Algebraic Geometry

Ivan Tomašić

Queen Mary, University of London

LTCC 2012

Outline

What is algebraic geometry?

Intuition

Algebraic geometry is the study of geometric shapes that can be (locally/piecewise) described by polynomial equations.

Why restrict to polynomials?

Because they make sense in any field or ring, including the ones which carry no intrinsic topology.
This gives a 'universal' geometric intuition in areas where classical geometry and topology fail.
Applications in number theory: Diophantine geometry.
Even in positive characteristic.

Example

A plane curve X defined by

$$x^2 + y^2 - 1 = 0.$$

- Over $\mathbb{R}$, this defines a circle.
- Over $\mathbb{C}$, it is again a quadratic curve, even though it may be difficult to imagine (as the complex plane has real dimension 4).

k-valued points

But we can consider the solutions

$$X(k) = \{(x, y) \in k^2 : x^2 + y^2 = 1\}$$

for any field k.

- What can be said about $X(\mathbb{Q})$? It is infinite, think of Pythagorean triples, e.g. $(3/5, 4/5) \in X(\mathbb{Q})$.
- How about $X(\mathbb{F}_q)$? With certainty we can say

  $$|X(\mathbb{F}_q)| < q \cdot q = q^2,$$

  but this is a very crude bound. We intend to return to this issue (Weil conjectures/Riemann hypothesis for varieties over finite fields) at the end of the course.

Problems with non-algebraically closed fields

Example

Problem: for a plane curve Y defined by $x^2 + y^2 + 1 = 0$,

$$Y(\mathbb{R}) = \emptyset.$$

(Historical) approaches

- Thus, if we intend to pursue the line of naïve algebraic geometry and study algebraic varieties through their sets of points, we better work over an algebraically closed field.
  - Italian school: Castelnuovo, Enriques, Severi–intuitive approach, classification of algebraic surfaces;
  - American school: Chow, Weil, Zariski–gave solid algebraic foundation to above.
- For the scheme-theoretic approach, we can work over arbitrary fields/rings, and the machinery of schemes automatically performs all the necessary bookkeeping.
  - French school: Artin, Serre, Grothendieck–schemes and cohomology.

Affine space

Definition

Let k be an algebraically closed field.

- The affine n-space is
$$\mathbb{A}_k^n = \{(a_1, \ldots, a_n) : a_i \in k\}.$$
- Let
$$A = k[x_1, \ldots, x_n]$$
be the polynomial ring in n variables over k.
- Think of an $f \in A$ as a function
$$f : \mathbb{A}_k^n \to k;$$
for $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$, we let $f(P) = f(a_1, \ldots, a_n)$.

Vanishing set

Definition

- For $f \in A$, we let
$$V(f) = \{P \in \mathbb{A}^n : f(P) = 0\}.$$
- Let
$$D(f) = \mathbb{A}^n \setminus V(f).$$
- More generally, for any subset $E \subseteq A$,
$$V(E) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in E\} = \bigcap_{f \in E} V(f).$$

Properties of V

Proposition (✎)

- $V(0) = \mathbb{A}^n$, $V(1) = \emptyset$;
- $E \subseteq E'$ *implies* $V(E) \supseteq V(E')$;
- *for a family* $(E_\lambda)_\lambda$, $V(\cup_\lambda E_\lambda) = V(\sum_\lambda E_\lambda) = \cap_\lambda V(E_\lambda)$;
- $V(EE') = V(E) \cup V(E')$;
- $V(E) = V(\sqrt{\langle E \rangle})$, *where* $\langle E \rangle$ *is an ideal of* A *generated by* E *and* $\sqrt{\cdot}$ *denotes the radical of an ideal,* $\sqrt{I} = \{a \in A : a^n \in I \text{ for some } n \in \mathbb{N}\}$.

This shows that sets of the form $V(E)$ for $E \subseteq A$ (called algebraic sets) are closed sets of a topology on $\mathbb{A}^n$, which we call the Zariski topology.
Note: $D(f)$ are basic open.

Example

Algebraic subsets of $\mathbb{A}^1$ are just finite sets.

Thus any two open subsets intersect, far from being Hausdorff.

Proof.

$A = k[x]$ is a principal ideal domain, so every ideal $\mathfrak{a}$ in A is principal, $\mathfrak{a} = (f)$, for $f \in A$. Since k is ACF, f splits in k, i.e.

$$f(x) = c(x - a_1) \cdots (x - a_n).$$

Thus $V(\mathfrak{a}) = V(f) = \{a_1, \ldots, a_n\}$. □

Affine varieties

Definition

An affine algebraic variety is a closed subset of $\mathbb{A}^n$, together with the induced Zariski topology.

Associated Ideal

Definition

Let $Y \subseteq \mathbb{A}^n$ be an arbitrary set (not necessarily closed). The ideal of Y in A is

$$I(Y) = \{f \in A : f(P) = 0 \text{ for all } P \in Y\}.$$

Proposition

1. *$Y \subseteq Y'$ implies $I(Y) \supseteq I(Y')$;*
2. *$I(\cup_\lambda Y_\lambda) = \cap_\lambda I(Y_\lambda)$;*
3. *for any $Y \subseteq \mathbb{A}^n$, $V(I(Y)) = \overline{Y}$, the Zariski closure of Y in $\mathbb{A}^n$;*
4. *for any $E \subseteq A$, $I(V(E)) = \sqrt{\langle E \rangle}$.*

Proof.

3. Clearly, $V(I(Y))$ is closed and contains Y. Conversely, if $V(E) \supseteq Y$, then, for every $f \in E$, $f(y) = 0$ for every $y \in Y$, so $f \in I(Y)$, thus $E \subseteq I(Y)$ and $V(E) \supseteq V(I(Y))$.

✎4. Is commonly known as Hilbert's Nullstellensatz. Let us write $\mathfrak{a} = \langle E \rangle$. It is clear that $\sqrt{\mathfrak{a}} \subseteq I(V(\mathfrak{a}))$. For the converse inclusion, we shall assume:

the weak Nullstellensatz (in $(n+1)$ variables):

for a proper ideal J in $k[x_0, \ldots, x_n]$, we have $V(J) \neq 0$ (it is crucial here that k is algebraically closed).

Suppose $f \in I(V(\mathfrak{a}))$. The ideal $J = \langle 1 - x_0 f \rangle + \mathfrak{a}$ in $k[x_0, \ldots, k_n]$ has no zero in k^{n+1} so we conclude $J = \langle 1 \rangle$, i.e. $1 \in J$. It follows (by substituting $1/f$ for x_0 and clearing denominators) that $f^n \in \mathfrak{a}$ for some n.
For a complete proof see Atiyah-Macdonald. □

Quasi-compactness

Corollary

$D(f)$ is quasi-compact. (not Hausdorff)

Proof.

If $\cup_i D(f_i) = D(f)$, then $V(f) = \cap_i V(f_i) = V(\{f_i : i \in I\})$, so $f \in \sqrt{\{f_i : i \in I\}}$, so there is a finite $I_0 \subseteq I$ with $f \in \sqrt{\{f_i : i \in I_0\}}$. □

Corollary

There is a 1-1 inclusion-reversing correspondence

$$\begin{aligned} Y &\longmapsto I(Y) \\ V(\mathfrak{a}) &\longleftarrow\!\!\mapsfrom \mathfrak{a} \end{aligned}$$

between algebraic sets and radical ideals.

Given a point $P = (a_1, \dots, a_n) \in \mathbb{A}^n$, the ideal $\mathfrak{m}_P = I(P)$ is maximal (because the set $\{P\}$ is minimal), and $\mathfrak{m}_P = (x_1 - a_1, \dots, x_n - a_n)$. Weak Nullstellensatz tells us that every maximal ideal is of this form.
Thus,

$$I(V(\mathfrak{a})) = \bigcap_{P \in V(\mathfrak{a})} I(P) = \bigcap_{P \in V(\mathfrak{a})} \mathfrak{m}_P = \bigcap_{\substack{\mathfrak{m} \supseteq \mathfrak{a} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}.$$

On the other hand, it is known in commutative algebra that

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \supseteq \mathfrak{a} \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}$$

Thus, Nullstellensatz in fact claims that the two intersections coincide, i.e., that A is a Jacobson ring.

Affine coordinate ring

Definition

If Y is an affine variety, its affine coordinate ring is $\mathscr{O}(Y) = A/I(Y)$.

$\mathscr{O}(Y)$ should be thought of as the ring of polynomial functions $Y \to k$. Indeed, two polynomials $f, f' \in A$ define the same function on Y iff $f - f' \in I(Y)$.

Remark

- *If Y is an affine variety, $\mathscr{O}(Y)$ is a finitely generated k-algebra.*
- *Conversely, any finitely generated reduced (no nilpotent elements) k-algebra is a coordinate ring of an irreducible affine variety.*

Indeed, suppose B is generated by $b_1, \ldots, b_n$ as a k-algebra, and define a morphism $A = k[x_1, \ldots, x_n] \to B$ by $x_i \mapsto b_i$. Since B is reduced, the kernel is a radical ideal $\mathfrak{a}$, so $B = \mathscr{O}(V(\mathfrak{a}))$.

Maximal spectrum

Remark

Let Specm(B) *denote the set of all maximal ideals of* B*. Then we have 1-1 correspondences between the following sets:*

1. *(points of)* Y*;*
2. $Y(k) := \mathrm{Hom}_k(\mathscr{O}(Y), k)$*;*
3. Specm($\mathscr{O}(Y)$)*;*
4. *maximal ideals in* A *containing* $I(Y)$*.*

Let $P \in Y$, $P = (a_1, \ldots, a_n)$. We know $I(P) \supseteq I(Y)$, so the morphism $a : \mathscr{O}(Y) = A/I(Y) \to k$, $x_i + I(Y) \mapsto a_i$ is well-defined. Since the range is a field, $\mathfrak{m}_P = \ker(a)$ is maximal in $\mathscr{O}(Y)$, and its preimage in A is exactly $I(P) = \{f \in A : f(P) = 0\}$.

Irreducibility

Definition

A topological space X is irreducible if it cannot be written as the union $X = X_1 \cup X_2$ of two proper closed subsets.

Proposition

An algebraic variety is irreducible iff its ideal is prime iff $\mathscr{O}(Y)$ is a domain.

Proof.

Suppose Y is irreducible, and let $fg \in I(Y)$. Then

$$Y \subseteq V(fg) = V(f) \cup V(g) = (Y \cap V(f)) \cup (Y \cap V(g)),$$

both being closed subsets of Y. Since Y is irreducible, we have $Y = Y \cap V(f)$ or $Y = Y \cap V(g)$, i.e., $Y \subseteq V(f)$ or $Y \subseteq V(g)$, i.e., $f \in I(Y)$ or $g \in I(Y)$. Thus $I(Y)$ is prime.

Conversely, let $\mathfrak{p}$ be a prime ideal and suppose $V(\mathfrak{p}) = Y_1 \cup Y_2$. Then $\mathfrak{p} = I(Y_1) \cap I(Y_2) \supseteq I(Y_1)I(Y_2)$, so we have $\mathfrak{p} = I(Y_1)$ or $\mathfrak{p} = I(Y_2)$, i.e., $Y_1 = V(\mathfrak{p})$ or $Y_2 = V(\mathfrak{p})$, and we conclude that $V(\mathfrak{p})$ is irreducible. □

Examples

- $\mathbb{A}^n$ is irreducible; $\mathbb{A}^n = V(0)$ and 0 is a prime ideal since A is a domain.
- if $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$, then $\{P\} = V(\mathfrak{m}_P)$, $\mathfrak{m}_P = (x_1 - a_1, \ldots, x_n - a_n)$ is a max ideal, hence prime, so $\{P\}$ is irreducible.
- Let $f \in A = k[x, y]$ be an irreducible polynomial. Then $V(f)$ is an irreducible variety (affine curve); (f) is prime since A is an unique factorisation domain.
- $V(x_1 x_2) = V(x_1) \cup V(x_2)$ is connected but not irreducible.

Noetherian topological spaces

Definition

A topological space X is noetherian, if it has the descending chain condition (or DCC) on closed subsets: any descending sequence $Y_1 \supseteq Y_2 \supseteq \cdots$ of closed subsets eventually stabilises, i.e., there is an $r \in \mathbb{N}$ such that $Y_r = Y_{r+i}$ for all $i \in \mathbb{N}$.

Proposition (✎)

In a noetherian topological space X, every nonempty closed subset Y can be expressed as an irredundant finite union

$$Y = Y_1 \cup \cdots \cup Y_n$$

of irreducible closed subsets Y_i (irredundant means $Y_i \not\subseteq Y_j$ for $i \neq j$).The Y_i are uniquely determined, and we call them the irreducible components of Y.

Noetherian rings

Definition

A ring A is noetherian if it satisfies the following three equivalent conditions:

1. A has the ascending chain condition on ideals: every ascending chain $I_1 \subseteq I_2 \subseteq \cdots$ of ideals is stationary (eventually stabilises);
2. every non-empty set of ideals in A has a maximal element;
3. every ideal in A is finitely generated.

Hilbert's Basis Theorem

Theorem (Hilbert's Basis Theorem)

If A is noetherian, then the polynomial ring $A[x_1, \ldots, x_n]$ is noetherian.

Corollary

If A is noetherian and B is finitely generated A-algebra, then B is also noetherian.

Remark

This means that any algebraic variety $Y \subseteq \mathbb{A}^n$ is in fact a set of solutions of a finite system of polynomial equations:

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

Irreducible components

Corollary

Every affine algebraic variety is a noetherian topological space and can be expressed uniquely as an irredundant union of irreducible varieties.

Proof.

$\mathscr{O}(Y)$ is a finitely generated k-algebra and a field k is trivially noetherian, so $\mathscr{O}(Y)$ is a noetherian ring. A descending chain of closed subsets $Y_1 \supseteq Y_2 \supseteq \cdots$ in Y gives rise to an ascending chain of ideals $I(Y_1) \subseteq I(Y_2) \subseteq \cdots$ in $\mathscr{O}(Y)$, which must be stationary. Thus the original chain of closed subsets must be stationary too. □

Finding/computing irreducible components in a concrete case is a non-trivial task, which can be made efficient by the use of Gröbner bases.

Example (Exercise✎)

Let $Y = V(x^2 - yz, xz - x) \subseteq \mathbb{A}^3$. Show that Y is a union of 3 irreducible components and find their prime ideals.

Dimension

Definition

- The dimension of a topological space X is the supremum of all n such that there exists a chain

$$Z_0 \subset Z_1 \subset \cdots \subset Z_n$$

  of distinct irreducible closed subsets of X.
- The dimension of an affine variety is the dimension of its underlying topological space.

not every noetherian space has finite dimension.

Definition

- In a ring A, the height of a prime ideal $\mathfrak{p}$ is the supremum of all n such that there exists a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ of distinct prime ideals.
- The Krull dimension of A is the supremum of the heights of all the prime ideals.

Fact

Let B be a finitely generated k-algebra which is a domain. Then

1. $\dim(B) = \text{tr.deg}(\mathbf{k}(B)/k)$, *where* $\mathbf{k}(B)$ *is the fraction field of* B*;*
2. *for any prime ideal* $\mathfrak{p}$ *of* B*,*

$$\text{height}(\mathfrak{p}) + \dim(B/\mathfrak{p}) = \dim(B).$$

Topological and algebraic dimension

Proposition

For an affine variety Y,

$$\dim(Y) = \dim(\mathscr{O}(Y)).$$

By the previous Fact, the latter equals the number of algebraically independent coordinate functions, and we deduce:

Proposition

$$\dim(\mathbb{A}^n) = n.$$

Proposition (✎)

Let Y be an affine variety.

1. *If Y is irreducible and Z is a proper closed subset of Y, then* $\dim(Z) < \dim(Y)$.
2. *If $f \in \mathscr{O}(Y)$ is not a zero divisor nor a unit, then* $\dim(V(f) \cap Y) = \dim(Y) - 1$

Examples

1. Let $X, Y \subseteq \mathbb{A}^2$ be two irreducible plane curves. Then $\dim(X \cap Y) < \dim(X) = 1$, so $X \cap Y$ is of dimension 0 and thus it is a finite set.
2. A classification of irreducible closed subsets of $\mathbb{A}^2$.
   - If $\dim(Y) = 2 = \dim(\mathbb{A}^2)$, then by Prop, $Y = \mathbb{A}^2$;
   - If $\dim(Y) = 1$, then $Y \neq \mathbb{A}^2$ so $0 \neq I(Y)$ is prime and thus contains a non-zero irreducible polynomial f. Since $Y \supseteq V(f)$ and $\dim(V(f)) = 1$, it must be $Y = V(f)$.
   - If $\dim(Y) = 0$, then Y is a point.

Example (The twisted cubic curve)

Let $Y \subseteq \mathbb{A}^3$ be the set $\{t, t^2, t^3) : t \in k\}$. Show that it is an affine variety of dimension 1 (i.e., an affine curve).
Hint: Find the generators of $I(Y)$ and show that $\mathscr{O}(Y)$ is isomorphic to a polynomial ring in one variable over k.

Morphisms of affine varieties

Definition

Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be two affine varieties. A morphism

$$\varphi : X \to Y$$

is a map such that there exist polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ with

$$\varphi(P) = (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)),$$

for every $P = (a_1, \ldots, a_n) \in X$.

Remark (✎)

Morphisms are continuous in Zariski topology.

Morphisms vs algebra morphisms

A morphism $\varphi : X \to Y$ defines a k-homomorphism

$$\tilde{\varphi} : \mathscr{O}(Y) \to \mathscr{O}(X), \quad \tilde{\varphi}(g) = g \circ \varphi,$$

when $g \in \mathscr{O}(Y)$ is identified with a function $Y \to k$.

A k-homomorphism $\psi : \mathscr{O}(Y) \to \mathscr{O}(X)$ defines a morphism

$$^a\psi : X \to Y.$$

Identify X with $X(k) = \mathrm{Hom}(\mathscr{O}(X), k)$ and Y by $Y(k)$. Then

$$^a\psi(\bar{x}) = \bar{x} \circ \psi.$$

Proposition $\quad ^a(\tilde{\varphi}) = \varphi \quad$ *and* $\quad (^a\psi)\tilde{} = \psi.$

Duality between algebra and geometry

Corollary

The functor

$$X \longmapsto \mathscr{O}(X)$$

defines an arrow-reversing equivalence of categories (✎) between the category of affine varieties over k and the category of finitely generated reduced k-algebras.

- The 'inverse' functor is $A \mapsto \mathrm{Specm}(A)$. For $\psi : B \to A$, $\mathrm{Specm}(\psi) = {}^a\psi : \mathrm{Specm}(A) \to \mathrm{Specm}(B)$, ${}^a\psi(\mathfrak{m}) = \psi^{-1}(\mathfrak{m})$, $\mathfrak{m}$ a max ideal in A.
- This means that X and Y are isomorphic iff $\mathscr{O}(X)$ and $\mathscr{O}(Y)$ are isomorphic as k-algebras.

A translation mechanism

That means: every time you see a morphism

$$X \longrightarrow Y,$$

you should be thinking that this comes from a morphism

$$\mathscr{O}(X) \longleftarrow \mathscr{O}(Y),$$

and vice-versa, every time you see a morphism

$$A \longleftarrow B,$$

you should be thinking of a morphism

$$\mathrm{Specm}(A) \longrightarrow \mathrm{Specm}(B).$$

Methodology of algebraic geometry

- In physics, one often studies a system X by considering certain 'observable' functions on X.
- In algebraic geometry, all of the relevant information about an affine variety X is contained in its coordinate ring $\mathscr{O}(X)$, and we can study the geometric properties of X by using the tools of commutative algebra on $\mathscr{O}(X)$.

Examples (✎)

1. Let $X = \mathbb{A}^1$ and $Y = V(x^3 - y^2) \subseteq \mathbb{A}^2$, and let

$$\varphi : X \to Y, \quad \text{defined by} \quad t \mapsto (t^2, t^3).$$

Then φ is a morphism which is bijective and bicontinuous (a homeomorphism in Zariski topology), but φ is not an isomorphism.

2. Let $char(k) = p > 0$. The Frobenius morphism

$$\varphi : \mathbb{A}^1 \to \mathbb{A}^1, \quad t \mapsto t^p$$

is a bijective and bicontinuous morphism, but it is not an isomorphism.

Sheaves

Definition

Let X be a topological space. A presheaf $\mathscr{F}$ of abelian groups on X consists of the data:

- for every open set $U \subseteq X$, an abelian group $\mathscr{F}(U)$;
- for every inclusion $V \overset{i}{\hookrightarrow} U$ of open subsets of X, a morphism of abelian groups $\rho_{UV} = \mathscr{F}(i) : \mathscr{F}(U) \to \mathscr{F}(V)$,

such that

1. $\rho_{UU} = \mathscr{F}(id : U \to U) = id : \mathscr{F}(U) \to \mathscr{F}(U)$;
2. if $W \overset{j}{\hookrightarrow} V \overset{i}{\hookrightarrow} U$, then $\mathscr{F}(i \circ j) = \mathscr{F}(j) \circ \mathscr{F}(i)$, i.e., $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.

Presheaves as functors

The axioms above, in categorical terms, state that a presheaf $\mathscr{F}$ on a topological space X, is nothing other than a contravariant functor from the category $\mathcal{Top}(X)$ of open subsets with inclusions to the category of abelian groups:

$$\mathscr{F} : \mathcal{Top}(X)^{op} \to \mathcal{Ab}.$$

Sections jargon and stalks

For $s \in \mathscr{F}(U)$ and $V \subseteq U$, write $s \restriction_V = \rho_{UV}(s)$ and we refer to ρ_{UV} as restrictions. Write (2) above as

$$s \restriction_W = (s \restriction_V) \restriction_W .$$

Elements of $\mathscr{F}(U)$ are sometimes called sections of $\mathscr{F}$ over U, and we sometimes write $\mathscr{F}(U) = \Gamma(U, \mathscr{F})$, where Γ symbolises 'taking sections'.

Definition

If $P \in X$, the stalk $\mathscr{F}_P$ of $\mathscr{F}$ at P is the direct limit of the groups $\mathscr{F}(U)$, where U ranges over the open neighbourhoods of P (via the restriction maps).

Stalks and germs of sections

Define the relation $\sim$ on pairs (U, s), where U is an open nhood of P, and $s \in \mathscr{F}(U)$:

$$(U_1, s_1) \sim (U_2, s_2)$$

if there is an open nhood W of P with $W \subseteq U_1 \cap U_2$ such that

$$s_1 \restriction_W = s_2 \restriction_W .$$

Then $\mathscr{F}_P$ equals the set of $\sim$-equivalence classes, which can be thought of as 'germs' of sections at P.

Sheaves

Definition

A presheaf $\mathscr{F}$ on a topological space X is a sheaf provided:

3. if $\{U_i\}$ is an open covering of U, and $s, t \in \mathscr{F}(U)$ are such that $s \restriction U_i = t \restriction U_i$ for all i, then $s = t$.
4. if $\{U_i\}$ is an open covering of U, and $s_i \in \mathscr{F}(U_i)$ are such that for each i, j, $s_i \restriction_{U_i \cap U_j} = s_j \restriction_{U_i \cap U_j}$, then there exists an $s \in \mathscr{F}(U)$ such that $s \restriction U_i = s_i$. (note that such an s is unique by 3.)

'Unique glueing property'.

Examples

- Sheaf $\mathscr{F}$ of continuous $\mathbb{R}$-valued functions on a topological space X:
  - $\mathscr{F}(U)$ is the set of continuous functions $U \to \mathbb{R}$,
  - for $V \subseteq U$, let $\rho_{UV} : \mathscr{F}(U) \to \mathscr{F}(V)$, $\rho_{UV}(f) = f \restriction_V$.
- Sheaf of differentiable functions on a differentiable manifold;
- Sheaf of holomorphic functions on a complex manifold.
- Constant presheaf: fix an abelian group Λ and let $\mathscr{F}(U) = \Lambda$ for all U. This is not a sheaf (✎), its associated sheaf satisfies

  $$\mathscr{F}^+(U) = \Lambda^{\pi_0(U)},$$

  where $\pi_0(U)$ is the number of connected components of U. (provided X is locally connected)

Sheaf morphisms

Definition

Let $\mathscr{F}$ and $\mathscr{G}$ be presheaves of abelian groups on X.
A **morphism** $\varphi : \mathscr{F} \to \mathscr{G}$ consists of the following data:

- For each U open in X, we have a morphism

$$\varphi(U) : \mathscr{F}(U) \to \mathscr{G}(U).$$

- For each inclusion $V \overset{i}{\hookrightarrow} U$, we have a diagram

$$\begin{array}{ccc} \mathscr{F}(U) & \xrightarrow{\varphi(U)} & \mathscr{G}(U) \\ {\scriptstyle \mathscr{F}(i)}\downarrow & & \downarrow{\scriptstyle \mathscr{G}(i)} \\ \mathscr{F}(V) & \xrightarrow{\varphi(V)} & \mathscr{G}(V) \end{array}$$

Sheaf morphisms as natural transformations

In categorical terms, if $\mathscr{F}$ and $\mathscr{G}$ are considered as functors $\mathcal{Top}(X)^{op} \to \mathcal{Ab}$, a morphism

$$\varphi : \mathscr{F} \to \mathscr{G}$$

is nothing other than a natural transformation (✐) between these functors.

Interlude on localisation

Definition

Let A be a commutative ring with 1, and let $S \ni 1$ be a multiplicatively closed subset of A. Define a relation $\equiv$ on $A \times S$:

$$(a_1, s_1) \equiv (a_2, s_2) \quad \text{if} \quad (a_1 s_2 - a_2 s_1)s = 0 \quad \text{for some} \quad s \in S.$$

Then $\equiv$ is an equivalence relation and the ring of fractions $S^{-1}A = A \times S/\equiv$ has the following structure (write a/s for the class of (a, s)):

$$(a_1/s_1) + (a_2/s_2) = (a_1 s_2 + a_2 s_1)/s_1 s_2,$$
$$(a_1/s_1)(a_2/s_2) = (a_1 a_2/s_1 s_2).$$

We have a morphism $A \to S^{-1}A$, $a \mapsto a/1$.

Interlude on localisation

Examples

- If A is a domain, $S = A \setminus \{0\}$, then $S^{-1}A$ is the ring of fractions of A.
- If $\mathfrak{p}$ is a prime ideal in A, then $S = A \setminus \mathfrak{p}$ is multiplicative and $S^{-1}A$ is denoted $A_{\mathfrak{p}}$ and called the localisation of A at $\mathfrak{p}$. NB ✐ $A_{\mathfrak{p}}$ is indeed a local ring, i.e., it has a unique maximal ideal.
- Let $f \in A$, $S = \{f^n : n \geq 0\}$. Write $A_f = S^{-1}A$.
- $S^{-1}A = 0$ iff $0 \in S$.

Regular functions

Remark

Let X be an affine variety and $g, h \in \mathscr{O}(X)$. Then

$$P \mapsto \frac{g(P)}{h(P)}$$

is a well-defined function $D(h) \to k$.

We would like to consider functions defined on open subsets of X which are locally of this form.

Regular functions

Definition

Let U be an open subset of an affine variety X.

- A function $f : U \to k$ is regular if for every $P \in U$, there exist $g, h \in \mathscr{O}(X)$ with $h(P) \neq 0$, and a neighbourhood V of P such that the functions f and g/h agree on V.
- The set of all regular functions on U is denoted $\mathscr{O}_X(U)$.

Proposition (✎)

The assignment $U \mapsto \mathscr{O}_X(U)$ defines a sheaf of k-algebras on X.

It is called the structure sheaf of X.

Structure sheaf

Proposition

Let X be an affine variety and let $A = \mathscr{O}(X)$ be its coordinate ring. Then:

- *For any $P \in X$, the stalk*

  $$\mathscr{O}_{X,P} \simeq A_{\mathfrak{m}_P},$$

  where the maximal ideal $\mathfrak{m}_P = \{f \in A : f(P) = 0\}$ is the image of $I(P)$ in A.
- *For any $f \in A$,*

  $$\mathscr{O}_X(D(f)) \simeq A_f.$$

- *In particular,*

  $$\mathscr{O}_X(X) = A.$$

  (so our notation for the coordinate ring is justified)

Spectrum of a ring

Let A be a commutative ring with 1.

Definition

Spec(A) is the set of all prime ideals in A.

Our goal is to turn $X = \mathrm{Spec}(A)$ into a topological space and equip it with a sheaf of rings, i.e., make it into a ringed space.

Notation:

- write $x \in X$ for a point, and $\mathfrak{j}_x$ for the corresponding prime ideal in A;
- $A_x = A_{\mathfrak{j}_x}$, the local ring at x;
- $\mathfrak{m}_x = \mathfrak{j}_x A_{\mathfrak{j}_x}$, the maximal ideal of A_x;
- $\mathbf{k}(x) = A_x/\mathfrak{m}_x$, the residue field at x, naturally isomorphic to $A/\mathfrak{j}_x$;
- for $f \in A$, write $f(x)$ for the class of f mod $\mathfrak{j}_x$ in $\mathbf{k}(x)$. Then '$f(x) = 0$' iff $f \in \mathfrak{j}_x$.

Examples

1. For a field F, $\mathrm{Spec}(F) = \{0\}$, $\mathbf{k}(0) = F$.
2. Let $\mathbb{Z}_p$ be the ring of p-adic integers. $\mathrm{Spec}(\mathbb{Z}_p) = \{0, (p)\}$, and $\mathbf{k}(0) = \mathbb{Q}_p$, $\mathbf{k}((p)) = \mathbb{F}_p$. Generalises to an arbitrary DVR. ✎
3. $\mathrm{Spec}(Z) = \{0\} \cup \{(p) : p \text{ prime }\}$. $\mathbf{k}(0) = \mathbb{Q}$, $\mathbf{k}((p)) = \mathbb{F}_p$. For $f \in \mathbb{Z}$, $f(0) = f/1 \in \mathbb{Q}$, and $f(p) = f \mod p \in \mathbb{F}_p$.
4. For an algebraically closed field k, let $A = k[x, y]$. Then by ◂ Classification of irred subsets of $\mathbb{A}^2$

$$\begin{aligned}\mathrm{Spec}(A) =& \{0\} \cup \{(x-a, y-b) : a, b \in k\} \\ & \cup \{(g) : g \in A \text{ irreducible }\}.\end{aligned}$$

$\mathbf{k}(0) = k(x, y)$, $\mathbf{k}((x-a, y-b)) = k$, $\mathbf{k}((g))$ is the fraction field of the domain $A/(g)$. For $f \in A$, $f(0) = f/1 \in k(x, y)$, $f((x-a, x-b)) = f(a, b) \in k$, $f((g)) = (f + (g))/1 \in \mathbf{k}(g)$.

Spectral topology

Definition

For $f \in A$, let

$$V(f) = \{x \in X : f \in \mathfrak{j}_x\}, \qquad \text{i.e., the set of } x \text{ with } f(x) = 0;$$
$$D(f) = X \setminus V(f).$$

For $E \subseteq A$,

$$V(E) = \bigcap_{f \in E} V(f) = \{x \in X : E \subseteq \mathfrak{j}_x\}.$$

The operation V has expected properties: ◂ Jump to properties of V
Thus, the sets $V(E)$ are closed sets for the Zariski topology on X.

Definition

For an arbitrary subset $Y \subseteq X$, the ideal of Y is

$$\jmath(Y) = \bigcap_{x \in Y} \jmath_x \quad \text{i.e., the set of } f \in A \text{ with } f(x) = 0 \text{ for } x \in Y;$$

Remark

Trivially:

$$\sqrt{E} = \bigcap_{x \in V(E)} \jmath_x .$$

The operation $\jmath$ has the expected properties: Jump to properties of I
and here the proof is trivial, no need for Nullstellensatz.

Direct image sheaf

Definition

Let $\varphi : X \to Y$ be a continuous map of topological spaces and let $\mathscr{F}$ be a presheaf on X. The direct image $\varphi_*\mathscr{F}$ is a presheaf on Y defined by

$$\varphi_*\mathscr{F}(U) = \mathscr{F}(\varphi^{-1}U).$$

Lemma (✎)

If $\mathscr{F}$ is a sheaf, so is $\varphi_*\mathscr{F}$.

Ringed spaces

Definition

- A ringed space $(X, \mathscr{O}_X)$ consists of a topological space X and a sheaf of rings $\mathscr{O}_X$ on X, called the structure sheaf.
- A locally ringed space is a ringed space $(X, \mathscr{O}_X)$ such that every stalk $\mathscr{O}_{X,x}$ is a local ring, $x \in X$.
- A morphism of ringed spaces $(X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ is a pair (φ, θ), where $\varphi : X \to Y$ is a continuous map, and

  $$\theta : \mathscr{O}_Y \to \varphi_* \mathscr{O}_X$$

  is a map of structure sheaves.
- (φ, θ) is a morphism of locally ringed spaces, if, additionally, each induced map of stalks

  $$\theta_x^\sharp : \mathscr{O}_{Y,\varphi(x)} \to \mathscr{O}_{X,x}$$

  is a local homomorphism of local rings.

Spectrum as a locally ringed space

Lemma

There exists a unique sheaf $\mathscr{O}_X$ *on* $X = \operatorname{Spec}(A)$ *satisfying*

$$\mathscr{O}_X(D(f)) \simeq A_f \qquad \textit{for } f \in A.$$

Its stalks are

$$\mathscr{O}_{X,x} \simeq A_x \qquad (= A_{\mathfrak{j}_x}).$$

Definition

By $\operatorname{Spec}(A)$ we shall mean the locally ringed space

$$(\operatorname{Spec}(A), \mathscr{O}_{\operatorname{Spec}(A)}).$$

Schemes

Definition

- An affine scheme is a ringed space $(X, \mathscr{O}_X)$ which is isomorphic to $\mathrm{Spec}(A)$ for some ring A.
- A scheme is a ringed space $(X, \mathscr{O}_X)$ such that every point has an open affine neighbourhood U (i.e., $(U, \mathscr{O}_X \restriction U)$ is an affine scheme).
- A morphism $(X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ is just a morphism of locally ringed spaces.

Ring homomorphisms induce morphisms of affine schemes

Definition

A ring homomorphism $\varphi : B \to A$ gives rise to a morphism of affine schemes $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(B)$:

$$({}^a\varphi, \tilde{\varphi}) : (\mathrm{Spec}(A), \mathscr{O}_{\mathrm{Spec}(A)}) \to (\mathrm{Spec}(B), \mathscr{O}_{\mathrm{Spec}(B)}),$$

where

- ${}^a\varphi(x) = y \quad \text{iff} \quad \mathfrak{j}_y = \varphi^{-1}(\mathfrak{j}_x); \qquad (\text{i.e., } {}^a\varphi(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p}))$
- $\tilde{\varphi} : \mathscr{O}_Y \to {}^a\varphi_* \mathscr{O}_X$ is characterised by (for $g \in B$):

$$\begin{array}{ccccc} \mathscr{O}_Y(D(g)) & \xrightarrow{\tilde{\varphi}(D(g))} & \mathscr{O}_X({}^a\varphi^{-1} D(g)) & = & \mathscr{O}_X(D(\varphi(g))) \\ \| & & & & \| \\ B_g & & \xrightarrow{\quad b/g^n \;\longmapsto\; \varphi(b)/\varphi(g)^n \quad} & & A_{\varphi(g)} \end{array}$$

A remarkable equivalence of categories

It turns out that every morphism of affine schemes is induced by a ring homomorphism.

Proposition

There is a canonical isomorphism

$$\mathrm{Hom}(\mathrm{Spec}(A), \mathrm{Spec}(B)) \simeq \mathrm{Hom}(B, A).$$

Corollary

The functors

$$A \longmapsto \mathrm{Spec}(A)$$
$$\mathscr{O}_X(X) \longleftarrow X$$

define an arrow-reversing equivalence of categories between the category of commutative rings and the category of affine schemes.

Adjointness of Spec and global sections

More generally:

Proposition

Let X be an arbitrary scheme, and let A be a ring. There is a canonical isomorphism

$$\mathrm{Hom}(X, \mathrm{Spec}(A)) \simeq \mathrm{Hom}(A, \Gamma(X)),$$

where $\Gamma(X) = \mathscr{O}_X(X)$ is the 'global sections' functor.

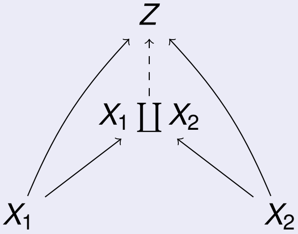
Sum of schemes

Proposition

Let X_1 and X_2 be schemes. There exists a scheme $X_1 \coprod X_2$, called the sum *of X_1 and X_2, together with morphisms $X_i \to X_1 \coprod X_2$ such that for every scheme Z*

$$\mathrm{Hom}(X_1 \coprod X_2, Z) \simeq \mathrm{Hom}(X_1, Z) \times \mathrm{Hom}(X_2, Z),$$

i.e., every solid commutative diagram



can be completed by a unique dashed morphism.

Proof.

We reduce to affine schemes $X_i = \mathrm{Spec}(A_i)$. Then

$$X_1 \coprod X_2 = \mathrm{Spec}(A_1 \times A_2).$$

□

The underlying topological space of $X_1 \coprod X_2$ is a disjoint union of the X_i.

Relative context

Definition

Let us fix a scheme S.

- An S-scheme, or a scheme over S is a morphism $X \to S$.
- A morphism of S-schemes is a diagram

$$\begin{array}{ccc} X & \longrightarrow & Y \\ & \searrow \quad \swarrow & \\ & S & \end{array}$$

Example

- Let k be a field (or even a ring) and $S = \mathrm{Spec}(k)$. The category of affine S-schemes is equivalent to the category of k-algebras.
- If k is algebraically closed, and we consider only reduced finitely generated k-algebras, the resulting category is essentially the category of affine algebraic varieties over k.

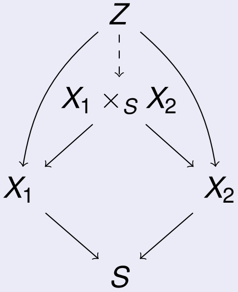
Products

Proposition

Let X_1 and X_2 be schemes over S. There exists a scheme $X_1 \times_S X_2$, called the (fibre) product of X_1 and X_2 over S, together with S-morphisms $X_1 \times_S X_2 \to X_i$ such that for every S-scheme Z

$$\mathrm{Hom}_S(Z, X_1 \times_S X_2) \simeq \mathrm{Hom}_S(Z_1, X_1) \times \mathrm{Hom}_S(Z, X_2),$$

i.e., every solid commutative diagram



can be completed by a unique dashed morphism.

Proof.

We reduce to affine schemes $X_i = \mathrm{Spec}(A_i)$ over $S = \mathrm{Spec}(R)$. Then A_i are R-algebras and

$$X_1 \times_S X_2 = \mathrm{Spec}(A_1 \otimes_R A_2).$$

□

Scheme-valued points

Definition

- Let X and T be schemes. The set of T-valued points of X is the set
$$X(T) = \mathrm{Hom}(T, X).$$
- In a relative setting, suppose X, T are S-schemes. The set of T-valued points of X over S is the set
$$X(T)_S = \mathrm{Hom}_S(T, X).$$

Example

This notation is most commonly used as follows. Consider:

- a system of polynomial equations $f_i = 0$, $i = 1, \dots, m$ defined over a field k, i.e., $f_i \in k[x_1, \dots, x_n]$;
- $A = k[x_1, \dots, x_n]/(f_1, \dots, f_n)$
- and let $K \supseteq k$ be a field extension.

The associated scheme is $X = \mathrm{Spec}(A)$. Then

$$
\begin{aligned}
X(K)_k &= \mathrm{Hom}_{\mathrm{Spec}(k)}(\mathrm{Spec}(K), X) \\
&= \mathrm{Hom}_k(A, K) \\
&\simeq \{\bar{a} \in K^n : f_i(\bar{a}) = 0 \text{ for all } i\}.
\end{aligned}
$$

When k is algebraically closed, $X(k) := X(k)_k \subseteq k^n$ is what we called an affine variety $V(\{f_i\})$ at the start. The scheme X contains much more information.

Example (✎)

Suppose S is a scheme over a field k, and let $X \xrightarrow{f} S$, $Y \xrightarrow{g} S$ be two schemes over S (in particular, over k). Then

$$\begin{aligned}(X \times_S Y)(k) &= X(k) \times_{S(k)} Y(k) \\ &= \{(\bar{x}, \bar{y}) : \bar{x} \in X(k), \bar{y} \in Y(k), \quad f(\bar{x}) = g(\bar{y})\}.\end{aligned}$$

Products vs topological products

Example

Zariski topology of the product is not the product topology, as shown in the following example.
Let k be a field, then

$$\begin{aligned}\mathbb{A}^1 \times \mathbb{A}^1 &= \mathbb{A}^1 \times_{\mathrm{Spec}(k)} \mathbb{A}^1 \\ &= \mathrm{Spec}(k[x_1] \otimes_k k[x_2]) \simeq \mathrm{Spec}(k[x_1, x_2]) = \mathbb{A}^2.\end{aligned}$$

The set of k-points $\mathbb{A}^2(k)$ is the cartesian product

$$\mathbb{A}^1(k) \times \mathbb{A}^1(k).$$

However, as a scheme, $\mathbb{A}^2$ has more points than the cartesian square of the set of points of $\mathbb{A}^1$.

Fibres of a morphism

Definition

Let $\varphi : X \to S$ be a morphism, and let $s \in S$. There exists a natural morphism ✐

$$\mathrm{Spec}(\mathbf{k}(s)) \to S.$$

The fibre of φ over s is

$$X_s = X \times_S \mathrm{Spec}(\mathbf{k}(s)).$$

Remark

X_s should be thought of as $\varphi^{-1}(s)$, except that the above definition gives it a structure of a $\mathbf{k}(s)$-scheme.

Morphisms and families

Example

Consider $R = k[z] \to A = k[x, y, z]/(y^2 - x(x-1)(x-z))$ and the corresponding morphism

$$\varphi : X = \text{Spec}(A) \to S = \text{Spec}(R).$$

Then, for $s \in S$ corresponding to the ideal $(z - \lambda)$, $\lambda \in k$,

$$X_s = X_\lambda = \text{Spec}(k[x, y]/(y^2 - x(x-1)(x-\lambda)))$$

so we can consider φ as a family of curves X_s with parameters s from S.

Reduction modulo p

Example

Consider $\mathbb{Z} \to A = \mathbb{Z}[x, y]/(y^2 - x^3 - x - 1)$ and the corresponding morphism

$$\varphi : X = \mathrm{Spec}(A) \to S = \mathrm{Spec}(\mathbb{Z}).$$

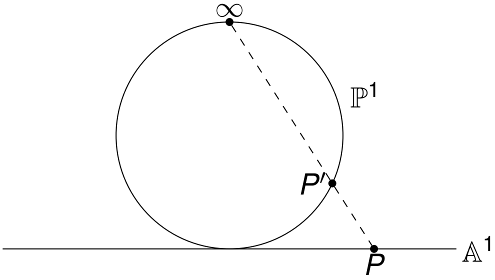
Then, for $\mathfrak{p} \in S$ corresponding to the ideal (p) for a prime integer p,

$$X_{\mathfrak{p}} = X_p = \mathrm{Spec}(\mathbb{F}_p[x, y]/(y^2 - x^3 - x - 1)),$$

as a scheme over $\mathbb{F}_p = \mathbf{k}(\mathfrak{p})$, considered as a reduction of X modulo p.

Projective line as a compactification of $\mathbb{A}^1$

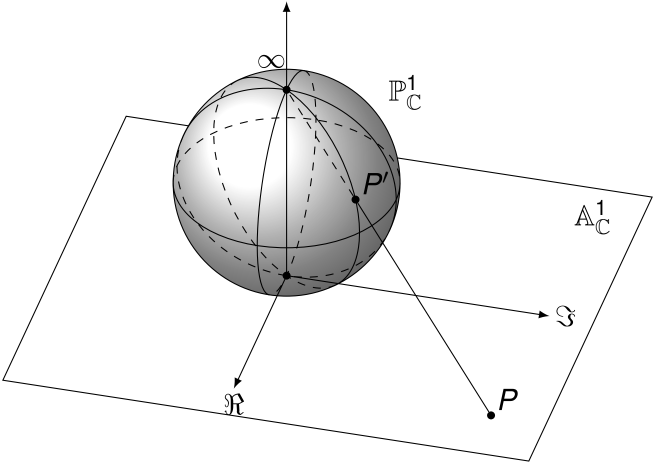
The picture for algebraic geometers:



- Think of $\mathbb{P}^1$ as the set of lines through a fixed point.
- An equation $ax + by + c = 0$ describes a line if not both a, b are 0, and what really matters is the ratio $[a : b]$.

Riemann sphere

The picture for analysts:



Projective space

Fix an algebraically closed field k.

Definition

The projective n-space over k is the set $\mathbb{P}_k^n$ of equivalence classes

$$[a_0 : a_1 : \cdots : a_n]$$

of $(n+1)$-tuples $(a_0, a_1, \ldots, a_n)$ of elements of k, not all zero, under the equivalence relation

$$(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n),$$

for all $\lambda \in k \setminus \{0\}$.

Homogeneous polynomials

Let $S = k[x_0, \ldots, x_n]$.

- For an arbitrary $f \in S$, $P = [a_0 : \cdots : a_n] \in \mathbb{P}^n$, the expression
$$f(P)$$
does not make sense.
- For a homogeneous polynomial $f \in S$ of degree d,
$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n),$$
so it does make sense to consider whether
$$f(P) = 0 \quad \text{or} \quad f(P) \neq 0.$$
- It is beneficial to consider S as a graded ring
$$S = \bigoplus_{d \geq 0} S_d,$$
where S_d is the abelian group consisting of degree d homogeneous polynomials.

Projective varieties

Definition

Let $T \subseteq S$ be a set of homogeneous polynamials. Let

$$V(T) = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all } f \in T\}.$$

We write

$$D(f) = \mathbb{P}^n \setminus V(f).$$

This has the expected properties and gives rise to the Zariski topology on $\mathbb{P}^n$.

Definition

A projective algebraic variety is a subset of $\mathbb{P}^n$ of the form $V(T)$, together with the induced Zariski topology.

Covering the projective space with open affines

Remark

Let

$$U_i = D(x_i) = \{[a_0 : \cdots : a_n] \in \mathbb{P}^n : a_i \neq 0\} \subseteq \mathbb{P}^n, \quad i = 0, \ldots, n.$$

The maps $\varphi_i : U_i \to \mathbb{A}^n$ *defined by*

$$\varphi_i([a_0 : \cdots : a_n]) = \left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i} \right).$$

are all homeomorphisms.
Thus we can cover $\mathbb{P}^n$ *by* $(n+1)$ *affine open subsets.*

Example (from affine to projective curve)

Start with your favourite plane curve, e.g., $X = V(y^2 - x^3 - x - 1)$. Substitute $y \leftarrow y/z$, $x \leftarrow x/z$:

$$\frac{y^2}{z^2} = \frac{x^3}{z^3} + \frac{x}{z} + 1.$$

Clear the denominators:

$$y^2 z = x^3 + xz^2 + z^3.$$

This is a homogeneous equation of a projective curve $\tilde{X}$ in $\mathbb{P}^2$, and $\tilde{X} \cap D(z) \simeq X$.

Graded rings

Definition

- S is a graded ring if
  - $S = \bigoplus_{d \geq 0} S_d$, S_d abelian subgroups;
  - $S_d \cdot S_e \subseteq S_{d+e}$.
- An element $f \in S_d$ is homogeneous of degree d.
- An ideal $\mathfrak{a}$ in S is homogeneous if

$$\mathfrak{a} = \bigoplus_{d \geq 0} (\mathfrak{a} \cap S_d),$$

i.e., if it is generated by homogeneous elements.

Projective schemes

Definition

Let S be a graded ring.

- Let
$$S_+ = \bigoplus_{d>0} S_d \trianglelefteq S.$$
- Let
$$\mathrm{Proj}(S) = \{\mathfrak{p} \trianglelefteq S : \mathfrak{p} \text{ prime, and } S_+ \not\subseteq \mathfrak{p}\}.$$
- For a homogeneous ideal $\mathfrak{a}$, let
$$V_+(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Proj}(S) : \mathfrak{p} \supseteq \mathfrak{a}\}.$$
-
$$D_+(f) = \mathrm{Proj}(S) \setminus V_+(f).$$

As expected, V_+ makes $\mathrm{Proj}(S)$ into a topological space.

Structure sheaf on Proj(S)

Notation: for $\mathfrak{p} \in \text{Proj}(S)$, let $S_{(\mathfrak{p})}$ be the ring of degree zero elements in $T^{-1}S$, where T is the multiplicative set of homogeneous elements in $S \setminus \mathfrak{p}$.

Intuition

If $a, f \in S$ are homogeneous of the same degree, then the function $P \mapsto a(P)/f(P)$ makes sense on $D_+(f)$.

Definition

For U open in Proj(S),

$$\begin{aligned}\mathscr{O}(U) = \{ s : U \to \coprod_{\mathfrak{p} \in U} S_{(\mathfrak{p})} \mid & \text{ for each } \mathfrak{p} \in U, s(\mathfrak{p}) \in S_{(\mathfrak{p})}, \\ & \text{and for each } \mathfrak{p} \text{ there is a nhood } V \ni \mathfrak{p}, \quad V \subseteq U \\ & \text{and homogeneous elements } a, f \text{ of the same degree} \\ & \text{such that for all } \mathfrak{q} \in V, f \notin \mathfrak{q}, \text{ and } s(\mathfrak{q}) = a/f \text{ in } S_{(\mathfrak{q})} \}.\end{aligned}$$

Projective scheme is a scheme

Proposition

1. *For* $\mathfrak{p} \in \mathrm{Proj}(S)$*, the stalk* $\mathscr{O}_{\mathfrak{p}} \simeq S_{(\mathfrak{p})}$*.*
2. *The sets* $D_+(f)$*, for* $f \in S$ *homogeneous, cover* $\mathrm{Proj}(S)$*, and*

$$\left(D_+(f), \mathscr{O}\restriction_{D_+(f)}\right) \simeq \mathrm{Spec}(S_{(f)}),$$

   where $S_{(f)}$ *is the subring of elements of degree 0 in* S_f*.*
3. $\mathrm{Proj}(S)$ *is a scheme.*

Thus we obtained an example of a scheme which is not affine.

Global regular functions on projective varieties

Remark (✐)

The property 2. shows that

$$\mathscr{O}(\mathrm{Proj}(S)) = S_0,$$

so the only global regular functions on $\mathbb{P}^n = \mathrm{Proj}(k[x_0, \ldots, x_n])$ *are constant functions, since* $k[x_0, \ldots, x_n]_0 = k$*.*
The same statements holds for projective varieties.

Exercise✐: for $k = \mathbb{C}$, deduce this from Liouville's theorem.

Properties of schemes

- X is connected, or irreducible, if it is so topologically;
- X is reduced, if for every open U, $\mathscr{O}_X(U)$ has no nilpotents.
- X is integral, if every $\mathscr{O}_X(U)$ is an integral domain.

Lemma (✎)

X is integral iff it is reduced and irreducible.

Finiteness properties

- X is noetherian if it can be covered by finitely many open affine $\mathrm{Spec}(A_i)$ with each A_i a noetherian ring;
- $\varphi : X \to Y$ is of finite type if there exists a covering of Y by open affines $V_i = \mathrm{Spec}(B_i)$ such that for each i, $\varphi^{-1}(V_i)$ can be covered by finitely many open affines $U_{ij} = \mathrm{Spec}(A_{ij})$ where each A_{ij} is a finitely generated B_i-algebra;
- $\varphi : X \to Y$ is finite if Y can be covered by open affines $V_i = \mathrm{Spec}(B_i)$ such that for each i, $\varphi^{-1}(V_i) = \mathrm{Spec}(A_i)$ with A_i is a B_i-algebra which is a finitely generated B_i-module.

Properness

Definition

Let $f : X \to Y$ be a morphism. We say that f is

- separated, if the diagonal Δ is closed in $X \times_Y X$;
- closed, if the image of any closed subset is closed;
- universally closed, if every base change of it is closed, i.e., for every morphism $Y' \to Y$, the corresponding morphism

$$X \times_Y Y' \to Y'$$

  is closed;
- proper, if it is separated, of finite type and universally closed.

Convention

Hereafter, all schemes are separated!!!

Example

Finite morphisms are proper.

Prove this using the going up theorem of Cohen-Seidenberg: If B is an integral extension of A, then $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is onto.

Projective vars as algebraic analogues of compact manifolds

Proposition

Projective varieties are proper (over k).

Images of morphisms

Example

Let $Z = V(xy - 1)$, $X = \mathbb{A}^1$ and let $\pi : Z \to X$ be the projection $(x, y) \mapsto x$.
The image $\pi(Z) = \mathbb{A}^1 \setminus \{0\}$, so not closed.

Theorem (Chevalley)

Let $f : X \to Y$ be a morphism of schemes of finite type. Then the image of a constructible set is a constructible set (i.e., a Boolean combination of closed subsets).

Singularity, intuition via tangents on curves

Suppose we have a point $P = (a, b)$ on a plane curve X defined by

$$f(x, y) = 0.$$

In analysis, the tangent to X at P is the line

$$\frac{\partial f}{\partial x}(P)(x - a) + \frac{\partial f}{\partial y}(P)(y - b) = 0.$$

- The partial derivatives of a polynomial make sense over any field or ring.
- In order for 'tangent line' to be defined, we need at least one of $\frac{\partial f}{\partial x}(P)$, $\frac{\partial f}{\partial y}(P)$ to be nonzero.
- Otherwise, the point P will be 'singular'.

Example

The curve $y^2 = x^3$ has a singular point $(0, 0)$.

There are various types of singularities, this is a cusp.

Tangent space

Definition

Let $X \subseteq \mathbb{A}^n$ be an irreducible affine variety, $I = I(X)$, $P = (a_1, \ldots, a_n) \in X$. The tangent space $T_P(X)$ to X at P is the solution set of all linear equations

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P)(x_i - a_i) = 0, \qquad f \in I.$$

It is enough to take f from a generating set of I. ✎

Intuitive definition for varieties:

We say that P is nonsingular on X if

$$\dim_k T_P(X) = \dim X.$$

Derivations

Definition

Let A be a ring, B an A-algebra, and M a module over B. An A-derivation of B into M is a map

$$d : B \to M$$

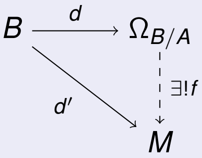
satisfying

1. d is additive;
2. $d(bb') = bd(b') + b'd(b)$;
3. $d(a) = 0$ for $a \in A$.

Module of relative differentials

Definition

The module of relative differential forms of B over A is a B-module $\Omega_{B/A}$ together with an A-derivation $d : B \to \Omega_{B/A}$ such that: for any A-derivation $d' : B \to M$, there exists a unique B-module homomorphism $f : \Omega_{B/A} \to M$ such that $d' = f \circ d$:



Construction of $\Omega_{B/A}$

$\Omega_{B/A}$ is obtained as a quotient of the free B-module generated by symbols $\{db : b \in B\}$ by the submodule generated by elements:

1. $d(bb') - bd(b') - b'd(b)$, for $b, b' \in B$;
2. da, for $a \in A$.

And the 'universal' derivation is just

$$d : b \longmapsto \text{(the coset of) } db.$$

An intrinsic definition of the tangent space

Lemma

Let X be an affine variety over an algebraically closed field k, $P \in X$. Let $\mathfrak{m}_P$ be the maximal ideal of $\mathscr{O}_P$. We have isomorphisms

$$\mathrm{Der}_k(\mathscr{O}_P, k) \xrightarrow{\sim} \mathrm{Hom}_{k\text{-linear}}(\mathfrak{m}_P/\mathfrak{m}_P^2, k) \xrightarrow{\sim} T_P(X).$$

Thus

$$\Omega_{\mathscr{O}_P/k} \otimes_{\mathscr{O}_P} k \simeq \mathfrak{m}_P/\mathfrak{m}_P^2.$$

Thus P is nonsingular iff $\dim_k(\mathfrak{m}_P/\mathfrak{m}_P^n) = \dim(\mathscr{O}_P)$ iff $\Omega_{\mathscr{O}_P/k}$ is a free $\mathscr{O}_P$-module of rank $\dim(\mathscr{O}_P)$.

Nonsingularity

Definition

A noetherian local ring $(R, \mathfrak{m})$ with residue field $k = R/\mathfrak{m}$ is regular, if $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim(R)$.

By Nakayama's lemma, this is equivalent to $\mathfrak{m}$ having $\dim(R)$ generators.

Definition

- A noetherian scheme X is regular, or nonsingular at x, if $\mathscr{O}_x$ is a regular local ring.
- X is regular/nonsingular if it is so at every point $x \in X$.

Sheaves of differentials; regularity vs smoothness

Let $\varphi : X \to Y$ be a morphism. There exists a sheaf of relative differentials $\Omega_{X/Y}$ on X and a sheaf morphism $d : \mathscr{O}_X \to \Omega_{X/Y}$ such that:
if $U = \mathrm{Spec}(A) \subseteq Y$ and $V = \mathrm{Spec}(B) \subseteq X$ are open affine such that $f(V) \subseteq U$, then $\Omega_{X/Y}(V) = \Omega_{B/A}$.

Proposition

Let X be an irreducible scheme of finite type over an algebraically closed field k. Then X is regular over k iff $\Omega_{X/k}$ is a locally free sheaf of rank $\dim(X)$, i.e., every point has an open neighbourhood U such that

$$\Omega_{X/k} \restriction U \simeq (\mathscr{O}_X \restriction U)^{\dim(X)}.$$

Over non-algebraically closed field the latter is associated with a notion of smoothness.

Generic non-singularity

Corollary

If X is a variety over a field k of characteristic 0, then there is an open dense subset U of X which is nonsingular.

Example

Funny things can happen in characteristic $p > 0$; think of the scheme defined by $x^p + y^p = 1$.

DVR's

Definition

Let K be a field. A discrete valuation of K is a map $v : K \setminus \{0\} \to \mathbb{Z}$ such that

1. $v(xy) = v(x) + v(y)$;
2. $v(x + y) \geq \min(v(x), v(y))$.

Then:

- $R = \{x \in K : v(x) \geq 0\} \cup \{0\}$ is a subring of K, called the valuation ring;
- $\mathfrak{m} = \{x \in K : v(x) > 0\} \cup \{0\}$ is an ideal in R, and $(R, \mathfrak{m})$ is a local ring.

Definition

A valuation ring is an integral domain R which the valuation ring of some valuation of $\mathrm{Fract}(R)$.

Characterisations of DVR's

Fact

Let $(R, \mathfrak{m})$ be a noetherian local domain of dimension 1. TFAE:

1. *R is a DVR;*
2. *R is integrally closed;*
3. *R is a regular local ring;*
4. *$\mathfrak{m}$ is a principal ideal.*

Remark

Let X be a nonsingular curve, $x \in X$. Then $\mathcal{O}_x$ is a regular local ring of dimension 1, and thus a DVR.

A uniformiser at x is a generator of $\mathfrak{m}_x$.

Dedekind domains

Fact

Let R be an integral domain which is not a field. TFAE:

1. *every nonzero proper ideal factors into primes;*
2. *R is noetherian, and the localisation at every maximal ideal is a DVR;*
3. *R is an integrally closed noetherian domain of dimension 1.*

Definition

R is a Dedekind domain if it satisfies (any of) the above conditions.

Remark

If X is a nonsingular curve, then $\mathscr{O}(X)$ is a Dedekind domain.

Divisors

Definition

Let X be an irreducibe nonsingular curve over an algebraically closed field k.

- A Weil divisor is an element of the free abelian group $\mathrm{Div}X$ generated by the (closed) points of X, i.e., it is a formal integer combination of points of X.
- A divisor $D = \sum_i n_i x_i$ is effective, denoted $D \geq 0$ if all $n_i \geq 0$.

Principal divisors

Definition

Let X be an integral nonsingular curve over an algebraically closed field k, and let $K = \mathbf{k}(X) = \mathscr{O}_\xi = \varinjlim_{U \text{ open}} \mathscr{O}_X(U)$ be its function field (where ξ is the generic point of X), which we think of as the field of 'rational functions' on X.
For $f \in K^\times$, we let the divisor (f) of f on X be

$$(f) = \sum_{x \in X^0} v_x(f) \cdot x,$$

where v_x is the valuation in $\mathscr{O}_x$. Any divisor which is equal to the divisor of a function is called a principal divisor.

Remark

Note this is a divisor: if f is represented as $f_U \in \mathscr{O}_X(U)$ on some open U, and thus (f) is 'supported' on $V(f_U) \cup X \setminus U$, which is a proper closed subset of X and it is thus finite.

Remark

$f \mapsto (f)$ is a homomorphism $K^\times \to \mathrm{Div} X$ whose image is the subgroup of principal divisors.

Definition

For a divisor $D = \sum_i n_i x_i$, we define the degree of D as

$$\deg(D) = \sum_i n_i,$$

making deg into a homomorphism $\mathrm{Div} X \to \mathbb{Z}$.

Divisor class group

Definition

Let X be a non-singular difference curve over k.

- Two divisors $D, D' \in \mathrm{Div}X$ are linearly equivalent, written $D \sim D'$, if $D - D'$ is a principal divisor.
- The divisor class group $\mathrm{Cl}X$ is the quotient of $\mathrm{Div}X$ by the subgroup of principal divisors.

Ramification

Definition

Let $\varphi : X \to Y$ be a morphism of nonsingular curves, $y \in Y$ and $x \in X$ with $\pi(x) = y$.
The ramification index of φ at x is

$$e_x(\varphi) = v_x(\varphi^\sharp t_y),$$

where $\varphi^\sharp$ is the local morphism $\mathscr{O}_y \to \mathscr{O}_x$ induced by φ and t_y is a uniformiser at y, i.e., $\mathfrak{m}_y = (t_y)$.
When φ is finite, we can define a morphism $\varphi^* : \operatorname{Div} Y \to \operatorname{Div} X$ by extending the rule

$$\varphi^*(y) = \sum_{\varphi(x)=y} e_x(\varphi) \cdot x$$

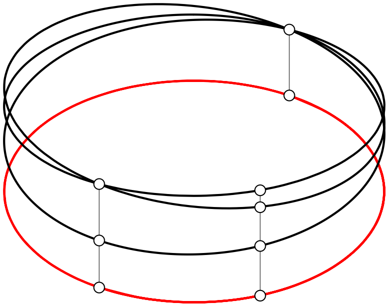
for prime divisors $y \in Y$ by linearity to $\operatorname{Div} Y$.

Preservation of multiplicity

Theorem

Let $\varphi : X \to Y$ be a morphism of nonsingular projective curves with $\varphi(X) = Y$, then $\deg \varphi = \deg(\varphi^*(y))$ for any point $y \in Y$.

Proof reduces to the Chinese Remainder Theorem.



The number of poles equals the number of zeroes

Corollary

The degree of a principal divisor on a nonsingular projective curve equals 0.

Proof.

Any $f \in \mathbf{k}(X)$ defines a morphism $f : X \to \mathbb{P}^1$. Then

$$\deg((f)) = \deg(f^*(0)) - \deg(f^*(\infty)) = \deg(f) - \deg(f) = 0.$$

□

Remark

Hence $\deg : \mathrm{Cl}(X) \to \mathbb{Z}$ *is well-defined.*

Bezout's theorem

Theorem (Bezout)

Let $X \subseteq \mathbb{P}^n$ be a nonsingular projective curve, and let $H = V_+(f) \subseteq \mathbb{P}^n$ be the hypersurface defined by a homogeneous polynomial f. Then, writing

$$X.H = \sum_{x \in X \cap H} i(x; X, H)x := (f),$$

we have that

$$\deg(X.H) = \deg(X) \deg(f),$$

where $\deg(X)$ *is the maximal number of points of intersection of X with a hyperplane in $\mathbb{P}^n$ (which does not contain a component of X).*

Proof.

Let $d = \deg(f)$. For any linear form l, $h = f/l^d \in \mathbf{k}(X)$, so

$$\deg((f)) = \deg((l^d)) + \deg((h)) = d\deg(l) + 0 = d\deg(X).$$

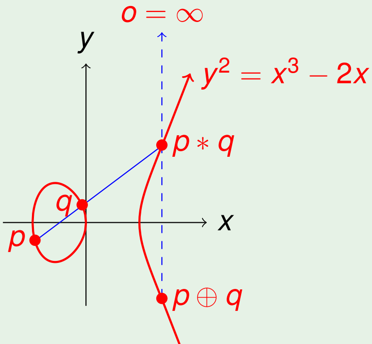
□

Elliptic curves

Let E be a nonsingular projective plane cubic, and pick a point $o \in E$. For points $p, q \in E$, let $p * q$ be the unique point such that, writing L for the line pq and using Bezout, $E.L = p + q + p * q$. We define

$$p \oplus q = o * (p * q).$$

Example ($E \ldots \quad y^2 z = x^3 - 2xz^2$, $o = \infty := [0:1:0]$)



Proposition

Let (E, o) *be an elliptic curve, i.e., a nonsingular projective cubic over* k. *Then* $(E(k), \oplus)$ *is an abelian group.*

Proof.

Only the associativity of $\oplus$ needs checking. For a fun proof ✐using nothing other than Bezout's Theorem see Fulton's Alg. Curves. □

Aside on algebraic groups

Definition

A group variety over $S = \mathrm{Spec}(k)$ is a variety $X \xrightarrow{\pi} S$ together with a section $e : S \to X$ (identity), and morphisms $\mu : X \times_S X \to X$ (group operation) and $\rho : X \to X$ (inverse) such that

1. $\mu \circ (id \times \rho) = e \circ \pi : X \to X$;
2. $\mu \circ (\mu \times id) = \mu \circ (id \times \mu) : X \times X \times X \to X$.

Clearly, for a field K extending k, $X(K)$ is a group.

Examples of algebraic groups

Examples

1. Additive group $\mathbb{G}_a = \mathbb{A}^1_k$. Multiplicative group $\mathbb{G}_m = \operatorname{Spec}(k[x, x^{-1}])$.
2. $SL_2(k) = \{(a, b, c, d) : ad - bc = 1\}$. $\rho(a, b, c, d) = (d, -b, -c, a)$ etc.
3. $GL_2(k) = \operatorname{Spec}(k[a, b, c, d, 1/(ad - bc)])$.

Elliptic curves are abelian varieties

Proposition

Let (E, o) be an elliptic curve. Then $(E, \oplus)$ is a group variety.

In other words, the operations $\oplus : E \times E \to E$ and $\ominus : E \to E$ are morphisms.

Definition

An abelian variety is a connected and proper group variety (it follows that the operation is commutative, hence the name).

Thus, elliptic curves are examples of abelian varieties.

The canonical divisor

Definition

Let X be an integral non-singular projective curve over k. Then $\Omega_{X/k}$ is a locally free sheaf of rank 1, and pick a non-zero global section $\omega \in \Omega_{X/k}(X)$. For $x \in X$, let t be the uniformiser at x, and let $f \in \mathbf{k}(X)$ be such that $\omega = f\,dt$. Define

$$v_x(\omega) = v_x(f),$$

and the resulting canonical divisor

$$W = \sum_x v_x(\omega)x.$$

The divisor W' of a different $\omega' \in \Omega_{X/k}(X)$ is linearly equivalent to W, $W' \sim W$, and thus W uniquely determines a canonical class K_X in $\mathrm{Cl}X$.

Example

[Canonical divisor of an elliptic curve]

Complete linear systems

Definition

Let D be a divisor on X, and write

$$L(D) = \{f \in \mathbf{k}(X) : (f) + D \geq 0\}.$$

A theorem of Riemann shows that these are finite dimensional vector spaces over k, and let

$$l(D) = \dim L(D).$$

Remark

f and f' define the same divisor iff $f' = \lambda f$, for some $\lambda \neq 0$, so we have a bijection

$$\{\textit{effective divisors} \sim D\} \leftrightarrow \mathbb{P}(L(D)).$$

Riemann-Roch Theorem

Definition

The genus of a curve X is $l(K_X)$.

Theorem (Riemann-Roch)

Let D be a divisor on a projective nonsingular curve X of genus g over an algebraically closed field k. Then

$$l(D) - l(K_X - D) = \deg(D) + 1 - g.$$

In particular, $\deg(K_X) = 2g - 2$.

The zeta function

Definition

Let X be a 'variety' over a finite field $k = \mathbb{F}_q$. Its zeta function is the formal power series

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{n\geq 1} \frac{|X(\mathbb{F}_{q^n})|}{n} T^n\right).$$

Examples

- Let $X = \mathbb{A}^N_{\mathbb{F}_q}$. We have $|\mathbb{A}^N_{\mathbb{F}_q}(\mathbb{F}_{q^n})| = q^{nN}$, so

$$Z(\mathbb{A}^N_{\mathbb{F}_q}, T) = \exp\left(\sum_{n\geq 1} \frac{(q^N T)^n}{n}\right) = \frac{1}{1 - q^N T}.$$

- For $X = \mathbb{P}^N_{\mathbb{F}_q}$,

$$\mathbb{P}^N_{\mathbb{F}_q}(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)} - 1}{q^n - 1} = 1 + q^n + q^{2n} + \cdots + q^{Nn}, \quad \text{so}$$

$$Z(\mathbb{P}^N_{\mathbb{F}_q}/\mathbb{F}_q, T) = \exp\left(\sum_{n\geq 1} \frac{T^n}{n} \sum_{j=0}^{N} q^{nj}\right) = \prod_{j=0}^{N} Z(\mathbb{A}^j_{\mathbb{F}_q}/\mathbb{F}_q, T)$$

$$= \prod_{j=0}^{N} \frac{1}{1 - q^j T}.$$

Frobenius

Suppose X is over $\mathbb{F}_q$, consider the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$, and the Frobenius automorphism

$$F_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, \quad F_q(x) = x^q.$$

Then F_q acts on $X(\bar{\mathbb{F}}_q) = \mathrm{Hom}(\mathrm{Spec}(\bar{\mathbb{F}}_q), X)$ by precomposing with ${}^a F_q$.

Intuitively, if X is affine in $\mathbb{A}^N$, then

$$F_q(x_1, \dots, x_N) = (x_1^q, \dots, x_N^q).$$

Remark

$$X(\mathbb{F}_{q^n}) = \mathrm{Fix}(F_q^n).$$

Points vs geometric points

Remark

A closed point $x \in X$ corresponds to an F_q-orbit of an $\bar{x} \in X(\bar{\mathbb{F}}_q)$, and

$$[\mathbf{k}(x) : \mathbb{F}_q] = |\{\textit{orbit of } \bar{x}\}| = \min\{n : \bar{x} \in X(\mathbb{F}_{q^n})\}.$$

Definition

For a closed point $x \in X$, let

$$\deg(x) = [\mathbf{k}(x) : \mathbb{F}_q], \qquad Nx = q^{\deg(x)}.$$

Comparison with the Riemann zeta

Recall Riemann's definition:

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{p \in \mathrm{Specm}\,\mathbb{Z}} (1 - p^{-s})^{-1}.$$

Lemma

$$Z(X/\mathbb{F}_q, T) = \prod_{x \in X^0} (1 - T^{\deg(x)})^{-1},$$

i.e., after a variable change $T \leftarrow q^{-s}$,

$$Z(X/\mathbb{F}_q, q^{-s}) = \prod_{x \in X^0} (1 - Nx^{-s})^{-1}.$$

Proof.

Exercise ✐ upon remarking that

$$|X(\mathbb{F}_{q^n})| = \sum_{r|n} r \cdot |\{x \in X^0 : \deg(x) = r\}|.$$

□

The Weil Conjectures

Let X be a smooth projective variety of dimension d over $k = \mathbb{F}_q$, $Z(T) := Z(X/k, T)$. Then

1. Rationality. $Z(T)$ is a rational function.
2. Functional equation.

$$Z(\frac{1}{q^d T}) = \pm T^\chi q^{\chi/2} Z(T),$$

   where χ is the 'Euler characteristic' of X.
3. Riemann hypothesis.

$$Z(T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)\cdots P_{2d}(T)},$$

   where each $P_i(T)$ has integral coefficients and constant term 1, and

$$P_i(T) = \prod_j (1 - \alpha_{ij} T),$$

   where α_{ij} are algebraic integers with $|\alpha_{ij}| = q^{i/2}$. The degree of P_i is the 'i-th Betti number' of X.

- The use of ‘Euler characteristic’ and ‘Betti numbers’ implies that the arithmetical situation is controlled by the classical geometry of X.
- History of proof: Dwork, Grothendieck-Artin, Deligne.
- We shall sketch the rationality for curves.

Divisors over non-algebraically closed base field

Definition

Let X be a curve over k.

- $\text{Div}(X)$ is the free abelian group generated by the closed points of X.
- For $D = \sum_i n_i x_i \in \text{Div}(X)$, let

$$\deg(D) = \sum_i n_i \deg(x_i).$$

- Write $\text{Div}(n) = \{D \in \text{Div}(X) : \deg(D) = n\}$ and $\mathrm{Cl}(n) = \text{Div}(n)/\sim$.

Structure of divisor class groups

Using Riemann-Roch, if $\deg(D) > 2g-2$, then $\deg(K_X - D) < 0$ so $l(K_X - D) = 0$ and thus

$$l(D) = \deg(D) + 1 - g.$$

Therefore, for $n > 2g-2$, the number E_n of effective divisors of degree n is

$$\infty > E_n = \sum_{\bar{D}\in \mathrm{Cl}(n)} \frac{q^{l(D)}-1}{q-1} = \sum_{\bar{D}\in \mathrm{Cl}(n)} \frac{q^{n+1-g}-1}{q-1} = |\mathrm{Cl}(n)| \frac{q^{n+1-g}-1}{q-1}.$$

In particular, $|\mathrm{Cl}(n)| < \infty$.

Structure of divisor class groups

Suppose the image of $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ is $d\mathbb{Z}$ (we will see later that $d = 1$). Choosing some $D_0 \in \mathrm{Div}(d)$ defines an isomorphism

$$\begin{aligned} \mathrm{Cl}(n) &\xrightarrow{\sim} \mathrm{Cl}(n+d) \\ D &\longmapsto D_0 + D, \end{aligned}$$

and therefore

$$|\mathrm{Cl}(n)| = \begin{cases} J & \text{if } d|n \\ 0 & \text{otherwise,} \end{cases}$$

where $J = |\mathrm{Cl}(0)|$ is the number of rational points on the Jacobian of X.
NB $d|2g-2$ since $\deg(K_X) = 2g-2$.

Rationality of zeta for curves

$$
\begin{aligned}
Z(X/\mathbb{F}_q, T) &= \prod_{x \in X^0} (1 - T^{\deg(x)})^{-1} = \sum_{D \geq 0} T^{\deg(D)} = \sum_{n \geq 0} E_n T^n \\
&= \sum_{\substack{n=0 \\ d|n}}^{2g-2} T^n \sum_{\bar{D} \in \mathrm{Cl}(n)} \frac{q^{l(D)} - 1}{q - 1} + \sum_{\substack{n=2g-2+d \\ d|n}}^{\infty} T^n J \frac{q^{n+1-g}}{q-1} \\
&= Q(T) + \frac{J}{q-1} T^{2g-2+d} \left[\frac{q^{g-1+d}}{1 - (qT)^d} - \frac{1}{1 - T^d} \right],
\end{aligned}
$$

so $Z(X/\mathbb{F}_q, T)$ is a rational function in T^d with first order poles at $T = \xi$, $T = \frac{\xi}{q}$ for $\xi^d = 1$.

Lemma (Extension of scalars ✎)

$$Z(X \times_{\mathbb{F}_q} \mathbb{F}_{q^r}/\mathbb{F}_{q^r}, T^d) = \prod_{\xi^r=1} Z(X/\mathbb{F}_q, \xi T).$$

Proposition

$d = 1$.

Proof.

By an analogous argument, $Z(X \times_{\mathbb{F}_q} \mathbb{F}_{q^d}/\mathbb{F}_{q^d}, T^d)$ has a first order pole at $T = 1$. Using extension of scalars and the fact that $Z(X/\mathbb{F}_q, T)$ is a function of T^d, we get

$$Z(X \times_{\mathbb{F}_q} \mathbb{F}_{q^d}/\mathbb{F}_{q^d}, T^d) = \prod_{\xi^d=1} Z(X/\mathbb{F}_q, \xi T) = Z(X/\mathbb{F}_q, T)^d.$$

Comparing poles, we conclude $d = 1$. □

Functional equation for curves

Remark

By inspecting the above calculation of $Z(X/\mathbb{F}_q, T)$, using Riemann-Roch, one can deduce the functional equation ✏

$$Z(X/\mathbb{F}_q, \frac{1}{qT}) = q^{1-g}T^{2-2g}Z(X/\mathbb{F}_q, T).$$

Cohomological interpretation of Weil conjectures

Let X be a variety of dimension d over $k = \mathbb{F}_q$, $\bar{X} = X \times_k \bar{k}$ and let $F : \bar{X} \to \bar{X}$ be the Frobenius morphism. Fix a prime $l \neq p = char(k)$. There exist l-adic étale cohomology groups (with compact support)

$$H^i(X) = H^i_c(\bar{X}, \mathbb{Q}_l), \quad i = 0, \dots, 2d$$

which are finite dimensional vector spaces over $\mathbb{Q}_l$
so that F induces vector space morphisms $F^* : H^i(X) \to H^i(X)$
and we have a Lefschetz fixed-point formula

$$|X(\mathbb{F}_{q^n})| = |Fix(F^n)| = \sum_{i=0}^{2d} (-1)^i \mathrm{tr}(F^{*n} | H^i(X)).$$

Weil rationality using cohomology

$$
\begin{aligned}
Z(X,T) &= \exp\left(\sum_{n\geq 1}\frac{T^n}{n}\sum_{i=0}^{2d}(-1)^i \mathrm{tr}(F^{*n}|H^i(X))\right)\\
&= \prod_{i=0}^{2d}\left[\exp\left(\sum_{n\geq 1}\mathrm{tr}(F^{*n}|H^i(X))\frac{T^n}{n}\right)\right]^{(-1)^i}\\
&= \prod_{i=0}^{2d}\left[\det(1-F^*T|H^i(X))\right]^{(-1)^i}
\end{aligned}
$$

an alternating product of the characteristic polynomials of the Frobenius on cohomology.