \text{ at } x_i, \text{ if } n_i \geq 1 \\ \bullet \text{ at least a zero of order } -n_i \text{ at } x_i, \text{ if } n_i \leq -1 \end{cases}$$

Fact: $\mathcal{L}(D)$ is invertible, the map $D \longrightarrow \mathcal{L}(D)$ induces a group morphism

$$\mathrm{Div}(C) \longrightarrow \mathrm{Pic}(C)$$

and $Cl(C) \xrightarrow{\sim} \mathrm{Pic}(C)$

Definition 7.8. $\ell(D) = \dim_K \Gamma(C, \mathcal{L}(D))$ (it is finite)

Proposition 7.9. *C curve over K. let $f \in K(C)^\times$ and let $\deg : \mathrm{Div}(C) \longrightarrow \mathbb{Z} : x \longmapsto [K(x) : K]$, then*

$$\deg(\mathrm{div}(f)) = 0$$

It means $\mathrm{div}(f)$ has as many poles as zeros.

Proof. (i) if $f \in K^\times$, the $\mathrm{div}(f) = 0$, has degree 0.

(ii) if $f \notin K^\times$, f is transcendental over K, so $K \subset K(f) \subset K(C)$, so $K(C)/K(f)$ is finite and corresponds to a morphism $C \xrightarrow{\pi} \mathbb{P}^1_K$, define

$$\pi^* : \mathrm{Div}(\mathbb{P}^1_K) \longrightarrow \mathrm{Div}(C)$$

$$x \longmapsto \sum_{y \in \pi^{-1}(x), y \text{ closed in } C} v_y(\pi_x) y$$

where v_y is the valuation on the local ring of C at y, $\pi_x \in K(f) \subset K(C)$ is a uniformizer at x.

• Observe that: $\pi^*(\mathrm{div}(g)) = \mathrm{div}(g \circ \pi)$,

$$\begin{tikzcd} C \arrow[r, "\pi"] \arrow[rr, bend right, "g\circ\pi"'] & \mathbb{P}^1_K \arrow[r, "g"] & \mathbb{P}^1_K \end{tikzcd}$$

So π^* induces a group morphism $\mathbb{Z}[\infty] = \mathbb{Z}[0] \cong Cl(\mathbb{P}^1_K) \xrightarrow{\pi^*} Cl(C)$, which must be $\pi^*(k) = k\pi^*([0])$, then check that $\mathrm{div}(f) = \pi^*([0]-[\infty]) \Longrightarrow \deg(\mathrm{div}(f)) = \deg(k\pi^*([0])) - k\pi^*(\infty) = 0$.

(in fact: $\deg(\pi^(D)) = \deg(\pi)\deg(D)$) $\square$

Theorem 7.10. (Riemann-Roch,R-R) C non-singular projective over K, then there exists $g \geq 0$ integer,("genus of C") and a divisor class K_C ("canonical divisor of C") on C, such that, for any divisor D on C, $\ell(D) - \ell(K_C - D) = \deg(D) + 1 - g$.

7.4 May 22nd: The proof of Riemann-Roch

Recall: $\deg(\mathrm{div}(f)) = 0, f \in K(C)^\times$.

Proof. $\mathrm{div}(f) = f^*([0]-[\infty])$, where $f^* : \mathrm{Div}(\mathbb{P}^1_K) \longrightarrow \mathrm{Div}(C)$. One checks that $\deg(f^*D) = \deg(f)\deg(D)$

$$\Longrightarrow \deg(\mathrm{div}(f)) = \deg(f)(\deg([0]-[\infty])) = 0$$

$\square$

• Riemann-Roch Theorem: K is a field, C is a nonsingular projective curve over K, there exists an integer $g \geq 0$ and divisor class $K_C \in Cl(C)$ such that for any $D \in \mathrm{Div}(C)$.

$$\ell(D) - \ell(K_C - D) = \deg(D) + 1 - g$$

, where $\ell(D) = \dim_K \Gamma(C, \mathcal{L}(D))$

• Interptation: $\Gamma(C, \mathcal{L}(D)) = \{0\} \cup \{f \in K(C)^\times | f$ has at x_i a pole of order $\leq n_i$ and a zero of order for

$$D = \sum_{i\in I} n_i x_i - \sum_{j \in J} m_j y_j$$

where x_i, y_j are pairwise distinct closed point in C.

$f \in K(C)^\times$ is in $\Gamma(C, \mathcal{L}(D))$, and U_i is an open set containing x_i and no other x_k or y_j, then $f|_U = f$ must belong to $\pi_i^{-n_i}\Gamma(U, \mathcal{O}_C)$, where π_i is the uniformizer at x_i, so $f\pi_i^{n_i} \in \Gamma(U, \mathcal{O}_C)$, so $v_{x_i}(f) \geq -n_i$, (which means pole of order $\leq n_i$)

In other words: $f \in \mathcal{L}(D) \Longleftrightarrow \mathrm{div}(f) + D \geq 0$, $\sum v_x(f) \cdot x + D \geq 0$

Corollary 7.11.

(1) if $\ell(D) \geq 1$, then $\deg(D) \geq 0$

(2) if $\ell(D) \geq 1$ and $\deg(D) = 0$, then D is principle ($0 \in Cl(D)$) and $\ell(D) \geq 1$.

Proof. (1) if $0 \neq f \in \mathcal{L}(D)$, f exists $\ell(D) \geq 1$. We then have $\operatorname{div}(d) + D \geq 0$ $\Longrightarrow 0 + \deg(D) \geq 0$, $[\deg(\operatorname{div}(f))] = 0$

(2) if $0 \neq f \in \mathcal{L}(D)$, then $D + \operatorname{div}(f) \sim D$ in $Cl(C)$. So, if $\deg(D) = 0$, D is equivalent to $D + \deg(f) \geq 0$, which is effective of degree 0, hence is the zero divisor.

In particular, if $\deg(D) > \deg(K_C)$, $\ell(K_C - D) = 0$ by part (1) in the Corollary above. So R-R gives $\ell(D) = \deg(D) + 1 - g$ in particular, if $\deg(D) > g - 1$, we have $\ell(D) \geq 1$. There exists $0 \neq f$ ikn $K(C)$ with poles/zeros controlled by D. □

Moreover to say that f has a zero at x is a linear condition on f. Similarly for f having a pole at x ($\Longleftrightarrow V_f$ has a zero).

Recall that for $D = 0$. $\Gamma(C, \mathcal{L}(D) = \Gamma(C, \mathcal{O}_C)) = K$ allowing a pole at x, gives intuitively one degree of free-dimension, for more poles, we get more and more possibilities.

$\Longrightarrow$, intuitively, we expect $\leq \deg(D)$ posibilities, and hope this should be close to the truth, this i s what R-R ccomes from.

•, Now for $D = D_1 - D_2$, where $D_1, D_2 \geq 0$, we get about $\deg(D_1)$ solutions by the above, and take at $\deg(D_2)$ by imposing extra linear conditions.

N.B. $\ell(D) \geq \deg(D) + 1 - g$,(by Riemann)

Corollary 7.12. (1) $\ell(K_C) = g$

(2) $\deg(K_C) = 2g - 2$

(3) K_C is unique, if $K_1.$, K_2 both satisfies R-R, we would know

$$K_1 \sim K_2 \in Cl(C)$$

Proof. 1 $D = 0$ in R-R, $\ell(D) - \ell(K_C) = 0 + 1 - g$, $\Longrightarrow \ell(K_C) = g$, because $\dim_K(C, \mathcal{L}([0])) = \dim_K(C, \mathcal{O}_C) = 1$

2 $D = K_C$ in R-R: $\ell(K_C) = \ell(0) = \deg(K_C) + 1 - g$

$$\Longrightarrow \deg(K_C) = 2g - 2$$

3 $D = K_2$ in R-R for K_1, $\ell(K_2) - \ell(K_1 - K_2) = \deg(K_2) + 1 - g = 2g - 2 + 1 - g$

$$\Longrightarrow \ell(K_1 - K_2) = 1$$

but $K_1 - K_2$ has degree 0, Then by part (2) of Corollary above,know $K_1 - K_2 \sim 0$

□

Example 7.13. (1) $[g = 0]$ $C = \mathbb{P}^1_K$, we know that $Cl(C) \simeq \mathbb{Z}$. say with $[\infty]$ as generator, (One we recovers this by noting that $\infty \neq x \sim \infty$ in $Cl(\mathbb{P}^1)$, because $f = (T - X)$ has single 0 at x and a single pole at ∞) So $D = \sum n_i x_i \sim (\sum n_i)\infty$. inparticular, if R-R holds, it means with $K_{\mathbb{P}^1} \sim (2g-2)\infty$.

Claim: R-R holds with $g = 0$, (hence $K_C = -2\infty$),

- R-R: (enough to check that for $n \in \mathbb{Z}$, $(n \cdot \infty) - \ell((-2-n)\infty) = n + 1$)
- Assume $n \geq 0$,

$$\begin{aligned}\Gamma(\mathbb{P}^1, \mathcal{L}(n\infty)) &= \{f \in K(T) \cap \Gamma(\mathbb{A}^1_K, \mathcal{O}_{\mathbb{P}^1} | v_\infty(f) \geq -n\} \\ &= \{f \in K[T] | \deg(f) \leq n\} (\text{ has dimension } n+1)\end{aligned}$$

Since $\ell(-(n+2)\infty) = 0$, we get R-R in that case $\deg < \infty$.

$n = -1$, $\ell(-\infty) - \ell(-\infty) \stackrel{?}{=} 0$

$n \leq -2$, $0 - \ell(-(n+2)\infty) \stackrel{?}{=} n + 1$, it is the case because $\ell(-(n+2)\infty) = -n - 2 + 1$ by the derivation above.

(2) $[g = 0,$ abstractly $]$ $K_1 = \overline{K}$,

Claim: if C satisfies R-R with $g = 0$, then C is isomorphic to $\mathbb{P}^1_K$.

Step 1: $Cl(C) \simeq \mathbb{Z}$, generated by any x closed point of C

proof: $\deg : Cl(C) \longrightarrow \mathbb{Z}$, is surjective, (because $\deg(X) = 1$ for a closed point) Let D be a divisor with $\deg(D) = 0$, apply R-R to D:

$$\ell(D) - \ell(k_C - D) = 0 + 1$$

where $\deg(K_C - D) = \deg(K_C) - \deg(D) = -2 - 0 < 0 \Longrightarrow \ell(K_C - D) = 0$.

$\Longrightarrow \ell(D) = 1 \Longrightarrow D$ is principle.

Step 2: Pick two distinct $x_0 \neq x_1 \in C$ (closed points), Consider $D = x_0 - x_1$, by step 1, D is principle, let $f \in K(C)^{\times}$ have divisor D, then f has a single zero at x_0, single pole at x_1.

Consider $\tilde{f} : C \longrightarrow \mathbb{P}^1_K$

$$\begin{cases} x_0 \longmapsto 0 \\ x_1 \longmapsto \infty \end{cases}$$

this is an isomorphism.

Augument 1: $\tilde{f}$ is a bijection on closed points, hence a homeomorphism for Zariski topology.

Consider $y \in \mathbb{P}^1_K - \{0, \infty\}$, closed point, consider g

7.5 May 25th:

Recall: Riemann-Roch C/K nonsingular projective curve over K , $\exists g \geq 0, \exists K_C \in$ Pic(C)
s.t. $\forall D \in$ Div(C)

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

We saw.

$$\deg(K_C) = 2g - 2$$

$$\ell(K_C) = g$$

(3) in the case $g = 1$, $\deg(K_C) = 0$ and $\ell(K_C) > 0 \Longrightarrow K_C = 0$ in $Cl(C)$ so that R-R implies

$$\ell(D) - \ell(-D) = \deg(D).$$

Denote Pic$^{\circ}(C) = \ker(\deg : Cl(C) \longrightarrow \mathbb{Z})$, where $Cl(C) \cong$ Pic(C)

Theorem 7.14. $K = \overline{K}$. Fix ∞ closed point of C, then

$$j : \begin{cases} \{\text{closed point of } C\} \longrightarrow \text{Pic}^{\circ}(C) \\ \qquad\qquad x \longmapsto [x - \infty] \end{cases}$$

is a bijection.

Remark 7.15. (1) $K = \overline{K} \Longrightarrow$ we can identify { closed points of C} with $C(\overline{K}) = \mathrm{Hom}_{\mathsf{Sch}}(\mathrm{Spec}\,(\overline{K}), C)$

(2) Cor: (a): $\mathrm{Pic}^{\circ}(C)$ has the structure of closed points of a scheme

(b) $C(\overline{K})$ has a structure of an abelian group (with ∞ as neutral element)

Both of the facts generalize to curves of higher $g \geq 2$ (and in come form to higher dimensional schemes) (1) is true but corresponding scheme $Jac(C)$ "Jacobian(variety) of C" is a nonsingular projective scheme over K of dimension g.

(2) $Jac(C)$ is a "group scheme" in the sense that it has agroup structure with operation given by morphisms. there are $Jac(C) \times Jac(C) \xrightarrow{m} Jac(C)$ and $Jac(C) \xrightarrow{j} Jac(C), 0 \in Jac(C)$ s.t. the diagrams expressing associativity, neutral element, inverse, commutativity. »»»>1

Definition 7.16. C genus 1 over K ∞ closed point with reside field K [$\longleftrightarrow$ an element of $C(K)$], (C, ∞) is called an elliptic curve over K. *Ex.* $K = \mathbb{Q}$ $S = \{3x^3 + 4y^3 + 5z^3 = 0\} \subset \mathbb{P}^2_{\mathbb{Q}}$ is of genus 1, but $S(\mathbb{Q}) =$.

Proof of theorem. $j(x) =$ class of $x - \infty$

(1) Injectivity: $j(x) = j(y) \iff x - \infty \sim y - \infty \iff x \sim y$. If $x \neq y$, we saw that $x \sim y$ implies that $C \simeq \mathbb{P}^1_K$ which has genus 0, so it is not possible.

(2) Surjectivity Let $D \in \mathrm{Div}(C)$ with $\deg(C) = 0$, written $D = D_1 - D_2$ where $D_i \geq 0$. We need to prove: $(*) D \sim x - \infty$ for some x closed point of C. Write
$$D_1 = \sum n_i x_i = \sum n_i (x_i - \infty) + (\sum n_i)\infty,$$
with $n_i \geq 1$. Do the same for D_2 and take $D_1 - D_2$:
$$D = \sum_{j \in J} m_j (y_j - \infty) + 0$$
for some $m_j \in \mathbb{Z}$ y_j closed points. By induction on $Card(J)$ to prove $(*)$ it suffices to prove

(1) $\forall x_1, x_2, \exists x_3, x_1 - \infty + x_2 - \infty \sim x_3 - \infty$.

(2) $\forall x_1, \exists x_2, -(x_1 - \infty) \simeq (x_2 - \infty)$

proof of (1): Consider $E = x_1 + x_2 - \infty \in \mathrm{Div}(C)$, $\deg(E) = 1 \implies \ell(-E) = 0$

R-R $\implies \ell(E) = 1$. So there exists a function $0 \neq f \in \Gamma(C, \mathcal{L}(E))$, unique up to multiplication by $\lambda \in K^{\times}$. So $\mathrm{div}(f) + E \geq 0$.

I.e. $E = x_1 + x_2 - \infty$, f has at most a pole of order 1 at x_1, and vanishes at ∞. So $\mathrm{div}(f) = k\infty - nx_1 - mx_2 + (\text{other zeros})$ where $k \geq 1, 0 \leq n \leq 1, 0 \leq m \leq 1$. If $n = 0$, then $f \in \Gamma(C, \mathcal{L}(x_2 - \infty)) \implies \ell(x_2 - \infty) \geq 1$, $\deg(x_2 - \infty) = 0$, $\implies x_2 - \infty \sim 0 \implies C \simeq \mathbb{P}^1_K$, so $n = 1$, and similarly $m = 1$. So $0 = \deg(\mathrm{div}(f)) = -2 + k + \deg(\text{other zeros})$ i.e. $k + \deg(\text{other zeros}) = 2$. So there is a unique x_3 closed point such that the zero of f are $\infty + x_3$. This x_3 only depends on x_1 and x_2, because $\mathrm{div}(\lambda f) = \mathrm{div}(f)$ if $\lambda \in K^\times$. So $\mathrm{div}(f) = \infty + x_3 - x_1 - x_2$ so $\infty + x_3 \sim x_1 + x_2 \iff x_1 - \infty + x_2 - \infty \sim x_3 - \infty$

(2), we should investigate

$$\infty - x_1 \overset{?}{\sim} x_2 - \infty.$$

Let $E = 2\infty - x_1$ $\deg(E) = 1 \implies 0 \neq f \in \Gamma(C, \mathcal{L}(2\infty - x_1))$. $\mathrm{div}(f) + 2\infty - x_1 \geq 0$. i.e. f has at most pole of order 2 at ∞ and a zero at x. f can not have a pole of order 1 at ∞. So f has a pole of order 2 so f has two zeros with multiplicity so $\mathrm{div}(f) = x_1 + x_2 - 2\infty$ for some unique x_2

$$\implies x_1 - \infty + x_2 - \infty \sim 0$$

$$\iff \infty - x_1 \sim x_2 - \infty$$

$\square$

Now we use RR to find equation for C. (Here K is not necessarily algebraic closed) Fix again ∞ a closed point of C. (Might not exist if $K \neq \overline{K}$) Let $D_n = n\infty$ for $n \geq 1$, a divisor of degree n, so that $\ell(D_n) = n$.

$\ell(D_1) = 1$, and $0 \neq 1 \in \Gamma(C, \mathcal{L}(\infty))$ so $V(D_1) = K \cdot 1$ where $V(D_n) = \Gamma(C, \mathcal{L}(D_n))$

$\ell(D_2) = 2$; let $0 \neq f$ in $V(D_2)$ be such that $V(D_2) = K \cdot 1 + \oplus K \cdot f$. Note $\mathrm{div}(f) = (zeros) - 2\infty$

$\ell(D_3) = 3$; let $0 \neq g$ in $V(D_3)$ not in $V(D_2)$ s.t.

$$V(D_3) = K \cdot 1 \oplus K \cdot f \oplus K \cdot g.$$

$\ell(D_4) = 4$ so since $f^2 \in V(D_4)$ and not to $V(D_3)$[because it has a pole of order 4 at ∞] we have

$$V(D_4) = K \cdot 1 \oplus K \cdot f \oplus K \cdot g \oplus K f^2$$

$\ell(D_5) = 5$

$$\Longrightarrow V(D_5) = K \cdot 1 \oplus K \cdot f \oplus K \cdot g \oplus Kf^2 \oplus Kfg$$

$\ell(D_6) = 6$ since f^3 and g^2 both belong to $V(D_6)$ and not to $V(D_5)$ the set $\{1, f, g, f^2, fg, f^3, g^2\}$ is not linearly independent. So we have $\alpha_1, ...\alpha_6, \beta_6$ with $\alpha_6 \neq 0$ and $\beta_6 \neq 0$ s.t.

$$0 = \alpha_1 + \alpha_2 f + \alpha_3 g + \alpha_4 f^2 + \alpha_5 fg + \alpha_6 f^3 + \beta_6 g^2$$

in $K(C)$. So $\forall x \neq \infty$, we have $\alpha_1 + \alpha_2 f(x) + ... + \alpha_6 f(x)^3 + \beta_6 g(x)^2 = 0$. Therefore, we have a map

$$C(\overline{K}) - \{\infty\} \longrightarrow \mathbb{A}^2_K(\overline{K})$$
$$x \longmapsto (f(x), g(x))$$

so that the image is contained in the algebraic set

$$\alpha_1 + \alpha_2 X + \alpha_3 Y + \alpha_4 XY + \alpha_5 X^2 + \alpha_6 X^6 + \beta_6 Y^2 = 0.$$

One proves that this corresponds to a morphism

$$C \longrightarrow \tilde{C}$$

where $\tilde{C} \subset \mathbb{P}^2_K$ is the corresponding plane curve. This is surjective because not constant and is in fact an isomorphism.

Remark 7.17. By Careful choice of f and g, one can find such an equation with $\alpha_3 = \alpha_4 = \alpha_5 = 0$ if the characteristic of K is larger than 5. So we have an equation like

$$Y^2 = X^3 + aX + b$$

This is called the Weierstrasse equation of an elliptic curve.

Now we look at a hyperelliptic curve C/K with equation

$$ZY^2 = X^3 + aXZ^2 + bZ^3, a, b \in K.$$

with $X^3 + aX + b$ without multiple roots

C is nonsingular, projective, and has a unique point $\infty = [0 : 1 : 0]$ in $\mathbb{P}^2_K - \mathbb{A}^2_K$

Theorem 7.18. $(C/K, \infty)$ is an elliptic curve over K (i.e. has genus 1) However, every elliptic curve over K is isomorphic to one the this form if $Char(K) \geq 5$.

Example 7.19. $Y^2 = X^3 - X$ and $Y^2 + X^3 + 1$

We will check
$$\ell(D_n) - \ell(-D_n) = \deg(D_n) = n$$
for $D_n = n\infty, n \in \mathbb{Z}$. We can assume $n \geq 0$. We have $C - \{\infty\} = C \cap \mathbb{A}^2_K = \{y^2 - x^4 - ax - b = 0\} =$ Spec $(K[X,Y]/(Y^2 - X^3 - aX - b))$

So any $f \in \Gamma(C, \mathcal{L}(D_n))$ is an element of $Frac(A)$ belonging to $\Gamma(C - \{\infty\}, \mathcal{O}_C) = A$.

This means any such f is a "polynomial"
$$f = f_1(x) + Yf_2(X). f_1, f_2 \in K[X].$$
The functions $X^i, YX^i, i \geq 0$ form a basis of $A = \cup_{ngeq0}\Gamma(C, \mathcal{L}(D_n))$

Claim: X has divisor
$$\sqrt{b} + (-\sqrt{b}) - 2(\infty)$$
Y has divisor
$$(\text{zeros of } f - 3(\infty)$$
So X^i has polar divisor $2i(\infty)$, YX^i has polar divisor $3\infty + 2j\infty = (3+2j)\infty$

$X = 0 \iff Y^2 = b$ so $\sqrt{b} + (-\sqrt{b})$ so deg(polar part) $= 2$, $y = 0 \iff x^3 + ax + b = 0$ so $x_1 + x_2 + x_3$ "zeros of cubic" so deg(polar part) $= 3$

To check that $\ell(D_n) = n$ for all $n \geq 1$, it suffices to consider the pairs i, j with
$$\begin{cases} 0 \leq 2i \leq n \\ 0 \leq 3 + 2j \leq n \end{cases}$$

7.6 May 29th-A: Group law of elliptic curves.

Recall: $C/K : Y^2Z = X^3 + aXZ^2 + bZ^3 \subset \mathbb{P}^2_K$ non-singular proj: if $X^3 + aX + b$ has 3 distinct roots in $\overline{K}$

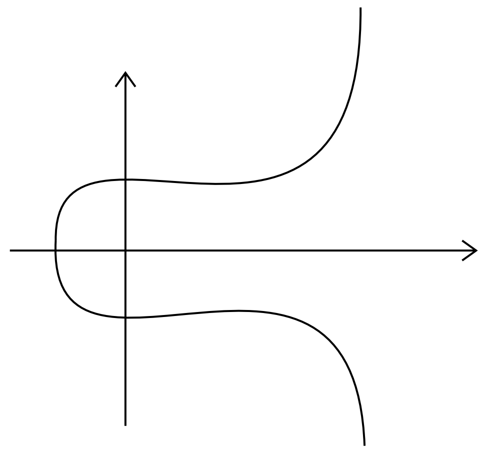
$\infty = [0:1:0]$ the only point in $C - \mathbb{A}^2_K$, $D_n = n\infty, n \in \mathbb{Z}$

$\implies \ell(D_n) - \ell(-D_n) = \deg(D_n) = n$

R-R: with $g = 1$ and $K_C = 0$,

Description of the group law on the set of closed points of C, with origin $[0:1:0]$,

$K = \overline{K}$, we can give an illustration of $C(\mathbb{R})$.



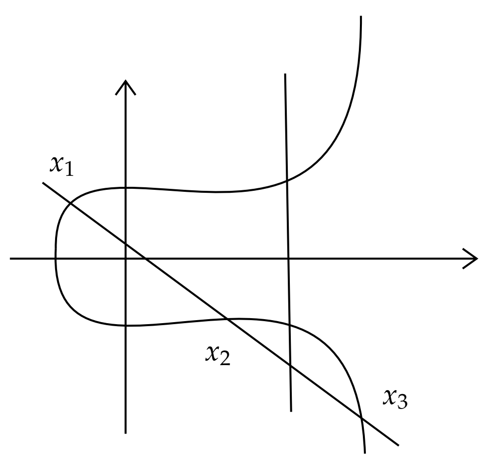
$$C(\overline{K}) \cong \{\text{closed points}\} \xrightarrow{f} \text{Pic}^\circ(C)$$
$$x \longmapsto x - \infty$$

gives a group isomorphism.

Let $f = \alpha X + \beta Y + \gamma$ as element of $K(C)$, with α or β non-zero.

$$\text{div}(f) = (\text{zeros}) - \begin{cases} 3\infty, \beta \neq 0 \\ 2\infty, \beta = 0 \end{cases}$$

so there are 3 zeros with multiplicity, or two.



These are exactly the intersection points (with multiplicity for tangents) of $C \cap \mathbb{A}^2_K \subset \mathbb{A}^2_K$ with the line $f = 0$.

Suppose $\text{div}(f) = x_1 + x_2 + x_3 - 3\infty$, $\Longrightarrow (x_1 - \infty) + (x_2 - \infty) + (x_3 - \infty) = 0$ in $\text{Pic}^\circ(C)$

$\iff x_1 + x_2 + x_3 = 0$ in {closed points}

Suppose $\beta = 0$, $\implies \mathrm{div}(f) = x_1 + x_2 - 2\infty \iff x_1 - \infty + x_2 - \infty = 0$, $\iff x_1 +_C x_2 = 0$, $\iff X_2 = -x_1$ in {Closed points}.

If $x_1 = (u_1, v_1)$ is a point on C, then $-x_1 = (u_1, -v_1)$ is the inverse.

To compute $x_1 +_C x_2$:

$(1a)$: if $x_1 \neq x_2$, draw the unique line $L \subset \mathbb{A}^2_K$ joining x_1, x_2 say $L : f = 0$.

$(1a')$ if L is not vertical, let x_3 be the third intersection point $\mathrm{div}(f) = x_1 + x_2 + x_3 - 3\infty$. Then $x_1 + x_2$ is the symmetric with x_3 with x-axis.

$(1a'')$ if L is vertical, $\implies x_1 + x_2 = 0$

$(2a)$ $x_1 = x_2$, let L be the tangent line to C at x_1,

$(2a')$ if L is not vertical, then $\mathrm{div}(f) = 2x_1 + x_3 - 3\infty$ for some $x - 3$ and $2x_1 = -x_3$

$(2a'')$ if L is vertical, then $2x_1 = 0$.

Remark 7.20.

(1) One can check directly that this geometric picture gives an Abelian group law on the set of closed points. Associativity is a famous theorem of euclidean geometry.

(2) Elliptic curve cryptography uses this group structure. Having cases leading to "timing attacks"; often models of elliptic curves are used to avoid this, where all operation are carefully designed to take the same amount of time.

(3) Elliptic curves (surprisingly) important in modern arithmetic. (Silverman, the arithmetic of elliptic curves)

8 Riemann hypothesis over finite fields

8.1 May 29th-B: The Riemann hypothesis for curves over finite fields.

History: A.Weil 1940s Great motivating problems for algebraic geometry from 1940s on, including generalizations (Weil conjectures) as motivating Grothendieck.

Classical Riemann hypothesis

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is defined over the region $Re(s) > 1$. Riemann showed this function has an analytic continuation to $\mathbb{C}$ with a simple pole at $s = 1$. This showed $\zeta(-2k) = 0$ for $k \geq 1$ integers. He conjectured all other zeros lies on the line of $Re(s) = \frac{1}{2}$.

$$\iff \sum_{p \leq x, p \text{ prime}} 1 = \int_2^x \frac{dt}{\log(t)} + \mathcal{O}(\sqrt{x}(\log(x)^2))$$

Question: Given a finite field $\mathbb{F}_q$ with q elements and $C/\mathbb{F}_q$ curve. is there an $\mathbb{F}_q$-rational point? How many are there?

(Note: if $C \hookrightarrow \mathbb{P}^n_{\mathbb{F}_q}$ then $|C(\mathbb{F}_q)| \leq |\mathbb{P}^n_{\mathbb{F}_q}(\mathbb{F}_q|)$ is finite, where the later equals

$$\frac{q^{n+1}-1}{q-1}.$$

Example 8.1. (1) Fix $k \geq 2$, $x^k + y^k = z^k$? $x, y, z \in \mathbb{F}_q$ not all zero. We will se that there are many situations if p is large enough.

(2) $a, b \in \mathbb{F}_q$,

$$\left|\{(x,y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + ax + b\}\right|?$$

We can find solution by taking any $x \in \mathbb{F}_q$ and computing $x^3 + ax + b \in \mathbb{F}_q$ and asking if it is a square or not in $\mathbb{F}_q$. If q is odd, there are

$$1 + \frac{q-1}{2} = \frac{q+1}{2}$$

squares in $\mathbb{F}_1$

$$\begin{cases} \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times \\ x \longmapsto x^2 \end{cases}$$

has kernel $\{\pm 1\}$ so $|Im| = \frac{q-1}{2}$. One guesses that there is about half chance that $x^3 + ax + b$ is a square, so altogether we might expect $\sim 2 \cdot \frac{q}{2} = q$ solutions.

Theorem 8.2. (Weil): $\mathbb{F}_q$ finite field $C/\mathbb{F}_q$ non-singular projective curve. Let $g \geq 0$ be its genus. Then

$$\big||C(\mathbb{F}_q)| - (q+1)\big| \leq 2g\sqrt{q}$$

N.B.

(a) $C = \mathbb{P}^1_{\mathbb{F}_q}, g = 0$

$$\begin{aligned} \big||C(\mathbb{F}_q)| - (q+1)\big| &\leq 0 \\ \Longrightarrow |\mathbb{P}^1(\mathbb{F}_q)| &= (q+1) \end{aligned}$$

(b) In fact, Weil proved there exist $\alpha_1, ..., \alpha_{2g}$ in $\mathbb{C}, |\alpha_i| = \sqrt{q}$ such that for any $\nu \geq 1$

$$\begin{aligned} |C(\mathbb{F}_{q^\nu})| &= q^\nu + 1 - \sum_{i=1}^{2g} \alpha_i^\nu \\ \Longrightarrow ||C(\mathbb{F}_{q^\nu})| - (q^\nu + 1)| &\leq 2g\sqrt{q}. \end{aligned}$$

In fact, from earlier work of Hasse, Artin. Schmidt...such a formula was knowen except that $|\alpha_i| = \sqrt{q}$, the α_i being zeros of a certain polynomial analogue of the zeta function. then $|\alpha_i| = \sqrt{q}$ plays the role of $Re(s) = 1/2$

(c) Higher dimensional version were conjectured by Weil (1948) proved by Dwark, Grothendieck for the counting formula. and especially R-H by Deligne. For reference see the appendix in Hartshorne or a monograph by James Milne on his webpage.

We will prove the weaker-looking (though equivalent) statement

Theorem 8.3. (Stepanov 1969 Bombieri 1973)

$C/\mathbb{F}_q$ nonsingular projective $q = p^{2\alpha}$, where p prime, $\alpha \geq 1$. If $q > (g+1)^4$, then

$$C(\mathbb{F}_q) \leq q + 1 + (2g+2)\sqrt{q}$$

Key idea

Recall $\mathbb{F}_q \subset \overline{\mathbb{F}}_q$ is the characterized as $\{x \in \overline{\mathbb{F}_q} | x^q = x\}$, which is the fixed point of the power morphism $\varphi_q : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q : x \longmapsto x^q$

Give $C/\mathbb{F}_q$, there is a Frobenius automorphism

$$\begin{aligned} \varphi_q : & C \longrightarrow C \\ & (x_i) \longmapsto (x_i^q) \end{aligned}$$

Intuitively: C is given as solution set of polynomial $f_i(x_1, ..., x_m)$ where $f_i \in \mathbb{F}_q[X_1, ..., X_m]$, then

$$f_i(X_1^q, .., X_m^q) = f_i(X_1, .., X_m)^q$$

so if $(x_1, ..., x_m)$ are solution then so of $(x_1^q, ..., x_m^q)$

Rigorously, the above gives a well-defined

$$\varphi_q : \text{Spec}(A) \longrightarrow \text{Spec}(A)$$

where $A = \mathbb{F}_q[X_1, ..., X_m]/(I)$ which satisfies the glueing.

Then

$$C(\mathbb{F}_q) \cong \{x \in C(\overline{\mathbb{F}}_q | \varphi_q(x) = x\}$$

Ex $f(x,y) = 0$, x, y is a solution in $\mathbb{F}_q^2 \iff$ it is a solution in $\overline{\mathbb{F}}_q^2$ and $(x,y)^q = (x^q, y^q) = (x,y)$

Idea of Stepanov Suppose we have

$$n \geq 1, m \geq 1 \text{ and } 0 \neq f \in \overline{\mathbb{F}}_q(C)$$

such that

1. f has at most n poles with multiplicity
2. every $x \in C(\mathbb{F}_q)$ is a zero of f with multiplicity $\geq m$. Tenn $\deg(\text{div}(f)) = 0$ implies

$$m|C(\mathbb{F}_q)| \leq n$$
$$\iff |C(\mathbb{F}_q)| \leq \frac{n}{m}.$$

Such ideas exists also in transcendence theory from Thue's time $\sim$ 1910s cf. D. Masser "Auxiliary polynomials in number theory".

Proof of Stepanov's theorem, following Bombieri. Let $x_0 \in C(\mathbb{F}_q)$ fixed. (If x_0 does not exist, the result is true). Let $D_n = nx_0 \in \text{Div}(C)$ and we will find a suitable auxiliary function f in $\Gamma(C, \mathcal{L}(D_n))$ for n large enough. Such a function certainly has poler divisor of degree $\leq n$. We will find $f = g^m$, with g vanishing at all $x \in C(\mathbb{F}_q) - \{x_0\}$

$$\implies m(|C(\mathbb{F}_q)| - 1) \leq n$$
$$|C(\mathbb{F}_q| \leq 1 + \frac{n}{m}$$

They key is to do this with n as small as posible and m as large as possible. $\square$

8.2 June 1st:

<u>Goal:</u> $C/\mathbb{F}_q$ nonsingular projective curve with genus $g \geq 0$.

$$||C(\mathbb{F}_q)| - (q+1| \leq 2g\sqrt{q}.$$

Theorem 8.4 (Stepanov)**.**

$$|C(\mathbb{F}_q)| \leq q + 1 + (2g+1)\sqrt{q}$$

if

$$\begin{cases} q > (g+1)^4 \\ q \text{ is a square} \end{cases}$$

Idea. constuct $f \in \mathbb{F}_q(C)$ non-zerp, wtih at most a pole of order $n \geq 1$ at some fixed $x_0 \in C(\mathbb{F}_q)$, and with zeros of multiplicity $\geq m$ at all $x \ni C(\mathbb{F}_q) - \{x_0\}$

$$\implies |C(\mathbb{F}_q| \leq 1 + \frac{n}{m}.$$

Fix x_0 (if $C(\mathbb{F}_q) = \emptyset$, then theorem holds)

$V_n = f(\Gamma(C \times \overline{\mathbb{F}}_q, \mathcal{L}(D_n)))$, V_n is a finite dimensional $\mathbb{F}_q$-vector space, where $D_n = nx_0$.

We search for f of the form

$$0 \neq \sum_i g_i^{p^\mu} \cdot (f_i \circ \varphi_q) = f$$

where $g_i \in V_n$, $f_i \in V_m$ for suitable n, m, μ, we want

$$\delta f = \sum_i g_i^{p^\mu} f_i = 0$$

in $\overline{\mathbb{F}}_q(C)$. If this is the case then $f(x) = 0$ for all $x \in C(\mathbb{F}_q) - \{x_0\}$ because for such an x

$$\begin{aligned} f(x) &= \sum_i g_i(x)^{p^\mu} f_i(\varphi_q(x)) \\ &= \sum_i g_i(x)^{p^\mu} f_i(x) \\ &= (\delta f)(x) = 0. \end{aligned}$$

If $p^\mu | q$ then f is also a p^μ-th power in $\overline{\mathbb{F}}_q(C)^x$:

$$\begin{aligned} f &= \sum_i g_i^{p^\mu} f_i \circ \varphi_q \\ &= \sum_i g_i^{p^\mu} \tilde{f}_i^q \\ &= \sum_i (g_i \tilde{f}_i^{q/p^\mu})^{p^\mu} = \left(\sum_i g_i \tilde{f}_i^{q/p^\mu} \right)^{p^\mu}. \end{aligned}$$

So the order of vanishing of f at $x \in C(\mathbb{F}_q) - \{x_0\}$ is $\geq p^\mu$. (Why is $f_i \circ \varphi_q$ a q-th power?)

Affine case:

$$\begin{aligned} f_i &\in \overline{\mathbb{F}}_q[X_1, .., X_m] \\ f_i \circ \varphi_q &= f_i(X_1^q, ..., X_m^q) \\ &= \sum_I \alpha_I X_1^{qi_1} \cdots X_m^{qi_m} \\ &= \left(\sum_I \beta_I X_i^{i_1} \cdots X_m^{i_m} \right)^q \end{aligned}$$

where $\beta_I^q = \alpha_I$.

$f = \sum_i g_i^{p^\mu}(f_i \circ \varphi_q)$, δf is linear in g_i, f_i but it could be that whenever we get $\delta f = 0$. we also have $f = 0$.

Define:

$$V_n^{(\mu)=\{g^{p^\mu} | g \in V_n\}}.$$

$V_n^{(\mu)}$ is an $\overline{\mathbb{F}}_q$-vector subspace of V_{np^μ}, $\dim V_n^{(\mu)} = \dim V)n = \ell(D_n)$.

$$\tilde{V}_m = \{f \circ \varphi_q | f \in V_m\}$$

is also an $\overline{\mathbb{F}}_q$-space, and

$$\begin{gathered} \tilde{V}_m \subset V_{qm}, \\ \dim(\tilde{V}_m) = \dim(V_m) = \ell(D_m). \end{gathered}$$

Lemma 8.5. Assume $m \geq 1, n \geq 1, \mu \geq 1$, and

$$np^\mu < q.$$

Then the multiplication map

$$\begin{cases} & V_n^{(\mu)} \otimes_{\overline{\mathbb{F}}_q} \tilde{V}_m \longrightarrow \overline{\mathbb{F}}_q(C) \\ g^{p^\mu} \otimes (f \circ \varphi_q) \longmapsto g^{p^\mu}(f \circ \varphi_q) & \end{cases}$$

is surjective. $\Longrightarrow$ the image has dimension $\ell(D_m)\ell(D_n)$.

Proof. Let $d = \ell(D)_m$, let $(f_1, ..., f_d)$ be a basis of V_m, chosen so that

$$V_{X_0}(f_i) < V_{X_0}(f_{i+1})$$

for $1 \leq i \leq d-1$ such a bsisi exists because $\dim(V_{i+1}/V_i) \leq 1$ since if $f_1, f_2 \in V_{i+1}$ have pole of order $i+1$, then some $\alpha f_1 + \beta f_2$ has pole of order ≤ 1.

For example, $\mathbb{P}^1$, $x_0 = \infty$ $V_\infty(f) = -\deg(f)$ for f polynomial. $f_1 = X^d$, $-d$, $f_2 = X^{d_1}$, $-d+1$

Any $f \in V_n^{(\mu)\otimes\tilde{V}_m}$ has an expansion

$$\sum_{i=1}^{d} g_i^{p^\mu} \cdot (f_i \circ \varphi_q)$$

for some $f_i \in V_m$ the tensor product is spanned by

$$\begin{aligned} &\sum_i \tilde{g}_j^{p^\mu} \otimes \left((\sum_i \alpha_{ij} f_i) \circ \varphi_q \right) \\ &= \sum_i (\sum_j \alpha_{ij} \tilde{g}_j^{p^\mu}) \otimes (f_i \circ \varphi_q) \end{aligned}$$

$$g_i --- (\sum_i \beta_{ij} \tilde{g}_j)^{p^\mu}$$

Assume

$$\sum_{i=1}^{d} g_i^{p^\mu} (f_i \circ \varphi_1) = 0,$$

we will check that $f_i = 0$ for all i, so that $f = 0$. Assume some $g_i \neq 0$, say $g_1 = \cdots = g_{k-1} = 0$ and $g_k \neq 0$ so

$$V_{x_0}(g_k^{p^\mu} f_k \circ \varphi_q) = V_{x_0}\left(\sum_{i \geq k} g_i^{p^\mu} (f_i \circ \varphi_q) \right).$$

The $LHS = p^\mu V_{x_0}(g_k) + qV_{x_0}(f_k)$, while the

$$\begin{aligned} RHS &\geq \min_{i > k} V_{x_0}(g_i^{p^\mu} f_i \circ \varphi_q) \\ &\geq -np^\mu + qV_{x_0}(f_i). \end{aligned}$$

So we have

$$p^\mu V_{x_0}(f_k) \geq -np^\mu + q(V_{x_0}(f_i) - V_{x_0}(f_k)) \geq -np^\mu + q \geq 1 \text{ by assumption}$$

where $V_{x_0}(f_i) - V_{x_0}(f_k) \geq 1$. Hence, g_k is defined at x_0 (in fact vanishes at x_0) so $g_k \in \Gamma(C \times \overline{\mathbb{F}}_q, \mathcal{O}_C)$ is constant, so equal to 0. Contradiction! ∎

Let $W_{n,m}$ be the image of this map. The lemma shows that if $np^{\mu} < q$, the map

$$\delta : \begin{cases} W_{n,m} \longrightarrow \overline{\mathbb{F}}_q(C) \\ \sum_{i=1}^{d} g_i^{p^{\mu}}(f_i \circ \varphi_q) \longmapsto \sum_{i=1}^{d} g_i^{p^{\mu}} f_i \end{cases}$$

is a well-defined $\overline{\mathbb{F}}_q$-linear map.

$$\dim \ker(\delta) = \dim(W_{n,m}) - \dim Im(\delta) = \ell(D_m)\ell(D_n) - - \dim Im(\delta).$$

But $Im_{\delta} \subset V_{np^{\mu}+m}$ so

$$\dim \ker(\delta) \geq \ell(D_n)\ell(D_m) - \ell(D_{np^{\mu}+m}).$$

Conclusion: if $n, m, \mu \geq 1$ and $p^{\mu}|q$, $np^{\mu} < q$ $\ell(D_n)\ell)D_m > \ell(D_{p^{\mu}n+m})$ then

$$|C(\mathbb{F}_q)| \leq 1 + \frac{p^{\mu}n + mq}{p^{\mu}} = 1 + n + \frac{mq}{p^{\mu}}$$

(need n, m as small as possible μ as large as possible)

R-R:

$$\ell(D)n - \ell(K_C - D_n) = n + 1 - g$$

so $\ell(D_n) \geq n + 1 - g$ $\ell(D_m) \geq m + 1 - g$. and $\ell(D_{np^{\mu}+m}) = np^{\mu} + m + 1 - g$ if $np^{\mu} + m > 2g - 2$. So we get non-trivial kernel if

$$(n + 1 - g)(m + 1 - g) > np^{\mu} + m + 1 - g$$

and

$$np^{\mu} < q.$$

Thinking that g is fixed and small, we guess that we can take $m \sim p^{\mu}$, the bound becomes $1 + n + q$. the bound becomes $1 + n + q$.

Looking at the "lower-order terms", we see that the best possible choice is $m \sim n \sim p^{\mu}$. Then the best μ is when $q = p^{2\mu}$ (so q is a square) and n just a bit smaller. More precisely, the values below work

$$q = p^{2\mu}$$

$$m = p^{\mu} + 2g = \sqrt{q} + 2g$$

$$n = \left\lfloor \frac{g}{g+1} p^{\mu} \right\rfloor + g + 1$$

and then

$$|C(\mathbb{F}_q)| \leq 1 + \frac{mq}{p^\mu} + n = 1 + q + 2gp^\mu + g + 1 + \left\lfloor \frac{g}{g+1} p^\mu \right\rfloor < 1 + q + (2g+1)\sqrt{q}$$

if $q > (g+1)^4$. How to get the lower bound ? To get a lower bound

$$|C(\mathbb{F}_q)| \geq q - C\sqrt{q}$$

for some $C \geq 1$, Stepanov(-Bambieri) use a trick from Galois theory.

Example 8.6. Suppose $C : Y^d = g(X)$, $d \geq 2$ and g is square free. Idea: find C_α auxiliary curve $\alpha \in A$, s.t.

$$\sum_{\alpha \in A} |C_\alpha(\mathbb{F}_q)| = (simple) = |A|q$$

and

$$|C_\alpha(\mathbb{F}_q| \leq q + C\sqrt{q}$$

then the sum of $C_\alpha(\mathbb{F}_q)$, $\alpha \neq 1$, cannot compensate a too small value of $|C_1(\mathbb{F}_q)|$.

Hence $A = \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^d$ is a cyclic group of order d (since $d|q-1$). Let $A \subset \mathbb{F}_q^\times$ be a set of representative of $\tilde{A}$, with $1 \in A$. $C_\alpha : \alpha Y^d = g(x)$, one can check that C_α is still of genus g. So Stepanov derived $\Longrightarrow |C_\alpha(\mathbb{F}_q)| \leq q + 1 + C\sqrt{q}$ where C is independent of α. But

$$\begin{aligned}
\sum_{\alpha \in A} |C_\alpha(\mathbb{F}_q)| &= \sum_{\alpha \in A} \sum_{x,y \in \mathbb{F}_q, y^d = \alpha^{-1} g(x)} 1 \\
&= \sum_{x \in \mathbb{F}_q} \sum_{g(x) = \alpha y^d} 1 \\
&= (\text{ at most } \deg g \text{ zeros of } g) + d(q - \#\text{ of zeros of } g) \\
&= dq + O(\deg(g)).
\end{aligned}$$

Last Step: from "

$$|C(\mathbb{F}_{q^{2\nu}})| = q^{2\nu} + O(q^\nu)$$

for all ν large enough." to

$$||C(\mathbb{F}_{q^\nu})| - (q^\nu + 1)| \leq 2g\sqrt{q^\nu}$$

We input

Theorem 8.7 (Hasse, Artin. Schmodt, 1930s). . There are $\alpha_1, ..., \alpha_{2g}$ in $\mathbb{C}$ such that

$$|C(\mathbb{F}_{q^\nu}| = q^\nu + 1 \sum_{i=1}^{2g} \alpha_i^\nu, \nu \geq 1$$

and q/α_i is one of the α_j's

and the proof uses Riemann-Roch again.

Combining the above arguments, we get $\exists C \geq 0$, $|\sum_{i=1}^{2g} \alpha_i^{2\nu}| \leq Cq^\nu$ for all $\nu \geq \nu_0$ in fact $\nu \geq 0$ by increasing C.

Lemma 8.8. Suppose $\beta_1, ..., \beta_r \in \mathbb{C}$, satisfy

$$|\sum_i^\nu \beta_i^r| \leq CB^\nu$$

for $\nu \geq 0$. Then $|\beta_i| \leq B$.

of Lemma.

$$\begin{aligned} f(z) &= \sum_{\nu \geq 0} \left(\sum_{i=1}^r \beta_i^\nu \right) z^\nu \\ &= \sum_{i=1}^r \sum_{\nu \geq 0} (\beta_i z)^\nu \\ &= \sum_{i=1}^r \frac{1}{1 - \beta_i z} \end{aligned}$$

has poles at each $\frac{1}{\beta_i}$.

Hypothesis $\implies f$ converges for $|z| < \frac{1}{|B|}$ so we have

$$\frac{1}{|\beta_i|} \geq \frac{1}{|B|}$$

$\implies |\beta_i| \leq |B|$ for all i. □

Conclusion $\beta_i = \alpha_i^2$, $B = q$

$\implies |\alpha_i^2| \leq q$, $\implies |\alpha_i| \leq \sqrt{q}$

$\implies ||C(\mathbb{F}_q| - (q+1)| \leq 2g\sqrt{q}$ but also $\left|\frac{q}{\alpha_i}\right| \leq \sqrt{q} \implies |\alpha_i| \geq \sqrt{q}$. These give us the final result

$$|\alpha_i| = \sqrt{q}$$

which is equivalent to the Riemann-Hypothesis on finite field.

Consider $C/\mathbb{F}_q$ elliptic curve
Step 1. $Z(T) = \exp\left(\sum_{\nu \geq 1} \frac{|C(\mathbb{F}_{q^\nu}|}{\nu} T^\nu\right)$. We have

$$Z(T) = \prod_{x \text{ closed point of } C} (1 - T^{\deg(x)})^{-1}$$

Step 2:

$$Z(T) = \sum_{D \geq 0 \text{ div of } C} T \deg(D) = 1 + \sum_{d \geq} T^d \sum$$