

# Computational Arithmetic - Geometry for Algebraic Curves

Yash Sharma



# CONTENTS

---

## Contents

<b>01 Foundations of Algebraic Geometry &amp; Varieties . . . . .</b>	<b>3</b>
1.1. Introduction & Motivation . . . . .	3
1.2. Affine Varieties . . . . .	6
1.3. Quasi-Affine Varieties . . . . .	8
1.4. The Correspondence . . . . .	12
1.5. Functions on Varieties . . . . .	14
1.6. Dimension of Affine Varieties . . . . .	15
1.7. Projective Varieties . . . . .	18
1.8. Regular Functions and Morphisms . . . . .	23
1.9. Localization of Rings . . . . .	28
1.10. The Sheaf of Regular Functions and Functoriality . . . . .	29
1.11. The Sheaf of Regular Functions and Distinguished Open Sets . . . . .	30
1.12. Rational Maps and Birational Equivalence . . . . .	32
1.13. Birationality and Hypersurfaces . . . . .	34
1.14. Non-singular (or Smooth) Varieties . . . . .	36
1.14.1. Singular and Non-Singular Points . . . . .	38
<b>02 Resolution of Singularities &amp; Valuations . . . . .</b>	<b>40</b>
2.1. Introduction: Resolving Singularities of Curves . . . . .	40
2.2. Blowing-Up: Resolving Singularities . . . . .	41
2.3. Discrete Valuation Rings (DVRs) . . . . .	42
2.4. Valuation Theory . . . . .	42
2.5. Classification of Valuations on the Rational Function Field . . . . .	46
2.6. Extension of Valuation Rings . . . . .	47
2.7. Abstract Curves and Their Morphisms . . . . .	48
<b>03 Divisors, Function Fields &amp; Approximation . . . . .</b>	<b>50</b>

3.1. Abstract Curves and Non-Singular Projective Models . . . . .	50
3.2. Points on a Smooth Projective Curve . . . . .	51
3.3. Approximation Theorems . . . . .	53
3.4. Divisors on Smooth Projective Curves . . . . .	56
<b>04 Zeta Function of a Curve over Finite Fields . . . . .</b>	<b>59</b>
4.1. Counting Points on Curves over Finite Fields . . . . .	59
4.2. The Zeta Function: Definition and Basic Properties . . . . .	60
4.3. Rationality, Functional Equation, and Fundamental Properties	62
4.4. Behavior under Base Change . . . . .	64
<b>05 Weil Bounds, Cohomology &amp; L-Functions . . . . .</b>	<b>66</b>
5.1. L-Functions and Zeta Functions . . . . .	66
5.2. Point Counting via Zeta Functions . . . . .	67
5.3. Riemann Hypothesis for Curves over Finite Fields . . . . .	68
5.4. Galois Covers and Point Counting . . . . .	70
5.5. Bombieri-Stepanov Method: Proof of Weil Bounds . . . . .	72
5.6. Conclusion and Results . . . . .	78
5.7. Cohomological Interpretation of L-Functions . . . . .	79
<b>References . . . . .</b>	<b>81</b>

# CHAPTER 1

## FOUNDATIONS OF ALGEBRAIC GEOMETRY & VARIETIES

---

### 1.1 Introduction & Motivation

#### Finite fields and algebraic closures

We begin with finite fields. The finite field  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , where  $p$  is a prime number, can be extended to larger fields such as  $\mathbb{F}_{p^2}$ , and so on, up to the algebraic closure  $\overline{\mathbb{F}_p}$ . Thus, we have the inclusion:

$$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \overline{\mathbb{F}_p}.$$

We are going to study polynomials over these fields, specifically  $\mathbb{F}_p[x_1, \dots, x_n]$ . Through these notes, we will primarily focus on the case where  $n = 2$ , i.e., polynomials in two variables.

#### Arithmetic geometry

Algebraic Geometry studies polynomial equations such as:

$$x^2 - 2 = 0, \quad y^2 = x^3 + x, \quad y^2 = x^n + x,$$

from a geometric point of view. This means we are interested in properties that can be understood or even *visualized*, sometimes even over finite fields like  $\mathbb{F}_p$ .

#### Arithmetic Geometry

Arithmetic Geometry, on the other hand, studies *counting questions*. For example, we may ask: How many points (or solutions, roots, or zeros) exist on the curve

$$y^2 = x^3 \pmod{p}?$$

*Solution.* We want to find the number of solutions

$$(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \text{ to } y^2 \equiv x^3 \pmod{p}.$$

For each fixed  $x \in \mathbb{F}_p$ , the number of corresponding  $y$ -values is

$$1 + \chi(x^3),$$

where  $\chi$  denotes the Legendre symbol modulo  $p$ , with  $\chi(0) = 0$ .

Hence, the total number of affine solutions is

$$N = \sum_{x \in \mathbb{F}_p} (1 + \chi(x^3)) = p + \sum_{x \in \mathbb{F}_p} \chi(x^3).$$

For  $x \neq 0$ , we have

$$\chi(x^3) = \chi(x)^3 = \chi(x),$$

since  $\chi(x) = \pm 1$  for nonzero  $x$ . Therefore,

$$\sum_{x \in \mathbb{F}_p} \chi(x^3) = \sum_{x \in \mathbb{F}_p^\times} \chi(x) = 0,$$

because the Legendre symbol sums to zero over all nonzero elements of  $\mathbb{F}_p$ .

Thus, the total number of affine solutions is

$$N = p.$$

If we also include the single point at infinity in the projective curve, the total number of points is

$$N = p + 1.$$

(Later on we will see that this is a special case of a more general result.)

## Algorithmic complexity and NP-completeness

In these notes, we are also interested in algorithmic problems. Given polynomials  $f_i \in \mathbb{F}_p[x_1, \dots, x_n]$ , we ask:

Does there exist  $P \in \mathbb{F}_p^n$  such that  $f_i(P) = 0$  for all  $i$ ?

A natural question is: How difficult is this problem?

## Complexity and Simplifications

It turns out that this problem is **NP-complete**, even when the degree of each  $f_i$  is only 2 and  $p = 2$ . Therefore, efficient or practical algorithms are unlikely to exist in general.

However, in these notes, we will focus on the simpler case where  $n = 2$ , that is, on *curves* over  $\mathbb{F}_q$ . This case is expected to be much easier to handle. In fact, much of modern

mathematics has grown from studying such objects.

## Course Overview

The first part of these notes will cover the fundamentals of Algebraic Geometry that are needed for counting zeros of polynomials. The second part will apply these ideas to Computer Science problems.

We will study curves using the modern language of Algebraic Geometry—through concepts such as *varieties*, *morphisms*, and *function fields*. The guiding idea is that the geometric properties of a curve are reflected in the algebraic properties of the functions defined on it.

Throughout the notes, I am using this book as a reference [1].

## Studying Curves Algebraically

To study the roots of an equation like

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

we look at the quotient ring:

$$\mathbb{F}_p[x, y]/\langle y^2 - x^3 - x \rangle.$$

One important result we will encounter is the **Riemann–Roch theorem**, which defines the *genus* of a curve in a purely algebraic way.

We will study this in detail later on in Chapter ??, where we will develop the necessary tools to state and prove the Riemann–Roch theorem.

We will also prove an estimate for the number of points on a curve over a finite field—this is known as the **Riemann Hypothesis for Curves**.

## Applications

There are many applications of these ideas, including:

- Algorithms for counting points on curves (an open problem: finding a fast algorithm for curves),
- Integer factorization algorithms (open problem),
- Computing  $\sqrt{a}$  or  $k$ -th roots of  $a$  in  $\mathbb{F}_p$ ,
- Cryptographic systems,
- Coding theory.

## 1.2 Affine Varieties

### Affine $n$ -space and coordinate rings

Let  $k$  be a field (e.g.,  $\mathbb{F}_p$ ,  $\mathbb{C}$ ).

#### Definition 1.2.1: Affine $n$ -space

Affine  $n$ -space over  $k$  is the set

$$\mathbb{A}_k^n := k^n.$$

If  $P \in \mathbb{A}_k^n$  and  $P = (a_1, \dots, a_n)$ , then  $a_i \in k$  is the  $i$ -th coordinate of  $P$ .

The polynomial ring

$$A := k[x_1, \dots, x_n]$$

is the *coordinate ring* of  $\mathbb{A}_k^n$ .

### Functions on affine space

For  $f \in A$ , define a function  $f : \mathbb{A}_k^n \rightarrow k$  by

$$P \mapsto f(P).$$

The *zeros* of  $f$  are

$$Z(f) = \{P \in \mathbb{A}_k^n \mid f(P) = 0\} \subseteq \mathbb{A}_k^n.$$

For a subset  $T \subseteq A$ , define

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

#### Example 1.2.1:

$$Z(x_1^2, x_1 + x_2) = \{(0, 0)\}, \quad Z(x_1^2) = \{(0, t) \mid t \in k\}.$$

#### Definition 1.2.2: Algebraic Set

A subset  $Y \subseteq \mathbb{A}_k^n$  is *algebraic* or *closed* if  $Y = Z(T)$  for some  $T \subseteq A$ .

**Example 1.2.0.1.**  $\mathbb{C} = \mathbb{A}_{\mathbb{C}}^1$  is closed (as  $\mathbb{C} = Z(0)$ ).  $\mathbb{C} \setminus \{0\}$  is not closed.

**Remark.** The complement of a closed set is *open*.

#### Definition 1.2.3: Ideal of a Set

For  $Y \subseteq \mathbb{A}_k^n$ , define

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

An ideal  $I \subseteq A$  satisfies  $I \triangleleft A$  if  $I$  is a subring and  $a \cdot I \subseteq I$  for all  $a \in A$ . We have the associations:

$$\begin{array}{ccc} \text{closed subsets of } \mathbb{A}_k^n & \xrightarrow{I(\cdot)} & \text{ideals of } A \\ Y & \mapsto & I(Y) \\ Z(T) & \leftarrow & T \\ & \xleftarrow{Z(\cdot)} & \end{array}$$

**Remark.** If  $I$  is the ideal generated by the set  $T$ , denoted  $I = \langle T \rangle$ , then  $Z(T) = Z(I)$ . Therefore, every algebraic set can be written as  $Z(I)$  for some ideal  $I \triangleleft A$ . By the Hilbert Basis Theorem, every ideal in  $A$  is finitely generated, so we can always take  $T$  to be a finite set of polynomials.

## The Zariski Topology

**Proposition 1.2.0.2** (Properties of Open Sets in the Zariski Topology). (a) The empty set  $\emptyset$  and the entire space  $\mathbb{A}^n$  are open.

- (b) The union of an arbitrary collection of open sets,  $\{Y_i\}_{i \in I}$ , is open.
- (c) The intersection of a finite collection of open sets,  $\{Y_i\}_{i=1}^m$ , is open.

*Proof.* (a) **Proof that  $\emptyset$  and  $\mathbb{A}^n$  are open:**

A set is open if its complement is a closed (algebraic) set.

- The complement of  $\mathbb{A}^n$  is the empty set,  $\emptyset$ . The empty set can be written as the zero set of the constant polynomial 1, i.e.,  $\emptyset = Z(1)$ . Since  $\emptyset$  is a closed set, its complement,  $\mathbb{A}^n$ , is **open**.
- The complement of  $\emptyset$  is the entire space  $\mathbb{A}^n$ . The entire space can be written as the zero set of the zero polynomial, i.e.,  $\mathbb{A}^n = Z(0)$ . Since  $\mathbb{A}^n$  is a closed set, its complement,  $\emptyset$ , is **open**.

(b) **Proof that an arbitrary union of open sets is open:**

Let  $\{Y_i\}_{i \in I}$  be an arbitrary collection of open sets.

- By definition, each  $Y_i$  is the complement of a closed set  $Z(T_i)$  for some set of polynomials  $T_i$ . So,  $Y_i = \mathbb{A}^n \setminus Z(T_i)$ .
- We examine the union:

$$\bigcup_{i \in I} Y_i = \bigcup_{i \in I} (\mathbb{A}^n \setminus Z(T_i))$$

- Using De Morgan's laws, the union of complements is the complement of the intersection:

$$\bigcup_{i \in I} Y_i = \mathbb{A}^n \setminus \left( \bigcap_{i \in I} Z(T_i) \right)$$

- The arbitrary intersection of closed sets is a closed set. Specifically,  $\bigcap_{i \in I} Z(T_i) = Z(\bigcup_{i \in I} T_i)$ .
- Since  $\bigcap_{i \in I} Z(T_i)$  is a closed set, its complement,  $\bigcup_{i \in I} Y_i$ , is by definition **open**.

**(c) Proof that a finite intersection of open sets is open:**

Let  $\{Y_i\}_{i=1}^m$  be a finite collection of open sets.

- By definition, each  $Y_i = \mathbb{A}^n \setminus Z(T_i)$  for some set of ideals (or sets of polynomials)  $T_i$ .
- We examine the intersection:

$$\bigcap_{i=1}^m Y_i = \bigcap_{i=1}^m (\mathbb{A}^n \setminus Z(T_i))$$

- Using De Morgan's laws, the intersection of complements is the complement of the union:

$$\bigcap_{i=1}^m Y_i = \mathbb{A}^n \setminus \left( \bigcup_{i=1}^m Z(T_i) \right)$$

- The union of a finite number of closed sets is a closed set. We know that  $Z(T_1) \cup Z(T_2) = Z(T_1 T_2)$ , where  $T_1 T_2$  is the set of all products of polynomials from  $T_1$  and  $T_2$ . By induction, the finite union  $\bigcup_{i=1}^m Z(T_i)$  is equal to  $Z(T_1 T_2 \cdots T_m)$ , which is a closed set.
- Since  $\bigcup_{i=1}^m Z(T_i)$  is a closed set, its complement,  $\bigcap_{i=1}^m Y_i$ , is by definition **open**.

□

E.g.,  $\bigcup_{\alpha \in \mathbb{C} \setminus \{0\}} \{\alpha\} = \mathbb{A}_{\mathbb{C}}^1 \setminus S \neq Z(T)$  (Not closed).

**Definition 1.2.4: Zariski Topology**

The **Zariski topology** on  $\mathbb{A}_k^n$  is defined by taking the open subsets to be the complements of the algebraic sets.

To verify this is a valid topology, we must show that the empty set and the whole space are closed, and that finite unions and arbitrary intersections of closed sets are also closed.

### 1.3 Quasi-Affine Varieties

## Varieties and Irreducibility

### Definition 1.3.1: Reducible and Irreducible Sets

A non-empty topological space  $Y$  is **reducible** if it can be written as the union of two proper closed subsets,  $Y = Y_1 \cup Y_2$ , where  $Y_1 \subsetneq Y$  and  $Y_2 \subsetneq Y$ . A non-empty topological space is **irreducible** if it is not reducible. By convention, the empty set is considered reducible.

If a space  $Y$  is reducible,  $Y = Y_1 \cup Y_2$ , we can study its properties by studying its simpler components  $Y_1$  and  $Y_2$ . If these are also reducible, we can decompose them further. E.g.,  $\mathbb{A}_{\mathbb{C}}^1$  is irreducible.

[Say,  $\mathbb{A}_{\mathbb{C}}^1 = Y_1 \cup Y_2 := Z(I_1) \cup Z(I_2) = Z(I_1 I_2) \implies I_1 I_2 = \langle 0 \rangle \implies I_1 = \langle 0 \rangle$  or  $I_2 = \langle 0 \rangle$ .]

## Affine and Quasi-affine Varieties

### Definition 1.3.2: Affine Variety

An **affine variety** is an irreducible closed subset of  $\mathbb{A}^n$ .

### Definition 1.3.3: Quasi-affine Variety

A **quasi-affine variety** is an open subset of an affine variety.

### Example 1.3.1:

1.  $Y = Z(x_1 x_2) \subset \mathbb{A}^2$ . This is the union of the two coordinate axes:  $Y = Z(x_1) \cup Z(x_2)$ . Both  $Z(x_1)$  (the  $x_2$ -axis) and  $Z(x_2)$  (the  $x_1$ -axis) are proper closed subsets of  $Y$ . Therefore,  $Y$  is reducible and is not an affine variety.
2.  $Y = Z(x_1^2) \subset \mathbb{A}^2$ . Any point  $(a_1, a_2)$  where  $a_1^2 = 0$  must have  $a_1 = 0$ . Thus,  $Z(x_1^2) = Z(x_1)$ , which is the  $x_2$ -axis. This is an irreducible set (isomorphic to  $\mathbb{A}^1$ ), so it is an affine variety.
3.  $Z(x_1^2) \setminus Z(x_1^2, x_2)$  is quasi-affine (The reason for it to be quasi-affine is that it is an open subset of the affine variety  $Z(x_1^2)$ ).

## The Nullstellensatz and the Algebra-Geometry Dictionary

The main goal is to prove one of the most fundamental theorems in algebraic geometry, Hilbert's Nullstellensatz. For an ideal  $J$  in a polynomial ring  $A = k[x_1, \dots, x_n]$  (where  $k$  is an algebraically closed field like  $\mathbb{C}$ ), the theorem states that the ideal of polynomials vanishing on the zero set of  $J$  is precisely the radical of  $J$ .

In mathematical notation:

$$I(Z(J)) = \sqrt{J}$$

Where:

- **$Z(J)$  (The Zero Set):** The set of all points  $(a_1, \dots, a_n) \in k^n$  where every polynomial in the ideal  $J$  evaluates to zero. This is the **geometric** object.
- **$I(V)$  (The Ideal of a Set):** The set of all polynomials that evaluate to zero for every point in the set  $V$ .
- **$\sqrt{J}$  (The Radical Ideal):** The set of all polynomials  $g$  such that some power of  $g$  is in  $J$ . That is,  $g \in \sqrt{J}$  if  $g^e \in J$  for some positive integer  $e$ . This is the **algebraic** object.

The proof relies on a simpler version of the theorem, known as the Weak Nullstellensatz.

## The Foundation: Weak Nullstellensatz

### Theorem (Weak Nullstellensatz)

Let  $k$  be an algebraically closed field and  $J$  be an ideal in  $A = k[x_1, \dots, x_n]$ . The zero set  $Z(J)$  is empty if and only if  $J$  is the entire ring  $A$  (i.e.,  $1 \in J$ ).

**Proof Sketch (for  $Z(J) = \emptyset \implies J = A$ ):**

1. **Assumption:** Assume  $Z(J) = \emptyset$ , but for the sake of contradiction, assume  $J$  is a proper ideal ( $J \neq A$ ).
2. **Find a Maximal Ideal:** Since  $J$  is a proper ideal, it must be contained within some maximal ideal  $\mathfrak{m}$ , so  $J \subseteq \mathfrak{m}$ .
3. **From Ideals to Zero Sets:** This inclusion implies  $Z(\mathfrak{m}) \subseteq Z(J)$ . If we can show that  $Z(\mathfrak{m}) \neq \emptyset$ , we will have a contradiction.
4. **The Key Insight (Zariski's Lemma):**
  - Since  $\mathfrak{m}$  is a maximal ideal, the quotient ring  $A/\mathfrak{m}$  is a field.
  - This field is a finitely generated  $k$ -algebra, and it contains  $k$ .
  - By Zariski's Lemma, this implies  $A/\mathfrak{m}$  is a finite algebraic extension of  $k$ .
  - **Because  $k$  is algebraically closed**, the only such extension is  $k$  itself.
  - Therefore, we must have an isomorphism  $A/\mathfrak{m} \cong k$ .
5. **Finding a Point:** This isomorphism gives a surjective homomorphism  $\phi : A \rightarrow k$  with  $\ker(\phi) = \mathfrak{m}$ . Let  $a_i = \phi(x_i) \in k$ . This defines a point  $P = (a_1, \dots, a_n) \in k^n$ . For any polynomial  $f \in \mathfrak{m}$ , we have  $\phi(f) = f(a_1, \dots, a_n) = 0$ . This means the point  $P$  is in the zero set of  $\mathfrak{m}$ . Thus,  $Z(\mathfrak{m}) \neq \emptyset$ .

6. **Contradiction:** We have found a point in  $Z(\mathfrak{m}) \subseteq Z(J)$ , which contradicts our initial assumption that  $Z(J)$  is empty. Therefore, the assumption that  $J$  was a proper ideal must be false, so  $J = A$ .

**Proof of the Full Nullstellensatz:**  $I(Z(J)) = \sqrt{J}$

**Part A: The "Easy" Direction ( $\sqrt{J} \subseteq I(Z(J))$ )**

- Let  $g \in \sqrt{J}$ . By definition, this means  $g^e \in J$  for some integer  $e \geq 1$ .
- Let  $P \in Z(J)$ . By definition,  $f(P) = 0$  for all  $f \in J$ .
- Since  $g^e \in J$ , we must have  $g^e(P) = (g(P))^e = 0$ .
- Since  $g(P)$  is an element of the field  $k$ , this implies  $g(P) = 0$ .
- Because this holds for every point  $P \in Z(J)$ ,  $g$  vanishes on  $Z(J)$ . By definition, this means  $g \in I(Z(J))$ .

**Part B: The "Hard" Direction ( $I(Z(J)) \subseteq \sqrt{J}$ )**

This proof uses the famous **Rabinowitsch trick**.

1. **Setup:** Let  $g \in I(Z(J))$ . This means  $g$  vanishes everywhere on  $Z(J)$ . We want to show that  $g \in \sqrt{J}$ .
2. **The Trick:** Introduce a new variable,  $y$ , and consider the polynomial ring  $A' = A[y] = k[x_1, \dots, x_n, y]$ . In this new ring, define a new ideal:

$$J' = JA' + \langle 1 - gy \rangle$$

3. **Zero Set of  $J'$ :** Consider the zero set  $Z(J') \subseteq k^{n+1}$ . A point  $(P, b) \in k^{n+1}$  is in  $Z(J')$  if  $f(P) = 0$  for all  $f \in J$  and  $1 - g(P)b = 0$ .
4. The first condition means  $P \in Z(J)$ . But by our initial assumption,  $g \in I(Z(J))$ , so  $g(P) = 0$ . Substituting this into the second condition gives  $1 - (0) \cdot b = 0$ , which simplifies to the contradiction  $1 = 0$ .
5. **Apply Weak Nullstellensatz:** Since there are no points in  $Z(J')$ , we have  $Z(J') = \emptyset$ . By the Weak Nullstellensatz, the ideal  $J'$  must be the entire ring  $A'$ . This means  $1 \in J'$ .

**6. Unpack the Algebra:** Since  $1 \in J'$ , we can write 1 as a linear combination of its generators. Let  $J = \langle f_1, \dots, f_m \rangle$ .

$$1 = \sum_{i=1}^m a_i(x, y) f_i(x) + a_0(x, y)(1 - gy)$$

for some polynomials  $a_0, a_i \in A'$ .

**7. Final Step:** In the field of fractions of  $A'$ , we can make the formal substitution  $y = 1/g$ :

$$1 = \sum_{i=1}^m a_i(x, 1/g) f_i(x)$$

The terms  $a_i(x, 1/g)$  are rational functions in  $g$ . To clear the denominators, we multiply the entire equation by a sufficiently large power of  $g$ , say  $g^e$ :

$$g^e = \sum_{i=1}^m \underbrace{(g^e \cdot a_i(x, 1/g))}_{\text{This is a polynomial in } A} \cdot f_i(x)$$

This shows that  $g^e$  is a linear combination of the generators of  $J$ , which means  $g^e \in J$ .

**8. Conclusion:** By the definition of the radical ideal, if  $g^e \in J$ , then  $g \in \sqrt{J}$ .

## Summary: The Algebra-Geometry Dictionary

The Nullstellensatz establishes a profound duality between geometry and algebra.

- There is a **one-to-one, order-reversing correspondence** between **algebraic sets** in  $k^n$  (the geometric side) and **radical ideals** in  $k[x_1, \dots, x_n]$  (the algebraic side).
- The maps that form this correspondence are  $V \mapsto I(V)$  and  $J \mapsto Z(J)$ .
- This allows geometric properties of sets to be studied using the algebraic properties of their corresponding ideals, and vice versa. For example, an irreducible algebraic set corresponds to a prime ideal.

## 1.4 The Correspondence

The Nullstellensatz establishes a fundamental, order-reversing correspondence between geometry (algebraic sets) and algebra (ideals).

**Corollary 1.4.1: Ideal-Variety Correspondence** There is a one-to-one, inclusion-reversing correspondence between:

$$\{\text{algebraic sets in } \mathbb{A}^n\} \longleftrightarrow \{\text{radical ideals in } A\}$$

Given by the maps  $\mathcal{I}$  and  $\mathcal{Z}$ .

Under this correspondence, we can ask what properties of an algebraic set correspond to what properties of its ideal.

**Proposition 1.4.1: Affine Varieties and Prime Ideals**

An algebraic set  $Y$  is an affine variety (i.e., is irreducible) if and only if its ideal  $\mathcal{I}(Y)$  is a prime ideal.

*Proof.* ( $\Rightarrow$ ) Let  $Y$  be an affine variety, so it is irreducible. We know  $I = \mathcal{I}(Y)$  is a radical ideal. Suppose  $fg \in I$  for some  $f, g \in A$ . Then  $Y \subseteq \mathcal{Z}(fg) = \mathcal{Z}(f) \cup \mathcal{Z}(g)$ . Let  $Y_1 = Y \cap \mathcal{Z}(f)$  and  $Y_2 = Y \cap \mathcal{Z}(g)$ . These are closed sets in  $Y$ . We have  $Y = Y_1 \cup Y_2$ . Since  $Y$  is irreducible, either  $Y = Y_1$  or  $Y = Y_2$ . If  $Y = Y_1$ , then  $Y \subseteq \mathcal{Z}(f)$ , which means  $f$  vanishes on all of  $Y$ . Thus,  $f \in \mathcal{I}(Y) = I$ . If  $Y = Y_2$ , then  $Y \subseteq \mathcal{Z}(g)$ , which means  $g \in \mathcal{I}(Y) = I$ . In either case, we have shown that if  $fg \in I$ , then  $f \in I$  or  $g \in I$ . This is the definition of a prime ideal.

( $\Leftarrow$ ) Let  $I$  be a prime ideal. A prime ideal is always radical, so  $Y = \mathcal{Z}(I)$  is an algebraic set with  $\mathcal{I}(Y) = I$ . Suppose  $Y = Y_1 \cup Y_2$  where  $Y_1, Y_2$  are closed subsets of  $Y$ . Then  $I = \mathcal{I}(Y) = \mathcal{I}(Y_1 \cup Y_2) = \mathcal{I}(Y_1) \cap \mathcal{I}(Y_2)$ . Assume for contradiction that  $Y_1 \neq Y$  and  $Y_2 \neq Y$ . Then  $\mathcal{I}(Y_1) \supsetneq I$  and  $\mathcal{I}(Y_2) \supsetneq I$ . So we can pick  $f \in \mathcal{I}(Y_1) \setminus I$  and  $g \in \mathcal{I}(Y_2) \setminus I$ . The product  $fg$  vanishes on  $Y_1$  (since  $f$  does) and on  $Y_2$  (since  $g$  does). So  $fg$  vanishes on  $Y_1 \cup Y_2 = Y$ . This means  $fg \in \mathcal{I}(Y) = I$ . But since  $I$  is prime, this implies  $f \in I$  or  $g \in I$ , which is a contradiction. Therefore, our assumption was false, and either  $Y_1 = Y$  or  $Y_2 = Y$ . This shows  $Y$  is irreducible.  $\square$

This correspondence can be refined further. The smallest non-empty algebraic sets are single points.

**Proposition 1.4.0.1.** The points of  $\mathbb{A}^n$  are in one-to-one correspondence with the maximal ideals of  $A$ .

*Proof.* Let  $P = (a_1, \dots, a_n) \in \mathbb{A}^n$ . Consider the ideal  $m_P = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ . The quotient ring  $A/m_P$  is isomorphic to  $\mathbb{k}$  via the evaluation map  $f \mapsto f(P)$ . Since  $\mathbb{k}$  is a field,  $m_P$  is a maximal ideal. Conversely, let  $M$  be a maximal ideal of  $A$ . By the proof of the Weak Nullstellensatz, we know that  $\mathcal{Z}(M)$  is a single point  $P = (a_1, \dots, a_n)$  and that  $M$  is the ideal of all functions vanishing at that point, which is precisely  $m_P$ . So  $\mathcal{I}(P) = m_P$ .  $\square$

### Summary of the Correspondence

Geometry (Subsets of $\mathbb{A}^n$ )	Algebra (Ideals of $A = \mathbb{k}[x_1, \dots, x_n]$ )
Affine space $\mathbb{A}^n$	Zero ideal $\langle 0 \rangle$
Empty set $\emptyset$	The whole ring $A$
Algebraic Set	Radical Ideal
Affine Variety (irreducible)	Prime Ideal
Point $P \in \mathbb{A}^n$	Maximal Ideal

## 1.5 Functions on Varieties

### Definition 1.5.1: Coordinate Ring

Let  $Y \subseteq \mathbb{A}^n$  be a closed set (an algebraic set). The **coordinate ring** of  $Y$ , denoted  $A(Y)$ , is the quotient ring

$$A(Y) := A/\mathcal{I}(Y) = \mathbb{k}[x_1, \dots, x_n]/\mathcal{I}(Y)$$

The elements of  $A(Y)$  can be thought of as equivalence classes of polynomials, where two polynomials are equivalent if they agree on all points of  $Y$ . Thus,  $A(Y)$  is the ring of polynomial functions from  $Y$  to  $\mathbb{k}$ .

### Remark 1.5.1: Important Special Cases

- $A(\mathbb{A}^n) = A/\mathcal{I}(\mathbb{A}^n) = A/\langle 0 \rangle \cong A = \mathbb{k}[x_1, \dots, x_n]$ .
- If  $Y$  is an affine variety, then  $\mathcal{I}(Y)$  is a prime ideal. Therefore, the coordinate ring  $A(Y) = A/\mathcal{I}(Y)$  is an integral domain.

**Example 1.5.1:** Let  $Y = \mathcal{Z}(f)$  where  $f$  is an irreducible polynomial in  $A$ . Since  $A$  is a Unique Factorization Domain, the ideal  $\langle f \rangle$  is prime. Thus  $Y$  is an affine variety. Its coordinate ring is  $A(Y) = A/\mathcal{I}(Y) = A/\sqrt{\langle f \rangle} = A/\langle f \rangle$ .

### Definition 1.5.2: Field of Fractions and Function Field

Let  $B$  be an integral domain. The **field of fractions** of  $B$ , denoted  $\text{Frac}(B)$ , is the set of formal fractions  $\{a/b \mid a, b \in B, b \neq 0\}$ , with the usual rules for addition and multiplication. If  $Y$  is an affine variety, its coordinate ring  $A(Y)$  is an integral domain. The **function field** of  $Y$ , denoted  $\mathbb{k}(Y)$ , is the field of fractions of  $A(Y)$ .

$$\mathbb{k}(Y) := \text{Frac}(A(Y))$$

Its elements are the rational functions on  $Y$ .

**Exercise** Every closed set  $Y \subseteq \mathbb{A}^n$  can be expressed as a finite union  $Y = \bigcup_{i=1}^m Y_i$  of affine varieties  $Y_i$ . If we require that  $Y_i \not\subseteq Y_j$  for  $i \neq j$ , this decomposition is unique up to reordering. The  $Y_i$  are called the irreducible components of  $Y$ .

*Proof.* This is a standard result for Noetherian topological spaces. The ring  $A = \mathbb{k}[x_1, \dots, x_n]$  is a Noetherian ring (by Hilbert's Basis Theorem). This implies that any descending chain of closed sets  $Y_1 \supseteq Y_2 \supseteq \dots$  in  $\mathbb{A}^n$  must eventually stabilize. If  $Y$  is reducible, we can write  $Y = Y_1 \cup Y_2$  with  $Y_1, Y_2$  proper closed subsets. If either is reducible, we decompose it further. The Noetherian property guarantees this process must terminate in a finite number of steps, leaving a decomposition into irreducible closed sets (affine varieties). Uniqueness is proven by showing that any irreducible component in one decomposition must be equal to an irreducible component in another.  $\square$

**Exercise** In  $A = \mathbb{k}[x_1, \dots, x_n]$ , every ideal  $I \triangleleft A$  is finitely generated.

*Proof.* This is a direct statement of the **Hilbert Basis Theorem**. The proof is a classic result in commutative algebra. It proceeds by induction on the number of variables, showing that if a ring  $R$  is Noetherian, then the polynomial ring  $R[x]$  is also Noetherian. Since a field  $\mathbb{k}$  is trivially Noetherian, it follows that  $\mathbb{k}[x_1]$  is Noetherian, and by induction  $\mathbb{k}[x_1, \dots, x_n]$  is Noetherian. Being a Noetherian ring means every ideal is finitely generated.  $\square$

**Exercise** Any radical ideal  $I$  can be expressed as a finite intersubsection  $I = \bigcap_{i=1}^m P_i$  where the  $P_i$  are prime ideals.

*Proof.* This is the algebraic counterpart to the first exercise. Let  $Y = \mathcal{Z}(I)$ . From Exercise 1, we can write  $Y = \bigcup_{i=1}^m Y_i$  where  $Y_i$  are affine varieties. Taking the ideal of both sides, we get:

$$I = \mathcal{I}(Y) = \mathcal{I}\left(\bigcup_{i=1}^m Y_i\right) = \bigcap_{i=1}^m \mathcal{I}(Y_i)$$

Let  $P_i = \mathcal{I}(Y_i)$ . Since each  $Y_i$  is an affine variety, each  $P_i$  is a prime ideal. This gives the desired decomposition .  $\square$

## 1.6 Dimension of Affine Varieties

### Intuitive and Formal Definitions

Intuitively, we are familiar with the concept of dimension from linear algebra. For example, we know that:

- $\dim(\{\bar{0}\}) = 0$

We wish to establish a rigorous definition for the dimension of algebraic sets.

**Definition 1.6.1: Dimension of an Affine Variety**

The **dimension** of an affine variety (AV)  $Y$ , denoted  $\dim(Y)$ , is the maximum integer  $n \in \mathbb{N}$  such that there exists a chain of distinct irreducible algebraic subsets (subvarieties) of the form:

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n = Y$$

where  $Z_0$  is a point  $\{P\}$ .

**Example 1.6.1:** Consider the affine line  $\mathbb{A}_k^1$ . Let  $A = k[x_1]$ . Any prime ideal in  $A$  is of the form  $\langle 0 \rangle$  or  $\langle x_1 - \alpha \rangle$  for some  $\alpha \in k$ . This gives rise to the maximal chain of varieties:

$$\mathcal{Z}(\langle x_1 - \alpha \rangle) \subsetneq \mathcal{Z}(\langle 0 \rangle)$$

which corresponds to:

$$\{\alpha\} \subsetneq \mathbb{A}_k^1$$

This is a chain of length 1. Thus,  $\dim(\mathbb{A}_k^1) = 1$ .

**Example 1.6.2:** Consider the affine plane  $\mathbb{A}_k^2$ . We can construct the chain:

$$\mathcal{Z}(\langle x_1, x_2 \rangle) \subsetneq \mathcal{Z}(\langle x_1 \rangle) \subsetneq \mathcal{Z}(\langle 0 \rangle)$$

which corresponds to:

$$\{(0, 0)\} \subsetneq \mathbb{A}_k^1 \times \{0\} \subsetneq \mathbb{A}_k^2$$

This is a chain of length 2, which implies that  $\dim(\mathbb{A}_k^2) \geq 2$ . In fact, it can be shown that  $\dim(\mathbb{A}_k^2) = 2$ .

**Definition 1.6.2: Affine Curve**

An affine variety of dimension 1 is called an **affine curve**.

**Theorem 1.6.1: Hypersurfaces**

An affine variety  $Y$  in  $\mathbb{A}_k^n$  has dimension  $n - 1$  if and only if  $Y = \mathcal{Z}(f)$  for some non-constant, irreducible polynomial  $f \in k[x_1, \dots, x_n]$ . Such a variety is called a hypersurface.

*Proof.* Let  $Y = \mathcal{Z}(f_1, \dots, f_m)$ . The core idea is to show that adding a polynomial to the ideal reduces the dimension. Specifically, one can show that if  $Y_1 = \mathcal{Z}(f_1)$  is a variety, then  $\dim(\mathcal{Z}(f_1, f_2)) < \dim(\mathcal{Z}(f_1))$ , provided  $\mathcal{Z}(f_2)$  does not contain  $Y_1$ . Since the dimension cannot be larger than  $n$ , a single irreducible polynomial defines a variety of dimension  $n - 1$ .  $\square$

**Example 1.6.3:** A curve  $Y$  in  $\mathbb{A}_k^2$  is the zero set  $Y = \mathcal{Z}(f(x_1, x_2))$  for an irreducible polynomial  $f \in k[x_1, x_2]$ .

**Remark 1.6.1:** The set  $Y = \mathcal{Z}(x_1, x_2)$  in  $\mathbb{A}_k^2$  is the point  $\{(0, 0)\}$ , which has dimension 0, not 1. It is not a curve because it cannot be defined by a single polynomial.

## Dimension and Transcendence Degree

There is a more algebraic and often more computable way to define dimension using the concept of transcendence degree.

### Theorem 1.6.2: Dimension and Transcendence Degree

The dimension of an affine variety  $Y$  is equal to the transcendence degree of its coordinate ring  $A(Y)$  over the field  $k$ .

$$\dim(Y) = \text{trdeg}_k A(Y)$$

### Definition 1.6.3: Transcendence Degree

Let  $B$  be a domain that is a  $k$ -algebra. The **transcendence degree** of the field of fractions  $k(B)$  over  $k$ , denoted  $\text{trdeg}_k(B)$ , is the maximum number of algebraically independent elements  $y_1, \dots, y_t \in B$  over  $k$ . A set of elements  $\{y_1, \dots, y_t\}$  is **algebraically independent** over  $k$  if there is no non-zero polynomial  $P \in k[Y_1, \dots, Y_t]$  such that  $P(y_1, \dots, y_t) = 0$ . The elements  $y_1, \dots, y_t$  form a **transcendence basis** if  $k(B)$  is a finite (algebraic) extension of the field  $k(y_1, \dots, y_t)$ .

### Example 1.6.4:

1.  $\text{trdeg}_k k = 0$ .
2.  $\text{trdeg}_k k[x] = 1$ . The element  $x$  is a transcendence basis.
3.  $\text{trdeg}_k k[x, y] = 2$ . The elements  $x, y$  are a transcendence basis.
4. Let  $B = k[x, y]/\langle y^2 - x^3 \rangle$ . In this ring,  $x$  and  $y$  are algebraically dependent. The element  $\bar{x}$  (the image of  $x$  in  $B$ ) is a transcendence basis. Thus,  $\text{trdeg}_k(B) = 1$ .

**Example 1.6.5:** The field extension  $\mathbb{Q} \subset \mathbb{Q}(\mathbb{P})$  is a transcendental extension. The field extension  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$  is an algebraic extension.

*Proof.* Let  $d = \dim(Y)$ . Then there exists a maximal chain of affine varieties in  $Y$ :

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_d = Y$$

where  $Z_i = \mathcal{Z}(\mathfrak{p}_i)$  for prime ideals  $\mathfrak{p}_i$ . This corresponds to a reversed chain of prime ideals in the coordinate ring  $A(Y)$ :

$$\mathfrak{p}_d \subsetneq \mathfrak{p}_{d-1} \subsetneq \cdots \subsetneq \mathfrak{p}_0$$

where  $\mathfrak{p}_d = \langle 0 \rangle$  and  $\mathfrak{p}_0$  is a maximal ideal. This in turn gives us a chain of field extensions of the fields of fractions:

$$k(A(Y)/\mathfrak{p}_0) \subsetneq k(A(Y)/\mathfrak{p}_1) \subsetneq \cdots \subsetneq k(A(Y)/\mathfrak{p}_d) = k(Y)$$

This is a maximal chain of field extensions within  $k(Y)$ . It is a result from commutative algebra that the length of such a chain is equal to the transcendence degree. Each field extension in this chain can be shown to have a transcendence degree of 1 relative to the previous one. Therefore,  $\text{trdeg}_k k(A(Y)) = d$ .  $\square$

## Fundamental Computational Problems

Given a set of polynomials  $f_1, \dots, f_m$  in  $A = k[x_1, \dots, x_n]$ , let  $\mathfrak{a} = \langle f_1, \dots, f_m \rangle$ . We can ask several fundamental questions:

1. **Emptiness Test:** Is the algebraic set  $\mathcal{Z}(\mathfrak{a})$  empty? This is equivalent to asking if  $1 \in \mathfrak{a}$  (Hilbert's Nullstellensatz). Are there fast algorithms (polynomial time in  $n, m, \deg(f_i)$ , etc.) for this?
2. **Dimension Computation:** What is  $\dim(\mathcal{Z}(\mathfrak{a}))$ ? The dimension can range from  $-1$  (for the empty set) to  $n$ .
3. **Finding Points:** Find a root of the system  $f_1 = \cdots = f_m = 0$ .
4. **Radical Computation:** Compute the radical of the ideal,  $\sqrt{\mathfrak{a}}$ .
5. **Irreducibility Test:** Is  $\mathcal{Z}(\mathfrak{a})$  an affine variety (i.e., is  $\sqrt{\mathfrak{a}}$  a prime ideal)? If not, find its decomposition into irreducible components, i.e., find prime ideals  $\mathfrak{p}_1, \mathfrak{p}_2$  such that  $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathfrak{p}_1) \cup \mathcal{Z}(\mathfrak{p}_2)$ .

## 1.7 Projective Varieties

### Motivation

The affine space  $\mathbb{A}^n$  is not "complete" in a certain sense (e.g., parallel lines never meet). Projective space is a natural compactification of affine space. The key idea is to work with objects that are invariant under scaling. If  $(a_1, \dots, a_n)$  is a root of a system of equations, we want to consider all points on the line through the origin and  $(a_1, \dots, a_n)$ , i.e., all points  $(ca_1, \dots, ca_n)$  for  $c \in k^*$ , as equivalent. This leads to the study of homogeneous polynomials.

A polynomial  $f$  is **homogeneous** if all its monomials have the same total degree.

- $f = x^2 - xy + y^2$  is homogeneous of degree 2.
- $g = x^2 + y^3$  is not homogeneous.

For a homogeneous polynomial  $f$  of degree  $d$ , we have the property:

$$f(\lambda x_1, \dots, \lambda x_n) = \lambda^d f(x_1, \dots, x_n)$$

This means that if  $f(a_1, \dots, a_n) = 0$ , then  $f(\lambda a_1, \dots, \lambda a_n) = 0$  for any  $\lambda \in k$ . The zero sets of homogeneous polynomials are unions of lines through the origin.

## Projective Space

### Definition 1.7.1: Projective n-space

Consider the set  $(\mathbb{A}^{n+1})^* = \mathbb{A}^{n+1} \setminus \{(0, \dots, 0)\}$ . We define an equivalence relation  $\sim$  on this set: For  $\bar{a} = (a_0, \dots, a_n)$  and  $\bar{b} = (b_0, \dots, b_n)$  in  $(\mathbb{A}^{n+1})^*$ , we say  $\bar{a} \sim \bar{b}$  if there exists a scalar  $\lambda \in k^*$  such that  $\bar{a} = \lambda \cdot \bar{b}$ .

**Projective n-space** over  $k$ , denoted  $\mathbb{P}_k^n$ , is the set of equivalence classes:

$$\mathbb{P}_k^n := (\mathbb{A}_k^{n+1})^*/\sim$$

The equivalence class of a point  $(a_0, \dots, a_n)$  is denoted by  $(a_0 : a_1 : \dots : a_n)$  and these are called **homogeneous coordinates**.

Geometrically,  $\mathbb{P}_k^n$  is the space of all lines passing through the origin in  $\mathbb{A}_k^{n+1}$ .

**Example 1.7.1:** If  $k = \mathbb{F}_p$  (the finite field with  $p$  elements), then  $|\mathbb{A}_k^{n+1}| = p^{n+1}$ . Each equivalence class in  $(\mathbb{A}_k^{n+1})^*$  has  $p - 1$  elements. Therefore, the number of points in projective space is:

$$|\mathbb{P}_k^n| = \frac{p^{n+1} - 1}{p - 1}$$

**Example 1.7.2:** In  $\mathbb{P}_{\mathbb{C}}^1$ , the points  $(2, 1 - i)$  and  $(1 + i, 1)$  are the same, because  $(1 + i)(1 - i) = 2$ . So  $(2, 1 - i) = (1 - i)(1 + i, 1)$ . Thus  $(2 : 1 - i) = (1 + i : 1)$ .

## Homogeneous Ideals and Projective Varieties

What is the algebraic analogue of  $\mathbb{P}_k^n$ ? We work with the polynomial ring in  $n + 1$  variables,  $S = k[x_0, \dots, x_n]$ . This ring has a natural **grading**:

$$S = \bigoplus_{d \geq 0} S_d$$

where  $S_d$  is the  $k$ -vector space of all homogeneous polynomials of degree  $d$ . This grading respects multiplication: for any  $d, e \in \mathbb{N}$ , if  $f \in S_d$  and  $g \in S_e$ , then  $f \cdot g \in S_{d+e}$ .

### Definition 1.7.2: Homogeneous Ideal

An ideal  $I \subseteq S$  is called **homogeneous** if for every polynomial  $f \in I$ , all of its homogeneous components are also in  $I$ .

### Proposition 1.7.1: Characterizations of Homogeneous Ideals

The following are equivalent for an ideal  $I \subseteq S$ :

1.  $I$  is homogeneous.
2.  $I = \bigoplus_{d \geq 0} (I \cap S_d)$ .
3.  $I$  can be generated by a set of homogeneous polynomials.

**Example 1.7.3: Counter-example** The ideal  $I = \langle x_1^2 + x_2 \rangle$  in  $k[x_1, x_2]$  is not homogeneous. Its generator is not homogeneous. We have  $I \cap S_1 = \{0\}$  and  $I \cap S_2$  does not contain  $x_1^2$  (only multiples of  $x_1^2 + x_2$ ), so  $I \neq (I \cap S_1) \oplus (I \cap S_2) \oplus \dots$ .

### Proposition 1.7.2: Operations on Homogeneous Ideals

The sum, product, intersubsection, and radical of homogeneous ideals are homogeneous.

### Definition 1.7.3: Projective Variety

Let  $T$  be a set of homogeneous polynomials in  $S = k[x_0, \dots, x_n]$ . The **projective zero set** of  $T$  is

$$\mathcal{Z}_p(T) := \{P \in \mathbb{P}_k^n \mid \forall f \in T, f(P) = 0\}$$

Note that the condition  $f(P) = 0$  is well-defined for homogeneous polynomials because if  $f(a_0, \dots, a_n) = 0$ , then  $f(\lambda a_0, \dots, \lambda a_n) = \lambda^{\deg(f)} f(a_0, \dots, a_n) = 0$ . A subset of  $\mathbb{P}_k^n$  is a **projective algebraic set** if it is of the form  $\mathcal{Z}_p(I)$  for some homogeneous ideal  $I \subseteq S$ .

**Example 1.7.4:** In  $\mathbb{P}_{\mathbb{C}}^1$ , with coordinates  $(x_0 : x_1)$ :

- $\mathcal{Z}_p(x_0^2 - x_1^2) = \mathcal{Z}_p((x_0 - x_1)(x_0 + x_1)) = \{(1 : 1), (1 : -1)\}$ .
- $\mathcal{Z}_p(x_0^2) = \{(0 : 1)\}$ .

## Projective Varieties and the Zariski Topology

Let  $k$  be an algebraically closed field ( $k = \bar{k}$ ). Let  $S = k[x_0, \dots, x_n]$  be the polynomial ring in  $n + 1$  variables. We refer to the elements of  $S$  as polynomials, and if all monomials

in a polynomial have the same total degree, we call it a homogeneous polynomial.

#### Definition 1.7.4: Projective Algebraic Set

A subset  $Y \subseteq \mathbb{P}^n$  is called a **closed set** (or an **algebraic set**) if there exists a set of homogeneous polynomials  $T \subseteq S$  such that  $Y$  is the zero locus of  $T$ . We denote this as:

$$Y = \mathcal{Z}(T) = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all } f \in T\}$$

An **open set** in  $\mathbb{P}^n$  is the complement of a closed set, i.e., a set of the form  $\mathbb{P}^n \setminus Y$  where  $Y$  is closed.

**Remark 1.7.1: Zariski Topology** The family of open sets defined above forms a topology on  $\mathbb{P}^n$ , which is known as the **Zariski topology**.

#### Definition 1.7.5: Projective Variety

A **projective variety** is an irreducible closed subset of  $\mathbb{P}^n$ . A topological space is irreducible if it cannot be written as the union of two proper closed subsets.

#### Definition 1.7.6: Quasi-Projective Variety

A **quasi-projective variety** is an open subset of a projective variety.

**Remark 1.7.2: Dimension of Projective and Quasi-Projective Varieties** The dimension of a projective or quasi-projective variety is defined, similarly to the affine case, as the supremum of lengths of chains of irreducible closed subsets.

$$\dim(Y) = \sup\{m \mid \emptyset \neq Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_m \subseteq Y, \text{ where each } Z_i \text{ is irreducible and closed in } Y\}$$

#### Example 1.7.5:

1. In  $\mathbb{P}_{\mathbb{C}}^1$ , consider the ideal  $T = \langle x_0^2 \rangle$ . The zero set  $\mathcal{Z}(x_0^2) = \mathcal{Z}(x_0)$  is the point  $[0 : 1]$ . A single point is an irreducible closed set, so it is a projective variety of dimension 0.
2. In  $\mathbb{P}_{\mathbb{C}}^1$ , consider  $T = \langle x_0^2 - x_1^2 \rangle$ . Since  $x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1)$ , the zero set is  $\mathcal{Z}(x_0 - x_1) \cup \mathcal{Z}(x_0 + x_1)$ , which corresponds to the two distinct points  $\{[1 : 1], [1 : -1]\}$ . This is a closed set, but it is not irreducible. Therefore, it is a projective algebraic set, but not a projective variety.
3. In  $\mathbb{P}_{\mathbb{C}}^2$ , consider  $T = \langle x_0^2, x_1 \rangle$ . The zero set  $\mathcal{Z}(x_0^2, x_1)$  consists of points  $[a_0 : a_1 : a_2]$  where  $a_0^2 = 0$  and  $a_1 = 0$ . This implies  $a_0 = 0$  and  $a_1 = 0$ , so the only point is  $[0 : 0 : 1]$ . This is a projective variety. *[Note: The original document calls this a "curve!", which is incorrect; it is a single point and thus 0-dimensional.]*

## Ideals and Coordinate Rings

Just as there is a correspondence between algebraic sets in affine space and ideals, a similar relationship exists in projective space, with the condition that all polynomials and ideals must be homogeneous.

### Definition 1.7.7: Homogeneous Ideal

For a closed set  $Y \subseteq \mathbb{P}^n$ , the **homogeneous ideal of  $Y$** , denoted  $\mathcal{I}(Y)$ , is the ideal generated by all homogeneous polynomials in  $S$  that vanish on every point in  $Y$ .

$$\mathcal{I}(Y) = \langle f \in S \mid f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in Y \rangle$$

### Definition 1.7.8: Homogeneous Coordinate Ring

The **homogeneous coordinate ring** of a closed set  $Y \subseteq \mathbb{P}^n$  is the quotient ring:

$$S(Y) := S/\mathcal{I}(Y)$$

**Remark 1.7.3: Projective Nullstellensatz** The diagram on page 3 of the notes illustrates the fundamental correspondence of the Projective Nullstellensatz for an algebraically closed field  $k$ . Let  $S_+ = \langle x_0, \dots, x_n \rangle$  be the irrelevant ideal.

Geometry in $\mathbb{P}^n$		Algebra in $S = k[x_0, \dots, x_n]$
Closed subsets of $\mathbb{P}^n$	$\longleftrightarrow$	Radical homogeneous ideals $\neq S_+$
$\cup$		$\cap$
$\cap$		$+$
Irreducible closed subsets (Projective Varieties)	$\longleftrightarrow$	Homogeneous prime ideals $\neq S_+$
Points	$\longleftrightarrow$	Homogeneous prime ideals maximal among proper homogeneous ideals other than $S_+$

The maps are given by  $Y \mapsto \mathcal{I}(Y)$  and  $I \mapsto \mathcal{Z}(I)$ .

## Affine Covering of Projective Space

A powerful technique for studying projective space is to cover it with open sets that are themselves affine spaces.

### Proposition 1.7.3: Affine Covering of Projective Space

Projective  $n$ -space,  $\mathbb{P}^n$ , has an open covering by  $n + 1$  sets, each of which is homeomorphic to affine  $n$ -space,  $\mathbb{A}^n$ .

*Proof.* For each  $i \in \{0, 1, \dots, n\}$ , define the open set  $U_i$  as:

$$U_i = \{[a_0 : \dots : a_n] \in \mathbb{P}^n \mid a_i \neq 0\}$$

Since a point in  $\mathbb{P}^n$  must have at least one non-zero coordinate, it is clear that  $\mathbb{P}^n = \bigcup_{i=0}^n U_i$ .

We define a map  $\varphi_i : U_i \rightarrow \mathbb{A}^n$  by dehomogenizing with respect to the  $i$ -th coordinate:

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

This map is well-defined because the ratios are independent of the choice of homogeneous coordinates. One can show that  $\varphi_i$  is a bijection and a homeomorphism, meaning it establishes a one-to-one correspondence between the open sets of  $U_i$  (in the subspace topology) and the open sets of  $\mathbb{A}^n$  (in the Zariski topology).  $\square$

This property is inherited by any projective or quasi-projective variety  $Y \subseteq \mathbb{P}^n$ . We can study  $Y$  by examining its intersection with each affine chart:

$$Y = \bigcup_{i=0}^n (Y \cap U_i)$$

Each piece  $Y_i = Y \cap U_i$  is an open subset of  $Y$ , and  $\varphi_i(Y_i)$  is a quasi-affine variety in  $\mathbb{A}^n$ .

## 1.8 Regular Functions and Morphisms

To study maps between varieties, we need a notion that preserves their algebraic structure. This leads to the concept of morphisms, which are built upon regular functions.

### Continuity

In topology, a map  $\phi : X \rightarrow Y$  is continuous if for every open set  $V \subseteq Y$ , its preimage  $\phi^{-1}(V)$  is open in  $X$ . While maps like  $\phi(x) = x^2$  on  $\mathbb{R}$  are continuous in the standard topology, the Zariski topology is much coarser, so continuity is a weaker condition. We need an additional algebraic condition.

### Regular Functions

#### Definition 1.8.1: Regular Function

Let  $Y$  be a quasi-projective variety.

1. A function  $f : Y \rightarrow k$  is **regular at a point**  $P \in Y$  if there exists an open neighborhood  $U$  with  $P \in U \subseteq Y$  and homogeneous polynomials  $g, h \in S$  of the same degree such that  $h(Q) \neq 0$  for all  $Q \in U$  and  $f(Q) = \frac{g(Q)}{h(Q)}$  for all  $Q \in U$ .

2. A function  $f$  is **regular on  $Y$**  if it is regular at every point  $P \in Y$ .

For a quasi-affine variety  $Y \subseteq \mathbb{A}^n$ , the definition is analogous, but  $g$  and  $h$  are simply polynomials in the affine coordinate ring  $A(Y) = k[x_1, \dots, x_n]/\mathcal{I}(Y)$ , and the condition of being homogeneous of the same degree is not required.

### Example 1.8.1:

1. Consider  $f(x) = \frac{1}{x^2+1}$  on  $\mathbb{A}^1$ .

- On  $\mathbb{A}_{\mathbb{R}}^1$ , the denominator is never zero, so  $f$  is regular everywhere.
- On  $\mathbb{A}_{\mathbb{C}}^1$ , the denominator is zero at  $x = \pm i$ . Thus,  $f$  is not regular on all of  $\mathbb{A}_{\mathbb{C}}^1$ . It is only regular on the open set  $\mathbb{A}_{\mathbb{C}}^1 \setminus \{i, -i\}$ .

2. Consider the function  $f([x_0 : x_1]) = \frac{x_0}{x_1}$  on  $\mathbb{P}_{\mathbb{C}}^1$ . Here  $g = x_0$  and  $h = x_1$  are homogeneous of degree 1. The function is defined where  $x_1 \neq 0$ , which is the open set  $U_1$ . Thus,  $f$  is regular on  $U_1$ . It is regular at the point  $[0 : 1]$  but not at the point  $[1 : 0]$  where the denominator vanishes. [Note: The original document states the opposite, which appears to be a mistake.]

**Remark 1.8.1:** A key theorem states that the only functions that are regular on all of an affine variety  $Y$  are the elements of its coordinate ring,  $A(Y)$ . For  $Y = \mathbb{A}_k^n$  with  $k$  algebraically closed, the only globally regular functions are the polynomials in  $k[x_1, \dots, x_n]$ .

## Morphisms

A "good" map between varieties should be continuous and should preserve the structure of regular functions.

### Definition 1.8.2: Morphism

Let  $X$  and  $Y$  be varieties. A **morphism**  $\phi : X \rightarrow Y$  is a continuous map (in the Zariski topology) such that for every open set  $V \subseteq Y$  and every regular function  $g : V \rightarrow k$ , the composition

$$g \circ \phi : \phi^{-1}(V) \rightarrow k$$

is a regular function on the open set  $\phi^{-1}(V) \subseteq X$ . This is often summarized as "a morphism is a continuous map that pulls back regular functions to regular functions."

## Rational Functions and Function Fields

In the study of algebraic varieties, we initially define regular functions as those that can be represented by polynomials on affine varieties, or locally as quotients of homogeneous polynomials of the same degree on projective varieties. The ring of globally regular functions on a variety  $Y$  is denoted by  $\mathcal{O}(Y)$ .

However, there are many other functions that are well-behaved (i.e., regular) on some open subset  $U \subseteq Y$ , but not necessarily on all of  $Y$ . This leads to a more general notion. We will use the pair  $(U, f)$  to denote a function  $f$  that is regular on an open set  $U \subseteq Y$ .

These pairs allow us to define an equivalence relation which identifies functions that agree on the intersubsection of their domains.

### Definition 1.8.3: Equivalence of Local Regular Functions

Let  $(U, f)$  and  $(V, g)$  be two pairs where  $f$  is regular on an open set  $U \subseteq Y$  and  $g$  is regular on an open set  $V \subseteq Y$ . We say that they are equivalent, denoted  $(U, f) \sim (V, g)$ , if the functions agree on the intersubsection of their domains, i.e.,  $f|_{U \cap V} = g|_{U \cap V}$ .

This equivalence relation allows us to define the concept of a rational function. A rational function is an equivalence class of such pairs  $[(U, f)]$ .

### Definition 1.8.4: Function Field

The set of all equivalence classes of pairs  $(U, f)$ , where  $U$  is a non-empty open subset of  $Y$  and  $f$  is a regular function on  $U$ , is called the **function field** of  $Y$ . It is denoted by  $K(Y)$ .

$$K(Y) := \{[(U, f)] \mid U \subseteq Y \text{ is open and non-empty, } f \text{ is regular on } U\}$$

The elements  $\alpha \in K(Y)$  are called **rational functions** on  $Y$ . If  $Y$  is an irreducible variety,  $K(Y)$  is a field.

### Example 1.8.2:

1. Let  $Y = \mathbb{A}_k^1$  be the affine line. The ring of regular functions (polynomials) is  $\mathcal{O}(Y) = k[x]$ . The function field is the field of rational functions in one variable,  $K(Y) = k(x)$ . An element of  $K(Y)$  is of the form  $f(x)/g(x)$  where  $f, g$  are polynomials and  $g \not\equiv 0$ .
2. Let  $Y = \mathbb{P}_k^1$  be the projective line. The globally regular functions are just the constants, so  $\mathcal{O}(Y) = k$ . The function field, however, is much larger. If the homogeneous coordinates on  $\mathbb{P}_k^1$  are  $[x_0 : x_1]$ , then  $K(Y)$  is the field of rational functions  $f(x_0, x_1)/g(x_0, x_1)$  where  $f$  and  $g$  are homogeneous polynomials of

the same degree and  $g \not\equiv 0$ . This field is isomorphic to the field of rational functions in one variable,  $k(t)$ , where  $t = x_1/x_0$ .

$$K(\mathbb{P}_k^1) \cong K(\mathbb{A}_k^1) = k(x)$$

## The Stalk of Germs at a Point

For a specific point  $P \in Y$ , it is useful to study the behavior of functions in arbitrarily small neighborhoods of  $P$ . This leads to the idea of "germs" of functions.

### Definition 1.8.5: Germs of Functions

The set of **germs** of regular functions on  $Y$  near a point  $P \in Y$  is the set of equivalence classes of pairs  $(U, f)$  where  $P \in U \subseteq Y$  is an open neighborhood of  $P$  and  $f$  is regular on  $U$ . The equivalence relation is the same as before:  $(U, f) \sim (V, g)$  if  $f = g$  on  $U \cap V$ . This set is denoted by  $\mathcal{O}_P(Y)$  or  $\mathcal{O}_{Y,P}$ .

$$\mathcal{O}_P(Y) := \{[(U, f)] \mid P \in U \subseteq Y \text{ is open, } f \text{ is regular on } U\} / \sim$$

This set  $\mathcal{O}_P(Y)$  forms a ring, often called the **local ring of  $Y$  at  $P$**  or the **stalk** of the sheaf of regular functions at  $P$ .

### Definition 1.8.6: Ideal of Germs Vanishing at a Point

Within the ring  $\mathcal{O}_P(Y)$ , the set of germs of functions that vanish at  $P$  forms a special subset.

$$\mathfrak{m}_P := \{[(U, f)] \in \mathcal{O}_P(Y) \mid f(P) = 0\}$$

This set  $\mathfrak{m}_P$  is an ideal of the ring  $\mathcal{O}_P(Y)$ .

**Example 1.8.3: Example: The Affine Line** Let  $Y = \mathbb{A}_k^1$  with coordinate ring  $\mathcal{O}(Y) = k[x]$ , and let  $P$  be the origin, corresponding to the point  $x = 0$ . A rational function  $g(x)/h(x)$  is regular in a neighborhood of  $P$  if and only if  $h(0) \neq 0$ . Therefore, the local ring at the origin is:

$$\mathcal{O}_P(Y) = \left\{ \frac{g(x)}{h(x)} \mid g, h \in k[x], h(0) \neq 0 \right\}$$

For instance:

- $1/x \notin \mathcal{O}_P(Y)$  because the denominator is zero at  $P = (0)$ .
- $1/(1-x) \in \mathcal{O}_P(Y)$  because the denominator is non-zero at  $P = (0)$ .
- $1/(x^2 + x + 1) \in \mathcal{O}_P(Y)$  for the same reason.

The ideal of germs vanishing at  $P$  is:

$$\mathfrak{m}_P = \left\{ \frac{g(x)}{h(x)} \in \mathcal{O}_P(Y) \mid g(0) = 0 \right\}$$

This ideal is generated by the function  $x$ . Examples of elements in  $\mathfrak{m}_P$  include  $x$ ,  $x/(1-x)$ , etc.

## Properties of the Local Ring $\mathcal{O}_P(Y)$

The ring of germs  $\mathcal{O}_P(Y)$  has a very special algebraic structure.

### Proposition 1.8.1: Properties of the Local Ring at a Point

Let  $P$  be a point on a variety  $Y$  over a field  $k$ .

1.  $\mathcal{O}_P(Y)$  is a  $k$ -algebra, and  $\mathfrak{m}_P$  is an ideal of  $\mathcal{O}_P(Y)$ .
2. The quotient ring  $\mathcal{O}_P(Y)/\mathfrak{m}_P$  is a field extension of  $k$ . This implies that  $\mathfrak{m}_P$  is a maximal ideal.
3.  $\mathfrak{m}_P$  is the *unique* maximal ideal of  $\mathcal{O}_P(Y)$ .

Rings that have a unique maximal ideal are called **local rings**.

### Proof Sketch

1. **( $k$ -algebra with ideal  $\mathfrak{m}_P$ ):** Addition and multiplication of germs are defined by performing the operations on representative functions on the intersubsection of their domains. This makes  $\mathcal{O}_P(Y)$  a ring. It is a  $k$ -algebra because we can embed  $k$  into  $\mathcal{O}_P(Y)$  via constant functions. It is straightforward to check that  $\mathfrak{m}_P$  is an ideal.
2. **( $\mathfrak{m}_P$  is maximal):** We can define an evaluation map  $ev_P : \mathcal{O}_P(Y) \rightarrow k$  by  $ev_P([(U, f)]) = f(P)$ . This map is a surjective ring homomorphism whose kernel is precisely  $\mathfrak{m}_P$ . By the First Isomorphism Theorem,  $\mathcal{O}_P(Y)/\mathfrak{m}_P \cong k$ . Since  $k$  is a field, the ideal  $\mathfrak{m}_P$  must be maximal.
3. **( $\mathfrak{m}_P$  is the unique maximal ideal):** To show  $\mathcal{O}_P(Y)$  is a local ring, we need to show that any element not in  $\mathfrak{m}_P$  is a unit (i.e., has a multiplicative inverse). Let  $[(U, f)] \in \mathcal{O}_P(Y) \setminus \mathfrak{m}_P$ . By definition of  $\mathfrak{m}_P$ , this means  $f(P) \neq 0$ . Since  $f$  is continuous, there exists a smaller open neighborhood  $V \subseteq U$  of  $P$  where  $f$  is non-zero everywhere. On this neighborhood  $V$ , the function  $1/f$  is well-defined and regular. Therefore, the germ  $[(V, 1/f)]$  is an element of  $\mathcal{O}_P(Y)$  and serves as the inverse to  $[(U, f)]$ . Thus, every element outside  $\mathfrak{m}_P$  is a unit.

Now, if  $I$  is any proper ideal of  $\mathcal{O}_P(Y)$ , it cannot contain any units. Therefore,  $I$  must be a subset of the set of non-units, which we have just shown is exactly  $\mathfrak{m}_P$ . This implies that every proper ideal is contained in  $\mathfrak{m}_P$ , making  $\mathfrak{m}_P$  the unique maximal ideal.

## 1.9 Localization of Rings

The algebraic structure of the local ring  $\mathcal{O}_P(Y)$  can be described elegantly using the concept of localization from commutative algebra.

### Definition 1.9.1: Localization of a Ring

Let  $A$  be a commutative ring and let  $T \subseteq A$  be a multiplicatively closed subset (i.e.,  $1 \in T$  and for all  $s, t \in T$ , we have  $st \in T$ ). The **localization of  $A$  with respect to  $T$**  is the ring denoted  $T^{-1}A$ , defined as the set of equivalence classes of pairs  $(a, t)$  with  $a \in A, t \in T$ :

$$T^{-1}A := \left\{ \frac{a}{t} \mid a \in A, t \in T \right\}$$

where two fractions  $\frac{a}{t}$  and  $\frac{a'}{t'}$  are equivalent if there exists some  $s \in T$  such that  $s(at' - a't) = 0$ . If  $A$  is an integral domain, this simplifies to  $at' = a't$ . The set  $T^{-1}A$  forms a ring, and there is a natural ring homomorphism  $A \rightarrow T^{-1}A$  given by  $a \mapsto a/1$ .

### Example 1.9.1: Examples of Localization

- Field of Fractions:** If  $A$  is an integral domain, the set  $T = A \setminus \{0\}$  is multiplicatively closed. The localization  $(A \setminus \{0\})^{-1}A$  is the **field of fractions** of  $A$ , denoted  $\text{Frac}(A)$ . For example,  $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$ , and if  $A(Y)$  is the coordinate ring of an irreducible affine variety,  $\text{Frac}(A(Y)) = K(Y)$ , the function field.
- Localization at a Prime Ideal:** If  $\mathfrak{p} \subseteq A$  is a prime ideal, then the set  $T = A \setminus \mathfrak{p}$  is multiplicatively closed. The localization  $(A \setminus \mathfrak{p})^{-1}A$  is called the **localization of  $A$  at  $\mathfrak{p}$**  and is denoted by  $A_{\mathfrak{p}}$ .

For example, let  $A = \mathbb{Z}$  and  $\mathfrak{p} = \langle 2 \rangle$ . Then  $T = \mathbb{Z} \setminus \langle 2 \rangle$  is the set of all odd integers. The localization is:

$$\mathbb{Z}_{\langle 2 \rangle} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \text{ is odd} \right\}$$

This ring  $A_{\mathfrak{p}}$  is a local ring with unique maximal ideal  $\mathfrak{p}A_{\mathfrak{p}}$ . The quotient by this maximal ideal gives the residue field,  $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \cong \text{Frac}(A/\mathfrak{p})$ . For our example,  $\mathbb{Z}_{\langle 2 \rangle}/\langle 2 \rangle \mathbb{Z}_{\langle 2 \rangle} \cong \mathbb{Z}/\langle 2 \rangle = \mathbb{F}_2$ .

## Localization and Varieties

For an irreducible affine variety  $Y$ , its coordinate ring  $A(Y)$  is an integral domain. For a point  $P \in Y$ , there is a corresponding maximal ideal  $\mathfrak{m}_P = \{f \in A(Y) \mid f(P) = 0\}$ . The local ring of germs at  $P$  is precisely the localization of the coordinate ring at this maximal ideal.

### Theorem 1.9.1: Local Ring as Localization

For an affine variety  $Y$  and a point  $P \in Y$ , there is a natural isomorphism:

$$\mathcal{O}_P(Y) \cong A(Y)_{\mathfrak{m}_P}$$

Under this isomorphism, both are subrings of the function field  $K(Y)$ . The function field itself can be seen as a localization at the zero ideal:  $K(Y) \cong A(Y)_{(0)}$ .

The dimension of the variety can also be defined algebraically in terms of these rings:

$$\dim Y = \text{tr.deg}_k A(Y) = \text{tr.deg}_k K(Y)$$

**Example 1.9.2: Example: A Cuspidal Cubic Curve** Consider the curve  $Y = Z(x_2^2 - x_1^3) \subset \mathbb{A}_k^2$ . Its coordinate ring is  $A(Y) = k[x_1, x_2]/\langle x_2^2 - x_1^3 \rangle$ . The function field is  $K(Y) = \text{Frac}(A(Y))$ . We can describe this as  $k(x_1)[x_2]/\langle x_2^2 - x_1^3 \rangle$ , which is isomorphic to  $k(x_1)(\sqrt{x_1^3})$ . A simpler description comes from the parametrization  $x_1 = t^2, x_2 = t^3$ , which shows  $K(Y) \cong k(t)$ .

Let's look at the origin  $P = (0, 0) \in Y$ . The corresponding maximal ideal in  $A(Y)$  is  $\mathfrak{m}_P = \langle x_1, x_2 \rangle$ . The local ring at the origin is:

$$\mathcal{O}_P(Y) = A(Y)_{\mathfrak{m}_P} = \left( \frac{k[x_1, x_2]}{\langle x_2^2 - x_1^3 \rangle} \right)_{\langle x_1, x_2 \rangle}$$

This ring contains elements like  $1/(1+x_1+x_2)$ , since the denominator is not in  $\mathfrak{m}_P$ . It does not contain elements like  $1/(x_1 - x_2)$  since  $x_1 - x_2 \in \mathfrak{m}_P$ . The rational function  $x_1/x_2$  is in  $K(Y)$  but not in  $\mathcal{O}_P(Y)$ . Using the parametrization,  $x_1/x_2 = t^2/t^3 = 1/t$ , which is not defined at the origin ( $t = 0$ ).

## 1.10 The Sheaf of Regular Functions and Functoriality

The concepts discussed can be formalized using the language of sheaves. For a variety  $X$ , we can define a sheaf  $\mathcal{O}_X$ , called the **sheaf of regular functions**.

- To each open set  $U \subseteq X$ , it assigns the ring of regular functions on that set,  $\mathcal{O}_X(U)$ .

For the whole variety,  $\mathcal{O}_X(X) = \mathcal{O}(X)$ .

- The **stalk** of this sheaf at a point  $P \in X$ , denoted  $\mathcal{O}_{X,P}$ , is precisely the local ring of germs  $\mathcal{O}_P(X)$ .

This assignment  $X \mapsto \mathcal{O}_X(X)$  is a bridge from geometry to algebra. It is a **contravariant functor**. This means that a morphism of varieties  $\phi : X \rightarrow Y$  induces a ring homomorphism in the opposite direction, called the pullback map:

$$\phi^* : \mathcal{O}_Y(Y) \rightarrow \mathcal{O}_X(X) \quad \text{defined by} \quad \phi^*(f) = f \circ \phi$$

Essentially, arrows are reversed when moving from the geometric category of varieties to the algebraic category of rings. Deeper connections exist, for instance, "covering maps" in geometry often correspond to ring extensions in algebra.

## Distinguished Open Sets

A special and important class of open sets on an affine variety  $X$  are the distinguished open sets.

**Definition (Distinguished Open Set)** For any regular function  $f \in A(X)$  on an affine variety  $X$ , the **distinguished open set** defined by  $f$  is the set of points where  $f$  does not vanish:

$$X_f := \{P \in X \mid f(P) \neq 0\}$$

This is an open set because it is the complement of the closed set  $Z(f) = \{P \in X \mid f(P) = 0\}$ . These sets form a basis for the Zariski topology on  $X$ .

## 1.11 The Sheaf of Regular Functions and Distinguished Open Sets

The structure sheaf  $\mathcal{O}_X(\cdot)$  is a fundamental contravariant functor in algebraic geometry, which translates geometric structures into algebraic ones. Contravariance means that it reverses the direction of morphisms. Given a morphism of varieties  $\phi : X \rightarrow Y$ , it induces a homomorphism of rings (a "pullback") in the opposite direction:

$$\phi^* : \mathcal{O}_Y(Y) \rightarrow \mathcal{O}_X(X)$$

This correspondence is central; for instance, inclusions of affine varieties  $X \hookrightarrow Y$  correspond to surjective ring extensions  $A(Y) \rightarrow A(X)$ .

Let's consider a special and important class of open subsets of an affine variety  $X$ .

### Definition 1.11.1: Distinguished Open Set

For an affine variety  $X$  with coordinate ring  $A(X)$ , and an element  $f \in A(X)$ , the **distinguished open set** associated with  $f$  is defined as:

$$X_f := \{P \in X \mid f(P) \neq 0\} = X \setminus \mathcal{Z}(f)$$

where  $\mathcal{Z}(f)$  is the zero set of  $f$ .

**Warning 1.11.1:** Any open set  $U \subseteq X$  can be expressed as a union of distinguished open sets. If  $U = X \setminus \mathcal{Z}(J)$  for some ideal  $J = \langle f_1, \dots, f_m \rangle$ , then:

$$U = X \setminus \bigcap_{i=1}^m \mathcal{Z}(f_i) = \bigcup_{i=1}^m (X \setminus \mathcal{Z}(f_i)) = \bigcup_{i=1}^m X_{f_i}$$

This means the set  $\{X_f \mid f \in A(X)\}$  forms a basis for the Zariski topology on  $X$ .

A key result connects the ring of regular functions on a distinguished open set to an algebraic construction: localization.

### Proposition 1.11.1: Regular Functions on Distinguished Open Sets

The ring of regular functions on the distinguished open set  $X_f$  is isomorphic to the localization of the coordinate ring  $A(X)$  at the multiplicative set generated by  $f$ .

$$\mathcal{O}_X(X_f) \cong A(X)_f := S^{-1}A(X), \quad \text{where } S = \{f^n \mid n \geq 0\}$$

*Proof.* First, we show that  $A(X)_f \subseteq \mathcal{O}_X(X_f)$ . An element of  $A(X)_f$  has the form  $g/f^n$  for some  $g \in A(X)$  and  $n \geq 0$ . This defines a function on  $X_f$  because for any point  $P \in X_f$ , the denominator  $f^n(P) = (f(P))^n \neq 0$ . This is a regular function by definition.

Conversely, let  $\phi \in \mathcal{O}_X(X_f)$  be a regular function. By definition, for every point  $P \in X_f$ , there exists an open neighborhood  $U_P \subseteq X_f$  and polynomials  $g_P, h_P \in A(X)$  such that  $h_P(Q) \neq 0$  for all  $Q \in U_P$  and  $\phi(Q) = g_P(Q)/h_P(Q)$  for all  $Q \in U_P$ .

We can cover  $X_f$  with a finite number of such neighborhoods. A more direct approach is as follows: Define an ideal  $J \subseteq A(X)$  by:

$$J := \{h \in A(X) \mid h \cdot \phi \text{ extends to a regular function on all of } X, \text{i.e., } h\phi \in A(X)\}$$

This is indeed an ideal of  $A(X)$ . For any point  $P \in X_f$ , there is some  $h_P$  in our local definition of  $\phi$  such that  $h_P(P) \neq 0$  and  $h_P \in J$ . This means that no point in  $X_f$  is in the zero set of  $J$ .

$$X_f \cap \mathcal{Z}(J) = \emptyset$$

This implies that the zero set of  $J$  must be contained within the complement of  $X_f$ , which

is  $\mathcal{Z}(f)$ .

$$\mathcal{Z}(J) \subseteq \mathcal{Z}(f)$$

By Hilbert's Nullstellensatz, this inclusion of zero sets implies a reverse inclusion for their corresponding radical ideals. Taking the ideal of functions vanishing on these sets, we get  $\mathcal{I}(\mathcal{Z}(J)) \supseteq \mathcal{I}(\mathcal{Z}(f))$ . This means  $\sqrt{J} \supseteq \sqrt{\langle f \rangle}$ , which implies that some power of  $f$  must lie in  $J$ .

$$f^r \in J \quad \text{for some integer } r > 0.$$

By the definition of  $J$ , this means  $f^r \cdot \phi = g$  for some  $g \in A(X)$ . Therefore, on  $X_f$ , we can write  $\phi = g/f^r$ , which is an element of  $A(X)_f$ .  $\square$

**Corollary 1.11.1: Stalk of the Structure Sheaf at a Point** The stalk of the structure sheaf at a point  $P \in X$  (which is an affine variety) is the localization of the coordinate ring at the maximal ideal  $m_P = \mathcal{I}(P)$  corresponding to that point.

$$\mathcal{O}_{X,P} = A(X)_{m_P}$$

## The Projective Case

The situation for a projective variety  $X \subseteq \mathbb{P}^n$  is similar but involves graded rings. Let  $S(X)$  be the homogeneous coordinate ring of  $X$ .

- For a homogeneous polynomial  $f \in S(X)$ , the ring of regular functions on the distinguished open set  $X_f = X \setminus \mathcal{Z}(f)$  is the degree-zero part of the localization of  $S(X)$  at  $f$ :

$$\mathcal{O}_X(X_f) = (S(X)_f)_0 := \left\{ \frac{g}{f^k} \mid g, f \in S(X) \text{ are homogeneous, } k \in \mathbb{N}, \deg(g) = \deg(f^k) \right\}$$

- A key difference is that for any projective variety  $X$ , the only globally regular functions are constants:  $\mathcal{O}_X(X) = k$ .
- The stalk at a point  $P \in X$  is the degree-zero part of the localization of  $S(X)$  at the homogeneous prime ideal  $m_P$  corresponding to  $P$ :  $\mathcal{O}_{X,P} = (S(X)_{(m_P)})_0$ .

## 1.12 Rational Maps and Birational Equivalence

We now define a more general type of map between varieties that is not necessarily defined everywhere.

**Definition 1.12.1: Rational Map**

For varieties  $X$  and  $Y$ , a **rational map**  $\phi : X \dashrightarrow Y$  is an equivalence class of pairs  $(U, \phi_U)$ , where  $U \subseteq X$  is a non-empty open set and  $\phi_U : U \rightarrow Y$  is a morphism. Two pairs  $(U, \phi_U)$  and  $(V, \phi_V)$  are considered equivalent if  $\phi_U$  and  $\phi_V$  agree on the intersubsection  $U \cap V$ . The largest possible open set on which  $\phi$  is defined as a morphism is called the domain of definition of  $\phi$ .

**Remark 1.12.1: Rational Functions and Function Fields** If we take  $Y = \mathbb{A}_k^1$ , this definition recovers the concept of a **rational function** on  $X$ . The set of all rational functions on  $X$  forms a field, the **function field** of  $X$ , denoted  $K(X)$ .

**Definition 1.12.2: Dominant Map**

A rational map  $\phi : X \dashrightarrow Y$  is **dominant** if for some (and therefore any) representative morphism  $\phi_U : U \rightarrow Y$ , the image  $\phi_U(U)$  is a dense subset of  $Y$ .

**Warning 1.12.1:** In the Zariski topology, any non-empty open subset of an irreducible variety  $Y$  is dense. Therefore,  $\phi$  is dominant if its image contains an open subset of  $Y$ .

A dominant rational map  $\phi : X \dashrightarrow Y$  induces a field homomorphism of the corresponding function fields,  $\phi^* : K(Y) \rightarrow K(X)$ .

**Definition 1.12.3: Birational Equivalence**

Varieties  $X$  and  $Y$  are **birationally equivalent** (or **birational**), written  $X \cong_{bir} Y$ , if there exists a rational map  $\phi : X \dashrightarrow Y$  which has a rational inverse  $\psi : Y \dashrightarrow X$ . This means that  $\psi \circ \phi = \text{id}_X$  and  $\phi \circ \psi = \text{id}_Y$  as rational maps (i.e., they are the identity on their domains of definition).

**Theorem 1.12.1: Birational Equivalence and Function Fields**

Two varieties  $X$  and  $Y$  are birationally equivalent if and only if their function fields are isomorphic as  $k$ -algebras.

$$X \cong_{bir} Y \iff K(X) \cong K(Y)$$

*Proof.* ( $\Rightarrow$ ) Let  $\phi : X \dashrightarrow Y$  and  $\psi : Y \dashrightarrow X$  be inverse rational maps. Since  $\phi$  must be dominant, it induces an injective field homomorphism  $\phi^* : K(Y) \rightarrow K(X)$ . Similarly, the dominant map  $\psi$  induces  $\psi^* : K(X) \rightarrow K(Y)$ . The compositions correspond to  $(\phi \circ \psi)^* = \psi^* \circ \phi^*$  and  $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ . Since the compositions are identity maps, the field homomorphisms must be inverses of each other. Thus,  $K(X) \cong K(Y)$ .

( $\Leftarrow$ ) Conversely, suppose there is a  $k$ -algebra isomorphism  $\Psi : K(Y) \rightarrow K(X)$ . Since

function fields of affine varieties are the fraction fields of their coordinate rings, we have  $K(Y) = \text{Frac}(A(Y))$  and  $K(X) = \text{Frac}(A(X))$ . We can find an affine open set  $U \subseteq X$  and an affine open set  $V \subseteq Y$  such that  $\Psi$  restricts to an isomorphism of their coordinate rings,  $\Psi : A(V) \rightarrow A(U)$ . An isomorphism of coordinate rings corresponds to an isomorphism of affine varieties,  $\phi : U \rightarrow V$ . This morphism can be extended to a rational map  $\phi : X \dashrightarrow Y$ . The inverse isomorphism gives an inverse rational map  $\psi : Y \dashrightarrow X$ . Thus,  $X$  and  $Y$  are birationally equivalent.  $\square$

### Example: A Cusp and the Affine Line

Consider the affine line  $X = \mathbb{A}_k^1$  and the cuspidal cubic curve  $Y = \mathcal{Z}(y^2 - x^3) \subseteq \mathbb{A}_k^2$ .

- The coordinate rings are  $A(X) = k[t]$  and  $A(Y) = k[x, y]/\langle y^2 - x^3 \rangle$ . These rings are not isomorphic (e.g., the local ring at the origin of  $Y$  is not a regular local ring, while all local rings of  $X$  are). Thus,  $X$  and  $Y$  are not isomorphic.
- Consider the morphism  $\phi : X \rightarrow Y$  given by  $t \mapsto (t^2, t^3)$ . This is a morphism.
- Consider the rational map  $\psi : Y \dashrightarrow X$  given by  $(x, y) \mapsto y/x$ . This is defined on the open set  $Y \setminus \{(0, 0)\}$ .
- The maps are inverses:  $\psi(\phi(t)) = t^3/t^2 = t$ , and  $\phi(\psi(x, y)) = ((y/x)^2, (y/x)^3) = (y^2/x^2, y^3/x^3)$ . Since on the curve  $y^2 = x^3$ , this is  $(x^3/x^2, y^3/x^2) = (x, y)$ .
- Their function fields are  $K(X) = k(t)$  and  $K(Y) = k(x, y)$  where  $y^2 = x^3$ . We can express  $x = (y/x)^2$  and  $y = (y/x)^3$  in terms of the rational function  $t = y/x$ . So  $K(Y) = k(y/x) \cong k(t)$ .

Since their function fields are isomorphic,  $\mathbb{A}_k^1$  and the cusp  $Y$  are birationally equivalent.

## 1.13 Birationality and Hypersurfaces

An important result states that from a birational point of view, all varieties are as simple as hypersurfaces.

### Proposition 1.13.1: Birational Equivalence to Hypersurfaces

Any irreducible algebraic variety of dimension  $r$  is birationally equivalent to a hypersurface in  $\mathbb{A}^{r+1}$ .

*Proof.* Let  $X$  be a variety of dimension  $r$ . The dimension is equal to the transcendence degree of its function field over the base field  $k$ .

$$r = \dim(X) = \text{tr.deg}_k(K(X))$$

This means there exist  $r$  algebraically independent elements  $x_1, \dots, x_r \in K(X)$  over  $k$ . Let  $K' = k(x_1, \dots, x_r)$  be the purely transcendental extension of  $k$ . The extension  $K'/k$  is the function field of  $\mathbb{A}^r$ .

The field extension  $K(X)/K'$  is a finite algebraic extension. By the Primitive Element Theorem, if the extension is separable (which is always true for fields of characteristic zero), we can find a single element  $x_{r+1} \in K(X)$  that generates the extension.

$$K(X) = K'(x_{r+1}) = k(x_1, \dots, x_r, x_{r+1})$$

Since  $x_{r+1}$  is algebraic over  $K'$ , it satisfies a minimal polynomial relation:

$$F(x_{r+1}) = 0, \quad \text{where } F \text{ is an irreducible polynomial with coefficients in } K'.$$

By clearing denominators, we can choose  $F$  to be an irreducible polynomial in  $k[X_1, \dots, X_r, X_{r+1}]$ . The zero set of this polynomial,  $H = \mathcal{Z}(F)$ , is a hypersurface in  $\mathbb{A}^{r+1}$ . Its function field is  $K(H) = \text{Frac}(k[X_1, \dots, X_{r+1}]/\langle F \rangle) \cong k(x_1, \dots, x_{r+1}) = K(X)$ .

Since  $K(X) \cong K(H)$ , the variety  $X$  is birationally equivalent to the hypersurface  $H$ .  $\square$

## The Primitive Element Theorem

This subsection briefly touches upon the Primitive Element Theorem, which is a fundamental result in field theory stating that every finite separable field extension is a simple extension. This concept is useful in algebraic geometry for simplifying the structure of function fields of varieties.

**Exercise** Given a function field  $K(X)$  over a base field  $k$ , can we write  $K(X)$  as a simple extension  $k(\alpha)$  for some element  $\alpha \in K(X)$ ?

The Primitive Element Theorem provides a positive answer in the case of separable extensions. If  $K(X)/k$  is a finite separable extension, then such an  $\alpha$ , called a primitive element, exists.

The minimal polynomial of this primitive element, let's call it  $f(y) = \text{minpoly}_{\alpha, k'}(y)$ , where  $k'$  is a subfield, satisfies the isomorphism:

$$k'(\alpha) := k'[y]/\langle f(y) \rangle \cong K(x)$$

This implies that the variety  $X$  is birationally equivalent to a hypersurface  $H = \mathcal{Z}(f)$ . This birational map is a key tool for studying varieties.

**Idea of the Proof of the Primitive Element Theorem (P.E.T.):** Consider a field extension generated by two elements,  $K = k(\alpha_1, \alpha_2)$ , where the extension  $K/k$  is separable.

The theorem asserts that we can find a single element  $\alpha$  such that  $K = k(\alpha)$ .

**Example 1.13.1: Example: Combining Square Roots** A classic example is the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . This can be expressed as a simple extension  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ .

The constructive proof for finding a primitive element often involves taking a "random" linear combination of the generators. For a field  $k$  of characteristic 0 (or a sufficiently large finite field), we can almost always write:

$$k(\alpha_1, \alpha_2) = k(c_1\alpha_1 + c_2\alpha_2) \quad \text{for some } c_1, c_2 \in k.$$

Typically, we can set  $\alpha = \alpha_1 + c\alpha_2$  for some  $c \in k$ .

**Exercise** Prove the existence of suitable constants  $c_1, c_2$  by considering a linear system.

## 1.14 Non-singular (or Smooth) Varieties

We now shift our focus to the local geometry of an algebraic variety. The key idea is to approximate the variety near a point with a linear space, known as the tangent space.

Let  $X \subseteq \mathbb{A}_k^n$  be an affine variety of dimension  $r$ . Let its defining ideal be  $\mathcal{I}(X) = \langle f_1, \dots, f_t \rangle \triangleleft k[x_1, \dots, x_n]$ . To study the local structure of  $X$  at a point  $P \in X$ , we can, without loss of generality, assume  $P = \bar{0} = (0, \dots, 0)$  by applying a coordinate transformation. Since  $P \in X$ , we have  $f_i(P) = 0$  for all  $i = 1, \dots, t$ .

To reduce the non-linear structure of  $X$  at  $P$  to a linear one (a  $k$ -vector space), we linearize the defining polynomials  $f_i$ . The Taylor expansion of  $f_i$  around  $P = \bar{0}$  is:

$$f_i(x_1, \dots, x_n) = \underbrace{f_i(\bar{0})}_{=0} + \underbrace{\sum_{j=1}^n \frac{\partial f_i}{\partial x_j} \Big|_P \cdot x_j}_{\text{linear part } f_i^{(1)}} + (\text{higher order terms})$$

### Definition 1.14.1: Zariski Tangent Space

Let  $X \subseteq \mathbb{A}_k^n$  be an affine variety and  $P \in X$ . Assume  $P = \bar{0}$  and  $\mathcal{I}(X) = \langle f_1, \dots, f_t \rangle$ . The **tangent space** to  $X$  at  $P$ , denoted  $T_{X,P}$ , is the affine linear subspace of  $\mathbb{A}_k^n$  defined by the vanishing of the linear parts of the polynomials in  $\mathcal{I}(X)$ .

$$T_{X,P} := Z(f_1^{(1)}, \dots, f_t^{(1)}) = Z \left( \left\{ \sum_{j=1}^n \frac{\partial f_i}{\partial x_j} \Big|_P \cdot x_j \quad \forall i \in [t] \right\} \right)$$

The ideal of these linear forms is denoted  $\mathcal{I}(X)^{(1)} = \langle f_1^{(1)}, \dots, f_t^{(1)} \rangle$ .

The linear functions on the tangent space form its dual vector space.

**Definition 1.14.2: Cotangent Space**

The dual space to the tangent space, known as the **cotangent space**, is given by

$$T_{X,P}^\vee := A^{(1)} / \mathcal{I}(X)^{(1)}$$

where  $A^{(1)}$  is the space of all linear forms in  $k[x_1, \dots, x_n]$ .

The dimension of the tangent space is determined by the rank of the Jacobian matrix.

**Proposition 1.14.1: Dimension of the Tangent Space**

The dimension of the tangent space  $T_{X,P}$  is given by:

$$\dim_k T_{X,P} = n - \text{rank}(J_P)$$

where  $J_P = \left( \frac{\partial f_i}{\partial x_j} \right)_{i \in [t], j \in [n]}$  is the Jacobian matrix of the generators of  $\mathcal{I}(X)$  evaluated at  $P$ .

*Proof.* The tangent space  $T_{X,P}$  is the solution space to the system of linear equations:

$$\forall i \in [t], \quad f_i^{(1)} = \sum_{j=1}^n \left( \frac{\partial f_i}{\partial x_j} \right)_P \cdot x_j = 0$$

This is a homogeneous linear system in the variables  $x_1, \dots, x_n$ . The coefficient matrix of this system is precisely the Jacobian matrix  $J_P$ . By the rank-nullity theorem, the dimension of the solution space is  $n - \text{rank}(J_P)$ .  $\square$

**Relation to the Local Ring**

The tangent space, which is defined extrinsically using embeddings in  $\mathbb{A}^n$ , has an intrinsic algebraic characterization in terms of the local ring of the variety at the point  $P$ .

Let  $\mathcal{O}_{X,P}$  be the local ring of  $X$  at  $P$ , and let  $M_P$  be its unique maximal ideal, consisting of rational functions on  $X$  that vanish at  $P$ . The quotient  $M_P/M_P^2$  is a  $k$ -vector space.

**Proposition 1.14.2: Cotangent Space and Local Ring**

The cotangent space  $T_{X,P}^\vee$  is canonically isomorphic to  $M_P/M_P^2$ .

$$T_{X,P}^\vee \cong M_P/M_P^2$$

*Proof.* Consider the natural map  $\varphi : T_{X,P}^\vee \rightarrow M_P/M_P^2$ . Since  $P = \bar{0}$ , a linear form  $f \in T_{X,P}^\vee$  vanishes at  $P$ , so its germ is in  $M_P$ . The map is defined by sending the class of a linear form  $f$  in  $T_{X,P}^\vee$  to its class in  $M_P/M_P^2$ . One can show this map is a well-defined  $k$ -vector space isomorphism.

- **Injectivity:** If  $\varphi(f) = 0$ , then  $f \in M_P^2$ . A linear form that lies in the square of the maximal ideal must be the zero form. Thus,  $f = 0$  in  $T_{X,P}^\vee$ .
- **Surjectivity:** Let  $\tau = f/g \in M_P$  be an arbitrary element (a germ of a function vanishing at  $P$ ). We can assume, without loss of generality, that  $g(P) = 1$ . The linear approximation of  $\tau$  at  $P$  is the linear form  $\tau' := \sum_{j=1}^n (\partial_j \tau)_P \cdot x_j$ . One can show that  $\tau - \tau' \in M_P^2$  using a Taylor expansion argument. This means  $\tau \equiv \tau' \pmod{M_P^2}$ , so the class of  $\tau$  is the image of the linear form  $\tau'$  under  $\varphi$ .

This proves that  $\varphi$  is an isomorphism.  $\square$

**Remark 1.14.1: Geometric Interpretation** The tangent space  $T_{X,P}$  and its dual  $T_{X,P}^\vee$  provide a first-order linear approximation of the variety  $X$  (or more precisely, the neighborhood of  $P$  in  $X$ ) and the germs of functions at  $P$ , respectively.

### 1.14.1 Singular and Non-Singular Points

A fundamental result in algebraic geometry relates the dimension of the tangent space to the local dimension of the variety at that point.

#### Theorem 1.14.1: Dimension Inequality for Tangent Spaces

For any point  $P$  on an affine variety  $X$ , we have the inequality:

$$\dim_k T_{X,P} \geq \dim X$$

(More precisely,  $\dim_k T_{X,P} \geq \dim \mathcal{O}_{X,P}$ , the local dimension of  $X$  at  $P$ .)

**Exercise** Prove this result.

*Proof.* The tangent space is constructed from the linear parts of the defining equations, "forgetting" the higher-order constraints. If the dimension of this linear approximation is strictly larger than the dimension of the variety itself, it means the linear approximation is a poor fit and has "lost" local information about the variety at that point. This happens at points we call "singular".  $\square$

#### Definition 1.14.3: Singularity

A point  $P$  on a variety  $X$  is **non-singular** (or **smooth**, or a **simple point**) if  $\dim_k T_{X,P} = \dim X$ .

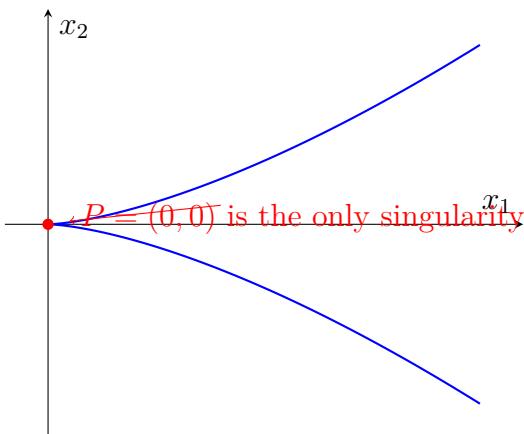
If  $\dim_k T_{X,P} > \dim X$ , then  $P$  is a **singular point** of  $X$ .

The variety  $X$  is called non-singular if every point  $P \in X$  is non-singular.

**Example 1.14.1:** Let  $X = \mathcal{Z}(x_2 - x_1^3) \subseteq \mathbb{A}^2$ , and let  $P = (0, 0)$ . The dimension of the curve is  $\dim X = 1$ . The Jacobian matrix is  $J = [\partial_{x_1} f, \partial_{x_2} f] = [-3x_1^2, 1]$ . At  $P = (0, 0)$ , the Jacobian is  $J_P = [-3(0)^2, 1] = [0, 1]$ . The rank is  $\text{rank}(J_P) = 1$ . The dimension of the tangent space is  $\dim_k T_{X,P} = n - \text{rank}(J_P) = 2 - 1 = 1$ . Since  $\dim_k T_{X,P} = \dim X$ , the point  $P = (0, 0)$  is a smooth point.

**Example 1.14.2: A Singular Curve: The Cusp** Let  $X = \mathcal{Z}(x_2^2 - x_1^3) \subseteq \mathbb{A}^2$ , and let  $P = (0, 0)$ . This is the cuspidal cubic. The dimension of the curve is  $\dim X = 1$ . The Jacobian matrix is  $J = [\partial_{x_1} f, \partial_{x_2} f] = [-3x_1^2, 2x_2]$ . At  $P = (0, 0)$ , the Jacobian is  $J_P = [-3(0)^2, 2(0)] = [0, 0]$ . The rank is  $\text{rank}(J_P) = 0$ . The dimension of the tangent space is  $\dim_k T_{X,P} = n - \text{rank}(J_P) = 2 - 0 = 2$ . Here,  $\dim_k T_{X,P} = 2 > \dim X = 1$ . Therefore, the point  $P = (0, 0)$  is a singularity of  $X$ . (In fact,  $P$  is the only singularity on this curve).

The Cuspidal Cubic  $x_2^2 = x_1^3$



At the singular point  $P = \bar{0}$ , the tangent space is  $T_{X,P} = \mathbb{A}_k^2$ , the entire ambient plane. For any other point  $P \neq \bar{0}$  on the curve, the tangent space is a line,  $T_{X,P} \cong \mathbb{A}_k^1$ . Even though  $X$  is singular, it is birational to the affine line  $\mathbb{A}_k^1$ .

# CHAPTER 2

## RESOLUTION OF SINGULARITIES & VALUATIONS

---

### 2.1 Introduction: Resolving Singularities of Curves

**Exercise** Can we find a non-singular curve that is birationally equivalent to a given singular curve  $X$ ?

The answer is yes. A major theorem in algebraic geometry states that every curve is birational to a non-singular projective curve. This process of finding such a smooth model is called "resolution of singularities."

#### Example: The Cuspidal Cubic

Let's see how to resolve the singularity at  $P = \bar{0}$  for the cuspidal cubic  $X = \mathcal{Z}(x_2^2 - x_1^3)$ .

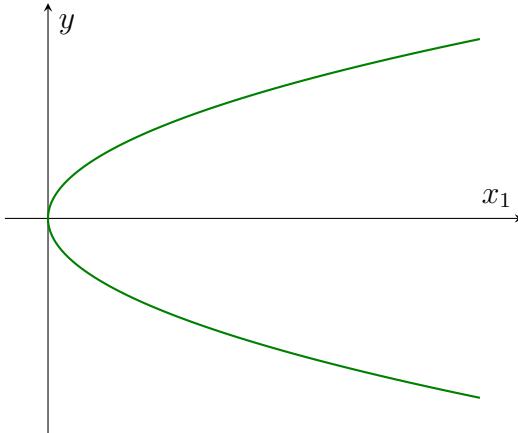
The issue at the origin is that the curve "crosses itself" in a way that is not smooth. The rational function  $y = x_2/x_1$  is not regular at  $P$  (it is in the form " $0/0$ "), but it encodes the direction of approach to the origin. Let's use this.

Consider a new curve  $\tilde{X}$  in the  $(x_1, y)$ -plane defined by the equation we get from substituting  $x_2 = yx_1$  into the original equation:  $(yx_1)^2 = x_1^3 \implies y^2 x_1^2 = x_1^3 \implies x_1^2(y^2 - x_1) = 0$ . The interesting component is  $\tilde{X} = \mathcal{Z}(y^2 - x_1)$ . This is a non-singular parabola.

We have a birational map  $\varphi : X \dashrightarrow \tilde{X}$  given by  $(x_1, x_2) \mapsto (x_1, y = x_2/x_1)$ . Its inverse is a regular map  $\psi : \tilde{X} \rightarrow X$  given by  $(x_1, y) \mapsto (x_1, x_1 y) = (y^2, y^3)$ .

The curve  $\tilde{X} = \mathcal{Z}(y^2 - x_1)$  is a non-singular curve and is birational to our original singular curve  $X$ . We have "resolved" the singularity.

The Smooth Parabola  $\tilde{X} = \mathcal{Z}(y^2 - x_1)$



The general goal is to develop systematic procedures (like blowing up points) to achieve this resolution for any curve, even those with multiple or more complex singularities.

## 2.2 Blowing-Up: Resolving Singularities

The process of resolving a singularity is also known as "blowing-up". The name comes from the fact that a singular point is mapped to a higher-dimensional space. For instance, a singular point  $(x_1, x_2)$  can be mapped to a point  $(x_1, yx_1, y)$ . A common example is blowing up the origin  $(0, 0)$  in the plane, where the point  $(0, 0)$  might be mapped to a point like  $(0, 0, 1)$  in a new space.

The goal of this process is to replace a singular point with a non-singular object (like a line). This transformation should satisfy certain desirable properties.

### Property I: Resolving the Local Ring Structure

The first property concerns the algebraic structure of the local ring at the point. We want the new ring to be "simpler" in a specific way.

#### Definition 2.2.1: Blowing-Up Property I

[Property I:] The transformed ring, which we can denote as  $A(\tilde{X})_{\langle x_1, y \rangle}$ , is a local domain whose unique maximal ideal is now a principal ideal.

**Example 2.2.1: Example: Resolving the Cusp** Consider the cusp curve defined by  $x_2^2 - x_1^3 = 0$ . The local ring at the origin,  $(k[x_1, x_2]/\langle x_2^2 - x_1^3 \rangle)_{\langle x_1, x_2 \rangle}$ , has a maximal ideal  $\langle x_1, x_2 \rangle$  which is not principal.

The blowing-up process involves the substitution  $x_2 = yx_1$ . The equation becomes  $(yx_1)^2 - x_1^3 = 0$ , which simplifies to  $x_1^2(y^2 - x_1) = 0$ . On the new chart defined by  $y^2 - x_1 = 0$ , the maximal ideal corresponding to the original singularity becomes  $\langle x_1, y \rangle$ . In the new coordinate ring  $A(\tilde{X}) = k[x_1, y]/\langle y^2 - x_1 \rangle$ , we can see that  $x_1 = y^2$ .

Therefore, the ideal simplifies:

$$\langle x_1, y \rangle = \langle y^2, y \rangle = \langle y \rangle$$

This new ideal is principal, generated by  $y$ . The original non-principal ideal has been resolved into a principal one.

## 2.3 Discrete Valuation Rings (DVRs)

### Definition and Examples

The property of having a principal maximal ideal in a local domain is central to the theory of resolving singularities. This leads to the definition of a Discrete Valuation Ring (DVR).

#### Definition 2.3.1: Discrete Valuation Ring (DVR)

A ring  $R$  is called a **Discrete Valuation Ring (dvr)** if it is a local domain with a principal maximal ideal.

#### Example 2.3.1: Examples of DVRs

- The ring  $(k[x_1, y]/\langle y^2 - x_1 \rangle)_{\langle x_1, y \rangle}$  from the previous example is a dvr.
- The ring  $(k[x_1, x_2]/\langle x_2^2 - x_1^3 \rangle)_{\langle x_1, x_2 \rangle}$  is **not** a dvr because its maximal ideal  $\langle x_1, x_2 \rangle$  is not principal.
- The ring of integers  $\mathbb{Z}$  is not a dvr because it is not a local ring, although every maximal ideal (generated by a prime  $p$ ) is principal. However, its localizations  $\mathbb{Z}_{(p)}$  are dvrs.

## 2.4 Valuation Theory

### Discrete Valuations

The second property relates dvrs to the concept of a valuation on a field.

#### Definition 2.4.1: Blowing-Up Property II

A dvr  $R$  with maximal ideal  $m$  and field of fractions  $K = k(R)$  gives rise to a discrete valuation on  $K$ . The field  $k \cong R/m$  is the residue field.

**Definition 2.4.2: Discrete Valuation**

A **discrete valuation** of a field  $K$  is a surjective map  $v : K^* \rightarrow \mathbb{Z}$  (where  $K^* = K \setminus \{0\}$ ) such that for all  $\alpha, \beta \in K^*$ :

1.  $v(\alpha\beta) = v(\alpha) + v(\beta)$  (i.e.,  $v$  is a group homomorphism).
2.  $v(\alpha + \beta) \geq \min(v(\alpha), v(\beta))$  (the non-Archimedean or triangle inequality).

By convention, we set  $v(0) = \infty$ .

**Remark 2.4.1:** A useful property that follows from the axioms is that if  $v(\alpha) \neq v(\beta)$ , then  $v(\alpha + \beta) = \min(v(\alpha), v(\beta))$ .

## Constructing a Valuation from a DVR

If  $R$  is a dvr, its maximal ideal  $m$  is principal, so  $m = \langle u \rangle$  for some element  $u \in R$ . This generator  $u$  is called a **uniformizer** of  $R$ .

Any non-zero element  $\alpha \in K = k(R)$  can be uniquely written in the form  $\alpha = u^e \cdot \alpha'$ , where  $e \in \mathbb{Z}$  and  $\alpha' \in R \setminus m$  (i.e.,  $\alpha'$  is a unit in  $R$ ).

We can then define a map  $v : K^* \rightarrow \mathbb{Z}$  by:

$$v(\alpha) := e$$

This map  $v$  is a discrete valuation.

**Example 2.4.1: Computing Valuations in a DVR** Let's return to  $R = (k[x_1, y]/\langle y^2 - x_1 \rangle)_{\langle x_1, y \rangle}$ , which is a dvr with uniformizer  $y$ . Any element  $\alpha$  in its fraction field  $K$  can be written as  $\alpha = y^e \cdot \alpha'$  for a unit  $\alpha'$ . The valuation  $v(\alpha)$  is this exponent  $e$ .

- $v(x_1) = v(y^2) = 2$ .
- In the original singular curve setting,  $x_2 = yx_1 = y(y^2) = y^3$ . Thus,  $v(x_2) = v(y^3) = 3$ .
- $v(1 + x_1)$ : Since  $1 + x_1$  is not in the maximal ideal  $\langle y \rangle$ , it is a unit in  $R$ . Thus,  $v(1 + x_1) = 0$ .
- $v(1/x_1) = v((y^2)^{-1}) = v(y^{-2}) = -2$ .

An arbitrary element in  $K$  can be written as  $\alpha = \frac{a(x_1) + yb(x_1)}{c(x_1)}$  for polynomials  $a, b, c$ .

## Key Properties of DVRs

There is a deep connection between a ring being a dvr, the existence of a valuation, and the property of being integrally closed.

### Characterizing a DVR via its Valuation

#### Proposition 2.4.1: Fractional Characterization

If  $R$  is a dvr with fraction field  $K$  and corresponding valuation  $v$ , then the ring  $R$ , its maximal ideal  $m$ , and its group of units  $R^*$  can be described entirely in terms of  $v$ :

- $R = \{\alpha \in K \mid v(\alpha) \geq 0\} \cup \{0\}$
- $m = \{\alpha \in K \mid v(\alpha) > 0\} \cup \{0\}$
- $R^* = \{\alpha \in K \mid v(\alpha) = 0\}$  (the units in  $R$ )

Conversely, if a field  $K$  has a valuation  $v : K^* \rightarrow \mathbb{Z}$ , then the set  $R = \{\alpha \in K \mid v(\alpha) \geq 0\} \cup \{0\}$  is a dvr with  $K$  as its field of fractions.

### Property III: Integral Closure

The third key property of a dvr is that it is integrally closed.

#### Definition 2.4.3: Blowing-Up Property III

A dvr  $R$  is integrally closed in its field of fractions  $K$ .

#### Definition 2.4.4: Integrally Closed Domain

A domain  $R$  is **integrally closed** in its field of fractions  $K$  if every element  $\alpha \in K$  that is a root of a monic polynomial with coefficients in  $R$  is already in  $R$ . That is, if  $\alpha \in K$  satisfies an equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

where all  $a_i \in R$ , then it must be that  $\alpha \in R$ .

**Example 2.4.2: Integral Closure Example** The ring of integers  $\mathbb{Z}$  is integrally closed in the field of rational numbers  $\mathbb{Q}$ . For instance, if  $\alpha = a/b \in \mathbb{Q}$  is a root of  $\alpha^2 + 2\alpha + 3 = 0$ , then substituting and clearing denominators gives  $a^2 + 2ab + 3b^2 = 0$ . From this, one can deduce that  $b$  must divide  $a$ , which means  $\alpha = a/b$  is an integer.

The idea for resolving singularities is to replace the local ring of the singular point,  $\mathcal{O}_{X,P}$ , with its integral closure in the function field  $K(X)$ .

## The Equivalence Theorem

For a large class of rings relevant to geometry, these three properties are equivalent.

### Proposition 2.4.2: Equivalence Theorem for DVRs

For a local domain  $R$  whose fraction field  $K$  has transcendence degree 1 over a base field  $k$ , the following are equivalent (TFAE):

1.  $R$  is a dvr.
2.  $R$  is the valuation ring for some discrete valuation on  $K$ .
3.  $R$  is integrally closed in  $K$ .

*Proof.* (1)  $\Leftrightarrow$  (2): As shown previously, a dvr defines a valuation via its uniformizer, and a valuation defines a dvr as the set of elements with non-negative valuation. The maximal ideal  $m = \{\alpha \in K \mid v(\alpha) > 0\}$  is generated by any element  $u \in m$  with the least positive valuation, making  $R$  a dvr.

(2)  $\Rightarrow$  (3): Let  $R$  be a valuation ring for  $v$ , and let  $\alpha \in K$  be integral over  $R$ . Then  $\alpha$  satisfies  $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$  for  $a_i \in R$ . Suppose, for contradiction, that  $\alpha \notin R$ . This means  $v(\alpha) < 0$ . We have  $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_0)$ . Applying the valuation  $v$ :

$$v(\alpha^n) = v(a_{n-1}\alpha^{n-1} + \cdots + a_0) \geq \min_{0 \leq i \leq n-1} \{v(a_i\alpha^i)\}$$

This gives  $n \cdot v(\alpha) \geq \min_{0 \leq i \leq n-1} \{v(a_i) + i \cdot v(\alpha)\}$ . Since  $a_i \in R$ , we have  $v(a_i) \geq 0$ . As  $v(\alpha) < 0$ , the term  $i \cdot v(\alpha)$  is strictly increasing with  $i$ . Therefore,  $v(a_i) + i \cdot v(\alpha) > v(a_j) + j \cdot v(\alpha)$  if  $i < j$ . The minimum value on the right is achieved when  $i$  is largest, i.e.,  $i = n - 1$ . So, we have:

$$n \cdot v(\alpha) \geq v(a_{n-1}) + (n - 1)v(\alpha)$$

Since  $v(a_{n-1}) \geq 0$ , this implies  $n \cdot v(\alpha) \geq (n - 1)v(\alpha)$ , which means  $v(\alpha) \geq 0$ . This contradicts our assumption that  $v(\alpha) < 0$ . Thus,  $\alpha$  must be in  $R$ .

(3)  $\Rightarrow$  (1): (This direction is more involved). Let  $R$  be integrally closed. For any two elements  $\alpha, \beta \in m$ , the transcendence degree condition ensures they are algebraically dependent over  $k$ , so there is a polynomial relationship  $F(\alpha, \beta) = 0$ . One can use this relationship to show that the element  $\alpha/\beta$  is integral over  $R[\beta]$ . Since  $R$  is integrally closed, this implies that for any  $\alpha, \beta \in m$ , either  $\alpha/\beta \in R$  or  $\beta/\alpha \in R$ . This property implies that the ideal  $m$  must be principal, hence  $R$  is a dvr.  $\square$

## 2.5 Classification of Valuations on the Rational Function Field

### Valuations on $k(x)$

We now seek to find all the valuations (and thus all the dvrs) of the rational function field  $K = k(x)$ , the function field of the affine line  $\mathbb{A}^1$ .

This problem is analogous to finding all valuations on  $\mathbb{Q}$ . For  $\mathbb{Q}$ , the discrete valuations correspond to the prime numbers  $p$ . For each prime  $p$ , the valuation ring is the localization of  $\mathbb{Z}$  at the prime ideal  $\langle p \rangle$ , denoted  $\mathbb{Z}_{(p)}$ , which is a dvr. The valuation  $v_p(a/b)$  is defined as the exponent of  $p$  in the prime factorization of  $a$  minus the exponent of  $p$  in the factorization of  $b$ . It is a known result that these, along with the trivial valuation, are all the discrete valuations on  $\mathbb{Q}$ .

For the field  $K = k(x)$ , the role of prime numbers is played by irreducible polynomials.

#### Definition 2.5.1: Localization at an Irreducible Polynomial

For any irreducible polynomial  $f \in k[x]$ , we define a subring of  $K = k(x)$  as:

$$R_f := \left\{ \frac{g}{h} \in K \mid g, h \in k[x], f \nmid h \right\}$$

This is the localization of  $k[x]$  at the prime ideal  $\langle f \rangle$ .

#### Theorem 2.5.1: Distinct Discrete Valuations on $k(x)$

The distinct dvrs (and thus the distinct non-trivial discrete valuations) of the field  $K = k(x)$  are precisely the following:

1. The rings  $R_f$  for every monic irreducible polynomial  $f \in k[x]$ .
2. A single additional ring,  $R_{x^{-1}}$ , which is defined by viewing  $x^{-1}$  as a variable and localizing the ring  $k[x^{-1}]$  at the ideal  $\langle x^{-1} \rangle$ . This is the "valuation at the point at infinity".

*Proof that these are the only ones.* Let  $R$  be a dvr whose field of fractions is  $K = k(x)$ .

Let  $m$  be its maximal ideal. We consider two cases for the element  $x \in K$ .

**Case I:**  $x \in R$ . In this case, the polynomial ring  $k[x]$  is a subring of  $R$ , i.e.,  $k[x] \subseteq R$ . Consider the ideal  $P = m \cap k[x]$ . This is a prime ideal of  $k[x]$ .

- $P$  cannot be the zero ideal  $\{0\}$ . If it were, every non-zero polynomial in  $k[x]$  would not be in  $m$ , and thus would be a unit in the local ring  $R$ . This would imply that the entire field  $k(x)$  is contained in  $R$ , so  $R = K$ , which is not a dvr (a dvr must be a proper subring of its fraction field).

- Therefore,  $P$  is a non-zero prime ideal in  $k[x]$ . Since  $k[x]$  is a Principal Ideal Domain (PID), every non-zero prime ideal is maximal and generated by a unique monic irreducible polynomial  $f(x)$ . So,  $m \cap k[x] = \langle f \rangle$  for some irreducible  $f$ .

Any element  $g/h \in K$  where  $f \nmid h$  has a denominator  $h \notin \langle f \rangle = m \cap k[x]$ . So  $h \notin m$ , which means  $h$  is a unit in  $R$ . Thus  $g/h = g \cdot h^{-1} \in R$ . This shows  $R_f \subseteq R$ . Since  $R_f$  is a dvr (and thus a maximal subring), it must be that  $R = R_f$ . The valuation  $v$  is  $v_f$ .

**Case II:**  $x \notin R$ . If  $x$  is not in  $R$ , then its valuation must be negative,  $v(x) < 0$ . For a valuation ring, this implies that the element  $x^{-1}$  must have positive valuation,  $v(x^{-1}) = -v(x) > 0$ . Therefore,  $x^{-1}$  must be in the maximal ideal  $m$ . This implies that the polynomial ring in the variable  $x^{-1}$ , denoted  $k[x^{-1}]$ , is a subring of  $R$ . We can now apply the exact same logic as in Case I, but with the ring  $k[x^{-1}]$  and variable  $y = x^{-1}$ . The ideal  $m \cap k[x^{-1}]$  is a non-zero prime ideal in  $k[x^{-1}]$ , so it must be generated by an irreducible polynomial  $f(x^{-1})$ . Since  $x^{-1} \in m$ , the generator must be  $x^{-1}$  itself (up to a constant). Thus  $m \cap k[x^{-1}] = \langle x^{-1} \rangle_{k[x^{-1}]}$ . This implies that  $R = R_{x^{-1}}$ , the ring of rational functions  $g(x)/h(x)$  such that when written in terms of  $x^{-1}$ , the denominator is not divisible by  $x^{-1}$ . This is equivalent to saying  $\deg(h) \geq \deg(g)$ . This completes the classification.  $\square$

## 2.6 Extension of Valuation Rings

### Extending to DVRs

### Curves and Function Fields

Any field  $K$  with transcendence degree  $\text{tr deg}_k(K) = 1$  can be written as a finite algebraic extension of a purely transcendental extension, i.e.,  $k(x) \subseteq K$  is a finite extension.

#### Theorem 2.6.1: Local Domain Extension to DVR

Let  $R$  be a local domain in a field  $K$ , and let  $m_R$  be its unique maximal ideal. Then, there exists a discrete valuation ring (DVR)  $B$  in  $K$ , with unique maximal ideal  $m_B$ , such that  $R \subseteq B$  and  $m_R \subseteq m_B$ .

*Proof.* If  $R$  is integrally closed in  $K$ , then  $R$  is already a DVR, and we are done.

Suppose  $R$  is not integrally closed. Consider the set  $\mathcal{F}$  of all local domains  $R'$  that dominate  $R$ :

$$\mathcal{F} = \{R' \text{ local domain} \mid R \subseteq R' \text{ and } m_R \subseteq m_{R'}\}$$

Let  $R^*$  be a maximal element in  $\mathcal{F}$  (such an element exists by Zorn's Lemma). This maximal element  $R^*$  must be integrally closed. If it were not, its integral closure would be a larger local domain dominating  $R$ , contradicting maximality.

Thus,  $R^*$  is an integrally closed local domain. A noetherian local domain of dimension 1 is a DVR if and only if it is integrally closed. Therefore,  $R^*$  is a DVR in  $K$  that extends (dominates)  $R$ .  $\square$

**Example 2.6.1: Resolving a Singularity via Extension** Consider the curve defined by  $X = Z(x_2^2 - x_1^3)$  and the local ring at the origin,  $R = A(X)_{(x_1, x_2)}$ . This ring  $R$  is not a DVR in its field of fractions  $k(X)$ .

The element  $y := x_2/x_1 \in K(X)$  is integral over  $R$  (since  $y^2 = x_1$ ), but  $y \notin R$ . We can extend the ring  $R$  by adjoining this element to get  $B = R[y]$ . This new ring is a DVR in  $K(X)$  that extends  $R$ , effectively "resolving" the singularity at the origin.

A key question arises: How do we repeat this process to resolve multiple singular points? The answer lies in the fact that an algebraic curve has only a finite number of singular points (the singular locus is a closed set).

## 2.7 Abstract Curves and Their Morphisms

### Defining Abstract Curves via Valuations

Consider any field  $K$  with  $\text{tr deg}_k(K) = 1$ . We can view this field as an "abstract curve" through the lens of its valuations.

#### Definition 2.7.1: The Set of Points on an Abstract Curve

Let  $C_K$  be the set of all discrete valuations  $v$  on  $K$ . Each valuation  $v$  corresponds to a DVR  $R_v$  with a unique maximal ideal  $m_v$ . We can think of the elements of  $C_K$  as the "points" of our curve.

We can define a topology on  $C_K$ :

- **Closed sets** are the finite subsets of  $C_K$ , along with  $C_K$  itself.
- **Open sets** are the complements of the closed sets.

### Regular Functions on Abstract Curves

#### Definition 2.7.2: Regular Functions

For any open set  $U \subseteq C_K$ , we define the ring of regular functions on  $U$  as:

$$\mathcal{O}(U) := \bigcap_{v \in U} R_v$$

Each function  $f \in \mathcal{O}(U)$  defines a map  $v \mapsto f(v)$ , where  $f(v)$  is the image of  $f$  in the residue field  $R_v/m_v \cong k$ . Two functions  $f, g \in \mathcal{O}(U)$  are the same if and only if  $f \equiv g$

(mod  $m_v$ ) for all  $v \in U$ . This means  $f - g \in \bigcap_{v \in U} m_v$ . If  $U$  is infinite, this intersection is  $\{0\}$ , so  $f = g$  in  $K$ .

### Lemma 2.7.1: Regularity Locus

For any  $f \in K$ , there exists an open set  $U \subseteq C_K$  such that  $f \in \mathcal{O}(U)$ .

*Proof.* Let  $f = g/h$  for some  $g, h$  in a polynomial ring. The function  $f$  is not defined at a valuation (point)  $v \in C_K$  if  $v(h) > 0$ , which is equivalent to  $h \in m_v$ . The set of such "bad points" where  $h$  vanishes is finite. The complement of this finite set is an open set  $U$  on which  $f$  is regular.  $\square$

### Definition 2.7.3: Abstract Curve

We call the set  $C_K$ , together with the sheaf of regular functions  $\mathcal{O}(\cdot)$  and the function field  $K$ , an **abstract curve**.

## Morphisms of Abstract Curves

### Definition 2.7.4: Morphism of Curves

A **morphism**  $\phi : X \rightarrow Y$  between two abstract curves is a continuous map such that for every open set  $V \subseteq Y$  and every regular function  $f \in \mathcal{O}_Y(V)$ , the pullback  $f \circ \phi$  is a regular function on the open set  $\phi^{-1}(V) \subseteq X$ , i.e.,  $f \circ \phi \in \mathcal{O}_X(\phi^{-1}(V))$ .

# CHAPTER 3

## DIVISORS, FUNCTION FIELDS & APPROXIMATION

---

### 3.1 Abstract Curves and Non-Singular Projective Models

There is a deep connection between abstract curves and geometric curves.

**Lemma 3.1.1:**

Every non-singular quasi-projective curve is isomorphic to an abstract curve.

*Proof Sketch.* Let  $X$  be a non-singular quasi-projective curve. We can define a map  $\phi : X \rightarrow C_{K(X)}$  by sending a point  $P \in X$  to the valuation  $v_P$  corresponding to its local ring  $\mathcal{O}_{X,P}$ . Since  $X$  is non-singular, each local ring  $\mathcal{O}_{X,P}$  is a DVR. This map can be shown to be an isomorphism.  $\square$

**Theorem 3.1.1: Non-Singular Projective Model Existence Theorem**

Let  $K$  be a field extension with  $\text{tr deg}_k(K) = 1$ . Then the abstract curve  $C_K$  is isomorphic to a non-singular projective curve.

*Proof Idea.* The idea is to "glue" together finitely many affine non-singular models, one for each "problematic" region of the curve, to form a complete non-singular projective curve.

1. For each singular point of a given projective model, we find a valuation  $v \in C_K$  that is not represented by a non-singular point on that model.
2. The DVR  $R_v$  can be realized as the local ring  $\mathcal{O}_{V,P}$  of a point  $P$  on some non-singular quasi-affine curve  $V$ . This  $V$  gives us an affine "chart" that resolves the singularity.
3. An algebraic curve has finitely many singular points, so we only need a finite number of such charts,  $\{V_i\}$ . Each chart  $V_i$  corresponds to an open set  $U_i \subseteq C_K$ . We get isomorphisms  $\phi_i : U_i \rightarrow V_i$ .
4. We can show that each  $\phi_i$  extends to a morphism  $\bar{\phi}_i : C_K \rightarrow Y_i$ , where  $Y_i$  is the projective closure of  $V_i$ . This is done by clearing denominators in the coordinate

representation of the map. If  $\phi_i(p) = (f_0(p) : \cdots : f_n(p))$  and all  $f_j(p)$  are zero at a point  $q \notin U_i$ , we can rescale by dividing by the  $f_s$  with the minimum valuation at  $q$ .

5. We combine these maps into a single "union" morphism:

$$\Phi : C_K \rightarrow Y_1 \times Y_2 \times \cdots \times Y_n$$

$$v \mapsto (\bar{\phi}_1(v), \bar{\phi}_2(v), \dots, \bar{\phi}_n(v))$$

6. Using the Segre embedding, which embeds a product of projective spaces into a larger projective space (e.g.,  $SE : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{(n+1)(m+1)-1}$ ), we embed the target space into a single  $\mathbb{P}^N$ .
7. The image  $Y = \text{cl}(\Phi(C_K))$  is the desired non-singular projective curve isomorphic to  $C_K$ .

□

This result shows that any curve (defined by its function field) is birational to a unique non-singular projective curve.

## Summary of Correspondences

- Non-singular point  $P \in X \longleftrightarrow$  The local ring  $\mathcal{O}_{X,P}$  is a DVR in  $k(X)$ .
- Tangent space rank  $\text{rk}(T_{X,P}) = 1 \longleftrightarrow T_{X,P}^* \cong m_P/m_P^2$ .
- Non-singular projective curve  $X \longleftrightarrow$  Abstract curve  $C_{k(X)}$ .

## 3.2 Points on a Smooth Projective Curve

From now on, we study only non-singular (smooth) projective curves. If  $k = \bar{k}$  (algebraically closed), any smooth projective curve  $C$  admits a finite morphism to the projective line  $\mathbb{P}^1_{\bar{k}}$ .

$$\pi : C \rightarrow \mathbb{P}^1_{\bar{k}}$$

A point  $P \in C$  corresponds to a DVR  $\mathcal{O}_{C,P}$  in the function field  $k(C)$ . The inclusion of function fields  $k(x) \hookrightarrow k(C)$  (where  $k(x)$  is the function field of  $\mathbb{P}^1_k$ ) induces the map  $\pi$ . A point  $Q \in \mathbb{P}^1_{\bar{k}}$  corresponds to a valuation on  $k(x)$ , and the points in the fiber  $\pi^{-1}(Q)$  correspond to the extensions of this valuation to  $k(C)$ . The number of points in the fiber is related to ramification.

## Correspondence between Points and Valuations

A smooth projective curve  $C$  over an algebraically closed field  $k = \bar{k}$  can be seen as a cover of the projective line  $\mathbb{P}_k^1$ .

$$\begin{array}{c} C \\ \downarrow \\ \mathbb{P}_k^1 \end{array}$$

A point  $P \in C$  corresponds to a discrete valuation ring (DVR), specifically the local ring at  $P$ , denoted  $\mathcal{O}_{C,P}$ . This gives a map from points on the curve to valuations on its function field.

The setup involves a tower of field extensions:  $k \subset k(x) \subset K := k(C)$ .

The correspondence works in both directions:

- A point  $P \in C$  gives a DVR  $\mathcal{O}_{C,P} \subset K$ . This in turn gives a point  $Q \in \mathbb{P}_k^1$  via the uniformizer. This mapping from  $C$  to  $\mathbb{P}_k^1$  can have ramification, where multiple points on  $C$  map to a single point on  $\mathbb{P}_k^1$ .
- A point  $Q \in \mathbb{P}_k^1$  gives a DVR  $R \subset k(x)$ . We can extend this valuation to a valuation (and a corresponding DVR  $\tilde{R}$ ) on the larger field  $K = k(C)$ . This gives a point  $P \in C$  via the uniformizer of  $\tilde{R}$ . Note that the extension of the DVR from  $k(x)$  to  $K(C)$  is not necessarily unique, and neither is the resulting point  $P$ .

**Exercise** For a finite field  $\mathbb{F}_q$ , what is the value of  $|C(\mathbb{F}_q)| - |\mathbb{P}^1(\mathbb{F}_q)| = |C(\mathbb{F}_q)| - (q+1)$ ?

A point corresponds to a DVR in  $K$ ; it may be a cluster of points over the algebraic closure.

### Definition 3.2.1: Point on a Curve

Let  $K$  be the function field of a curve  $C$  over  $k = \mathbb{F}_q$ . A point  $P$  on the curve defines a valuation  $v_P$  on  $K$ , given by the DVR  $\mathcal{O}_{C,P}$ .

## Degree of a Point

### Definition 3.2.2: Residue Field and Degree of a Point

The **residue field** at a point  $P$  is  $k_P := \mathcal{O}_{C,P}/m_P$ , where  $m_P$  is the maximal ideal of the local ring  $\mathcal{O}_{C,P}$ . The residue field  $k_P$  is a finite extension of the base field  $k$ .

### Definition 3.2.3: Degree of a Point

The **degree** of a point  $P$  is defined as  $d(P) := [k_P : k]$ .

**Proposition 3.2.1: Properties of Degree and Valuation at a Point**

Let  $P$  be a point on a smooth curve  $C$  with function field  $K$ . Let  $m_P$  be the maximal ideal of  $\mathcal{O}_{C,P}$  and let  $v_P$  be the corresponding valuation.

- (i) The degree  $d(P)$  is finite.
- (ii)  $\bigcap_{i>0} m_P^i = \{0\}$ .
- (iii) If  $m_P = \langle u \rangle$  (where  $u$  is a uniformizer), then for any  $\alpha \in K$ ,  $v_P(\alpha)$  is the largest integer  $i$  such that  $\alpha \in u^i \mathcal{O}_{C,P}$ .

*Proof.* (i) Let  $m_P = \langle u \rangle \mathcal{O}_{C,P}$ . The degree can be interpreted geometrically as the number of points in the intersubsection of the zero locus of the uniformizer with the curve over the algebraic closure,  $d(P) = |Z(u) \cap C(\bar{k})|$ , which is finite. Algebraically, this corresponds to the number of conjugates of the point under the Galois action of  $k_P/k$ .

(ii) Let  $y \in \bigcap_{i>0} u^i$ . By Krull's Intersubsection Theorem for the local ring  $\mathcal{O}_{C,P}$ , this implies  $y = 0$ .

(iii) This is clear from the definition of the valuation associated with a DVR.  $\square$

### 3.3 Approximation Theorems

Any function  $f \in K(C)$  gives rise to a sequence of integers  $\{v_P(f)\}_{P \in C}$ . A natural question arises: given such a sequence, does a corresponding function  $f$  exist? Generally, the answer is no. However, we can show that a function  $f$  can be constructed to match any finite part of such a sequence. This is the essence of the Approximation Theorem.

#### Weak Approximation Theorem

**Theorem 3.3.1: Weak Approximation Theorem**

Let  $K$  be the function field of a curve  $C$ . Let  $P_1, \dots, P_h \in C$  be distinct points with corresponding valuations  $v_1, \dots, v_h$ . Let  $u_1, \dots, u_h \in K$  and  $m_1, \dots, m_h \in \mathbb{Z}$ . Then, there exists an element  $u \in K$  such that for all  $i \in \{1, \dots, h\}$ , we have  $v_i(u - u_i) \geq m_i$ .

*Proof.* The proof relies on several claims.

**Lemma 3.3.1: Claim 1**

Given distinct valuations  $v_1, \dots, v_{h-1}$  and integers  $e_1, \dots, e_{h-1} \in \mathbb{Z}$ , there exists an element  $u \in K$  such that  $v_i(u) = e_i$  for all  $i \in \{1, \dots, h-1\}$ .

*Proof of Claim 1.* For each  $i \in \{1, \dots, h-1\}$ , we can find  $w_i \in K$  such that  $v_i(w_i) = e_i$ . Now consider the system of congruences:

$$v_i(u - w_i) \geq e_i + 1 \quad \forall i \in \{1, \dots, h-1\}$$

By the induction hypothesis of the main theorem (assuming it holds for  $h - 1$  points), such a  $u \in K$  exists. We can then check the valuation of  $u$ :

$$v_i(u) = v_i(w_i + (u - w_i))$$

Since  $v_i(u - w_i) \geq e_i + 1 > e_i = v_i(w_i)$ , the properties of non-archimedean valuations imply that  $v_i(u) = v_i(w_i) = e_i$ .  $\square$

### Lemma 3.3.2: Claim 2

The valuations  $v_1, \dots, v_h$  corresponding to distinct points  $P_1, \dots, P_h$  are  $\mathbb{Q}$ -linearly independent.

*Proof of Claim 2.* Suppose not. Then there exists a non-trivial relation  $\sum_{i=1}^h \lambda_i v_i(u) = 0$  for all  $u \in K$ , with  $\lambda_i \in \mathbb{Q}$ . Without loss of generality, let  $\lambda_h = -1$ , so  $v_h(u) = \sum_{i=1}^{h-1} \lambda_i v_i(u)$ .

Consider the base case  $h = 2$ , with  $v_2(u) = \lambda_1 v_1(u)$ . If we assume  $\lambda_1 > 0$ , this implies that for any  $z \in K$ ,  $v_1(z) \geq 0 \iff v_2(z) \geq 0$ . This means their corresponding valuation rings are identical:  $R_{v_1} = R_{v_2}$ . For valuations arising from points on a curve, this implies that the points themselves are identical,  $P_1 = P_2$ , which contradicts our assumption that the points are distinct. A similar argument holds for  $\lambda_1 < 0$ . The general case for  $h > 2$  can be reduced to this case.  $\square$

### Lemma 3.3.3: Claim 3

There exist elements  $z_1, \dots, z_h \in K^*$  such that the matrix  $U = (v_i(z_j))_{h \times h}$  is invertible (i.e., its determinant is non-zero).

*Proof of Claim 3.* This is a direct consequence of the  $\mathbb{Q}$ -linear independence of the valuations  $v_1, \dots, v_h$ . We can inductively find elements  $z_1, \dots, z_h$  such that the vectors  $(v_1(z_j), \dots, v_h(z_j))$  for  $j = 1, \dots, h$  are linearly independent over  $\mathbb{Q}$ .  $\square$

### Construction of the element $u$

Now, we construct the element  $u$  for the theorem. We first construct auxiliary elements  $y_m$  with specific valuation properties. Let  $U = (v_i(z_j))$  be the invertible matrix from Claim 3. We can solve the matrix equation  $U \cdot C = A$  for a matrix  $C = (c_{jm})$ , where  $A$  is the  $h \times h$  matrix with  $-1$  on the diagonal and  $1$  everywhere else.

$$\sum_{j=1}^h c_{jm} v_i(z_j) = \begin{cases} -1 & \text{if } i = m \\ 1 & \text{if } i \neq m \end{cases}$$

Let  $d$  be an integer that clears the denominators of the rational entries  $c_{jm}$ , so  $d \cdot c_{jm} \in \mathbb{Z}$

for all  $j, m$ . Define  $y_m$  for  $m \in \{1, \dots, h\}$  as:

$$y_m := \prod_{j=1}^h z_j^{d \cdot c_{jm}}$$

The valuation of  $y_m$  at  $P_i$  is then:

$$v_i(y_m) = \sum_{j=1}^h (d \cdot c_{jm}) v_i(z_j) = d \sum_{j=1}^h c_{jm} v_i(z_j) = \begin{cases} -d & \text{if } i = m \\ d & \text{if } i \neq m \end{cases}$$

Now define  $x_m \in K^*$  for  $m \in \{1, \dots, h\}$  as:

$$x_m := (1 + y_m^{-1})^{-1} = \frac{y_m}{y_m + 1}$$

Let's choose  $d > 0$ . The valuations of  $x_m$  and  $x_m - 1$  are as follows:

- For  $i \neq m$ :  $v_i(y_m) = d > 0$ , so  $v_i(y_m^{-1}) = -d < 0$ . Thus,  $v_i(1 + y_m^{-1}) = v_i(y_m^{-1}) = -d$ . This gives  $v_i(x_m) = -v_i(1 + y_m^{-1}) = d$ .
- For  $i = m$ :  $v_m(y_m) = -d < 0$ , so  $v_m(y_m^{-1}) = d > 0$ . Thus,  $v_m(1 + y_m^{-1}) = v_m(1) = 0$ . This gives  $v_m(x_m) = 0$ .
- For  $i = m$ , we also compute  $v_m(x_m - 1) = v_m(\frac{-1}{y_m+1})$ . Since  $v_m(y_m) = -d < 0$ ,  $v_m(y_m + 1) = v_m(y_m) = -d$ . Therefore,  $v_m(x_m - 1) = -v_m(y_m + 1) = d$ .

Finally, we define our desired element  $u$  as a linear combination of the target elements  $u_i$ :

$$u := \sum_{m=1}^h x_m u_m$$

Let's check the condition  $v_i(u - u_i) \geq m_i$ . We can write  $u - u_i$  as:

$$u - u_i = (x_i - 1)u_i + \sum_{m \neq i} x_m u_m$$

Now we evaluate  $v_i$  of each term:

- $v_i((x_i - 1)u_i) = v_i(x_i - 1) + v_i(u_i) = d + v_i(u_i)$
- $v_i(x_m u_m) = v_i(x_m) + v_i(u_m) = d + v_i(u_m)$  for  $m \neq i$

Using the property  $v(A + B) \geq \min(v(A), v(B))$ , we get:

$$v_i(u - u_i) \geq \min(d + v_i(u_i), \min_{m \neq i} \{d + v_i(u_m)\}) = d + \min_{m \in \{1, \dots, h\}} \{v_i(u_m)\}$$

We can choose the integer  $d$  to be large enough such that for all  $i \in \{1, \dots, h\}$ :

$$d + \min_{m \in \{1, \dots, h\}} \{v_i(u_m)\} \geq m_i$$

Such a  $d$  exists because the set of points and target values is finite. This completes the proof.  $\square$

**Corollary 3.3.1: Corollary: Existence of Functions with Prescribed Zeros and Poles**  
**Let  $S \subset C$  be a finite set of points. Let  $\{m_P | P \in S\} \subset \mathbb{Z}$  be a set of prescribed integer orders. Then there exists a function  $f \in K(C)^*$  such that  $v_P(f) = m_P$  for all  $P \in S$ .**

*Proof.* This is a direct application of the construction used to prove Claim 1, which itself relies on the main theorem.  $\square$

**Warning 3.3.1:** The function  $f$  is only guaranteed to have the specified orders at the points in  $S$ . The full set of its zeros and poles,  $Z(f) \cup Z(1/f)$ , may be strictly larger than  $S$ .

## 3.4 Divisors on Smooth Projective Curves

### Definition and Examples

**Definition 3.4.1: Group of Divisors**

The free abelian group  $\text{Div}(C) = \bigoplus_{P \in C} \mathbb{Z}P$  is the group of divisors of a smooth projective curve. ( $P \in C$  iff  $\mathcal{O}_{C,P}$  is a DVR in  $k(C)$ ).

**Note:**  $d(P)$  may not be equal to 1.

**Example 3.4.1:**

- $(P_1 + P_2) + (P_2 - P_1 + P_3) = 2P_2 + P_3$
- $P_1 - P_1 = 0$

Elements of  $\text{Div}(C)$  have finite support by definition. Therefore,  $\sum_{i=1}^{\infty} P_i$  is not in  $\text{Div}(C)$ .

### Maps on Divisors

Any element  $D \in \text{Div}(C)$  is a divisor.

- **Define the order map**,  $\text{ord}_P : \text{Div}(C) \rightarrow \mathbb{Z}$  such that for  $D = \sum_{P \in C} a_P P$ , the map is  $D \mapsto a_P$ .

The map  $\text{ord}_P$  is a group homomorphism.

- **Define the degree map**,  $d : \text{Div}(C) \rightarrow \mathbb{Z}$  such that for  $D = \sum_{P \in C} a_P P$ , the map is  $D \mapsto \sum_{P \in C} a_P d(P)$ .

The map  $d(\cdot)$  is a group homomorphism.

- The kernel of the degree map,  $\ker(d)$ , is the group of degree-0 divisors, denoted by  $\text{Div}_0(C)$ .

## Effective and Integral Divisors

- The **support of D** is defined as  $\text{supp}(D) := \{P \in C \mid \text{ord}_P(D) \neq 0\}$ .
- A divisor  $D$  is called **integral/positive/effective** if  $\forall P \in C, \text{ord}_P(D) \geq 0$ . We write this as  $D \geq 0$ .
- We say  $D_1$  **divides**  $D_2$  if  $D_2 - D_1 \geq 0$ . We write this as  $D_2 \geq D_1$  or  $D_1 \leq D_2$ .

These divisors (written additively) are new objects.

## Principal Divisors

Divisors are interesting because each rational function  $x \in K^*$  has an associated **principal divisor**, defined as:

$$(x) := \sum_{P \in C} v_P(x) \cdot P \in \text{Div}(C)$$

This is well-defined because  $v_P(x) \neq 0$  for only finitely many  $P \in C$ .

## Example Calculation

Let  $C = Z(x_2^2 x_0 - x_1^3 + x_1 x_0^2) \subset \mathbb{P}_k^2$ . For  $f := x_1/x_2 \in K(C)$ , what is  $(f)$ ?

- $P_1 = \langle x_1, x_0 \rangle = \langle x_1 \rangle_{R_{P_1}}$   
 $v_{P_1}(f) = v_{P_1}(x_1) - v_{P_1}(x_2) = 1 - 0 = 1$ .
- $P_2 = \langle x_1, x_2 \rangle = \langle x_2 \rangle_{R_{P_2}}$   
 $v_{P_2}(f) = v_{P_2}(x_1) - v_{P_2}(x_2) = 2 - 1 = 1$ .
- $P_3 = \langle x_2, x_1 + x_0 \rangle = \langle x_2 \rangle_{R_{P_3}}$  (up to units in  $R_{P_3}$ )  
 $v_{P_3}(f) = v_{P_3}(x_1) - v_{P_3}(x_2) = 0 - 1 = -1$ .

- $P_4 = \langle x_2, x_1 - x_0 \rangle = \langle x_2 \rangle_{R_{P_4}}$  (up to units in  $R_{P_4}$ )
- $$v_{P_4}(f) = v_{P_4}(x_1) - v_{P_4}(x_2) = 0 - 1 = -1.$$

So, the principal divisor is:

$$(x_1/x_2) = P_1 + P_2 - P_3 - P_4 \in \text{Div}(C)$$

Note that  $d((f)) = 0$ , which implies  $(f) \in \text{Div}_0(C)$ . We will later prove this for all principal divisors.

**Question:** Is the converse true? i.e.,  $\forall D \in \text{Div}_0(C)$ , does there exist an  $f \in K$  such that  $D = (f)$ ?

## Principal Divisor Group

### Proposition 3.4.1:

The set  $\text{Div}_a(C) := \{(x) \mid x \in K^*\}$  is a subgroup of  $\text{Div}(C)$ .

*Proof.*  $(x) + (y) = (xy), \forall x, y \in K^*$ . This follows from the valuation axiom  $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ .  $\square$

We have the following subgroup relationships:  $\text{Div}_a(C) \triangleleft \text{Div}_0(C) \triangleleft \text{Div}(C)$ . Our long-term goal is to compare these subgroups quantitatively.

# CHAPTER 4

## ZETA FUNCTION OF A CURVE OVER FINITE FIELDS

---

### 4.1 Counting Points on Curves over Finite Fields

#### Points on Curves and the Setup

Let  $C$  be a smooth projective curve defined over a finite field  $k = \mathbb{F}_q$ , where  $q = p^e$  for some prime  $p$ . The function field of  $C$  is denoted by  $K$ .

Let  $k = \mathbb{F}_q$ . Our goal is to count the number of points on the curve  $C$  over finite extensions of  $k$ . For any positive integer  $n \in \mathbb{N}_{>0}$ , we define  $N_n$  as the number of points on  $C$  defined over the extension field  $\mathbb{F}_{q^n}$ :

$$N_n := |C(\mathbb{F}_{q^n})|.$$

#### Closed Points and Residue Fields

A closed point  $P \in C$  corresponds to a Galois orbit of points over the algebraic closure  $\bar{k}$ . The residue field at  $P$ , denoted  $k(P)$ , is a finite extension of  $k$ . The degree of the point  $P$ , denoted  $d(P)$ , is the degree of this field extension:

$$d(P) = [k(P) : k].$$

A point is in  $C(\mathbb{F}_{q^n})$  if and only if its residue field  $k(P)$  is a subfield of  $\mathbb{F}_{q^n}$ , which occurs precisely when  $d(P)$  divides  $n$ . In this case, the closed point  $P$  contributes exactly  $d(P)$  points to  $C(\mathbb{F}_{q^n})$ .

Therefore, we can write

$$N_n = \sum_{\substack{P \in C \\ d(P) | n}} d(P).$$

## 4.2 The Zeta Function: Definition and Basic Properties

### Definition of the Zeta Function

To study the sequence of numbers  $\{N_n\}_{n \geq 1}$ , it is useful to encode them in a generating function:

$$G(t) := \sum_{n \geq 1} N_n t^n \in \mathcal{Z}[[t]]$$

However, a more structured object, called the Zeta function of  $C$  over  $k$ , proves to be better behaved.

#### Definition 4.2.1: Zeta Function

The Zeta function of the curve  $C$  over  $k$  is the formal power series  $Z(t) \in \mathcal{Z}[[t]]$  defined by the Euler product:

$$Z(t) := \prod_{P \in C} (1 - t^{d(P)})^{-1}$$

where the product is taken over all closed points  $P$  of the curve  $C$ .

By expanding each term in the product as a geometric series,  $(1 - t^{d(P)})^{-1} = \sum_{i=0}^{\infty} t^{i \cdot d(P)}$ , we can see the connection to effective divisors. An effective divisor is a formal sum  $D = \sum_P n_P P$  where  $n_P \geq 0$  are integers and almost all are zero. The degree of such a divisor is  $d(D) = \sum_P n_P d(P)$ . The product expansion gives:

$$Z(t) = \prod_{P \in C} \left( \sum_{i=0}^{\infty} t^{i \cdot d(P)} \right) = \sum_{D \geq 0} t^{d(D)}$$

where the final sum is taken over all effective divisors  $D$  on  $C$ .

### Reorganizing the Zeta Function by Divisor Classes

We can group the terms in the sum  $\sum_{D \geq 0} t^{d(D)}$  by the degree of the divisor. The degree map  $d : \text{Div}(C) \rightarrow \mathcal{Z}$  is a group homomorphism. Its image is a subgroup of  $\mathcal{Z}$ , and hence must be of the form  $\delta \mathcal{Z}$  for some integer  $\delta \geq 1$ .

We can stratify the sum by first summing over degrees  $d \in \delta \mathcal{Z}_{\geq 0}$ , then over divisor classes  $\mathcal{D}$  of degree  $d$ , and finally over effective divisors  $D$  within that class:

$$Z(t) = \sum_{d \in \delta \mathcal{Z}_{\geq 0}} \sum_{\mathcal{D} \in \text{Cl}_d(C)} \sum_{D \in \mathcal{D}, D \geq 0} t^d$$

where  $\text{Cl}_d(C)$  is the set of divisor classes of degree  $d$ .

To evaluate this, we need to count the number of effective divisors in a given class.

**Lemma 4.2.1: Counting Effective Divisors in a Class**

Let  $\mathcal{D}$  be a divisor class. The number of effective divisors in  $\mathcal{D}$  is given by

$$|\{D \in \mathcal{D} \mid D \geq 0\}| = \frac{q^{l(D_0)} - 1}{q - 1}$$

where  $D_0$  is any divisor in  $\mathcal{D}$  and  $l(D_0) = \dim_k H^0(C, \mathcal{O}(D_0))$  is the dimension of the Riemann-Roch space  $L(D_0)$ .

*Proof.* Fix a divisor  $D_0 \in \mathcal{D}$ . Any other divisor  $D' \in \mathcal{D}$  is linearly equivalent to  $D_0$ , meaning  $D' - D_0 = (f)$  for some function  $f \in K^\times$ , where  $K$  is the function field of  $C$ . The condition  $D' \geq 0$  is equivalent to  $(f) + D_0 \geq 0$ , which means  $f \in L(D_0) \setminus \{0\}$ .

Two functions  $f_1, f_2 \in L(D_0) \setminus \{0\}$  define the same divisor if and only if  $(f_1) = (f_2)$ , which means  $f_1 = c \cdot f_2$  for some constant  $c \in k^\times = \mathbb{F}_q^\times$ . Therefore, the number of distinct effective divisors in  $\mathcal{D}$  is the number of 1-dimensional subspaces in the  $k$ -vector space  $L(D_0)$ . This is the number of points in the projective space  $\mathbb{P}(L(D_0))$ , which is

$$\frac{|L(D_0)| - 1}{|k^\times|} = \frac{q^{l(D_0)} - 1}{q - 1}$$

□

## Divisor Class Groups and the Class Number

Next, we relate the number of divisor classes of different degrees.

**Lemma 4.2.2: Cardinality of Divisor Classes**

For any degree  $d \in \delta\mathcal{Z}$ , the set of divisor classes  $\text{Cl}_d(C)$  has the same cardinality as the set of degree-0 divisor classes,  $\text{Cl}_0(C)$ :

$$|\text{Cl}_d(C)| = |\text{Cl}_0(C)|$$

*Proof.* Fix a divisor  $D_0$  of degree  $d$ . The map  $\mathcal{D} \mapsto \mathcal{D} - [D_0]$  is a bijection from  $\text{Cl}_d(C)$  to  $\text{Cl}_0(C)$ . □

An important fact is that  $\text{Cl}_0(C)$  is a finite group.

**Definition 4.2.2: Class Number**

The **class number** of  $C$  over  $k$ , denoted  $h(C)$ , is the size of the degree-0 divisor class group:

$$h(C) := |\text{Cl}_0(C)|$$

Using these results, we can rewrite the formula for  $Z(t)$ . For any given degree  $d$ , the dimension  $l(D)$  is the same for all divisors  $D$  belonging to classes of degree  $d$  if  $d$  is large enough, but not necessarily for small  $d$ . The notes simplify this by writing  $l(D)$  as if it only depends on  $d$ . Let's denote the sum over classes as an average. Summing over all effective divisors of degree  $d$ :

$$\sum_{D \in \text{Cl}_d(C)} \frac{q^{l(D_D)} - 1}{q - 1} = \frac{h(C)}{q - 1} \left( \sum_{D \in \text{Cl}_d(C)} q^{l(D_D)} \right) - \frac{h(C)}{q - 1}$$

where  $D_D$  is any divisor in class  $\mathcal{D}$ . The expression for  $Z(t)$  becomes:

$$Z(t) = \sum_{d \in \delta \mathbb{Z}_{\geq 0}} \left( \sum_{D \in \text{Cl}_d(C)} \frac{q^{l(D_D)} - 1}{q - 1} \right) t^d$$

## Convergence and the Analytic Zeta Function

### Proposition 4.2.1: Convergence of $Z(t)$ and $\zeta(s)$

The power series  $Z(t)$  converges for all  $t \in \mathbb{C}$  with  $|t| < q^{-1}$ . Let  $t = q^{-s}$ . Then the function  $\zeta(s, C) := Z(q^{-s})$  is defined by the series

$$\zeta(s, C) = \sum_{D \geq 0} N(D)^{-s} = \prod_{P \in C} (1 - N(P)^{-s})^{-1}$$

where  $N(P) := q^{d(P)}$  is the norm of the prime divisor  $P$ . This series converges for  $\Re(s) > 1$ . This function is analogous to the Riemann zeta function  $\zeta(s) = \sum_{n \geq 1} n^{-s}$ .

## 4.3 Rationality, Functional Equation, and Fundamental Properties

### Rationality and the Functional Equation

#### Theorem 4.3.1: Rationality and Functional Equation

Let  $g$  be the genus of the curve  $C$ .

- (i) The zeta function  $Z(t)$  is a rational function of  $t$ , i.e.,  $Z(t) \in \mathbb{Q}(t)$ .
- (ii)  $Z(t)$  satisfies the following functional equation:

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

*Proof Sketch.* From the previous subsection, we have  $(q - 1)Z(t) = \sum_{D \geq 0} (q^{l(D)} - 1)t^{d(D)}$ .

We can write this as:

$$(q - 1)Z(t) = \sum_{d,\mathcal{D}} h(C)q^{l(D)}t^d - \sum_{d,\mathcal{D}} h(C)t^d$$

The second sum is a geometric series:  $\sum_{d \in \delta \mathcal{Z}_{\geq 0}} h(C)t^d = \frac{h(C)}{1-t^\delta}$ .

For the first sum,  $\sum h(C)q^{l(D)}t^d$ , we use the Riemann-Roch theorem. The canonical divisor class  $W$  has degree  $d(W) = 2g - 2$ . We split the sum over degrees  $d$  into two parts:  $0 \leq d \leq 2g - 2$  and  $d > 2g - 2$ . Let's assume for simplicity that  $\delta = 1$ . Let  $S_1 = \sum_{d=0}^{2g-2} \sum_{\mathcal{D} \in \text{Cl}_d(C)} h(C)q^{l(D)}t^d$  and  $S_2 = \sum_{d=2g-1}^{\infty} \sum_{\mathcal{D} \in \text{Cl}_d(C)} h(C)q^{l(D)}t^d$ .  $S_1$  is a finite sum, hence a polynomial in  $t$ .

For  $d > 2g - 2$ , the Riemann-Roch theorem states  $l(D) = d + 1 - g$ . Thus,  $l(D)$  only depends on the degree  $d$ .

$$S_2 = \sum_{d=2g-1}^{\infty} h(C)q^{d+1-g}t^d = h(C)q^{1-g} \sum_{d=2g-1}^{\infty} (qt)^d$$

This is a geometric series which sums to a rational function:

$$S_2 = h(C)q^{1-g} \frac{(qt)^{2g-1}}{1 - qt}$$

Since  $(q - 1)Z(t) = S_1 + S_2 - \frac{h(C)}{1-t}$ , and all terms on the right are rational functions,  $Z(t)$  must be a rational function.

To prove the functional equation, one shows that the expression for  $Z(t)$  is invariant under the transformation  $t \mapsto \frac{1}{qt}$  up to the factor  $(qt^2)^{g-1}$ . This is done by applying the Riemann-Roch theorem in the form  $l(D) = d(D) + 1 - g + l(W - D)$  to the sum  $S_1$ . This relates the sum over degrees  $d \in [0, 2g - 2]$  to itself in a symmetric way. The notes show this for functions  $F(t)$  and  $G(t)$  which correspond to the sums, eventually yielding:

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

which is equivalent to the stated functional equation. □

## Consequences of the Functional Equation

**Corollary 4.3.1: Functional Equation for  $\zeta(s, C)$**  The function  $\zeta(s, C)$  has a meromorphic continuation to all  $s \in \mathbb{C}$  and satisfies the functional equation:

$$\zeta(1 - s, C) = (q^{2g-2})^{s-1/2} \zeta(s, C)$$

This reveals a symmetry about the critical line  $\Re(s) = 1/2$ .

**Corollary 4.3.2: Explicit Form and Simple Poles** The zeta function can be written in the form

$$Z(t, C) = \frac{L(t, C)}{(1-t)(1-qt)}$$

where  $L(t, C) \in \mathbb{Z}[t]$  is a polynomial of degree  $2g$ . The poles of  $Z(t)$  are simple poles at  $t = 1$  and  $t = 1/q$ . This implies that  $\delta = 1$ .

## 4.4 Behavior under Base Change

### Zeta Function under Field Extensions

We now consider how the zeta function changes when we extend the base field from  $k = \mathbb{F}_q$  to  $k_n = \mathbb{F}_{q^n}$ . Let  $C_n$  be the curve  $C$  considered over the field  $k_n$ .

#### Theorem 4.4.1: Base Change Formula

The zeta function of  $C_n$  over  $k_n$  is related to the zeta function of  $C$  over  $k$  by the following identity:

$$Z(t^n, C_n) = \prod_{\eta^n=1} Z(\eta t, C)$$

where the product is over all  $n$ -th roots of unity  $\eta$ .

*Proof Sketch.* We compare the Euler products on both sides. Let  $P$  be a closed point of  $C$  over  $k$  with degree  $d(P)$ . Over the extension field  $k_n$ , the point  $P$  splits into  $e$  closed points  $Q_1, \dots, Q_e$  of  $C_n$ . The number of points is  $e = \gcd(n, d(P))$ . The degree of each new point  $Q_i$  over  $k_n$  is  $d'(Q_i) = d(P)/e$ .

The contribution from the points  $\{Q_i\}$  to the LHS,  $Z(t^n, C_n)$ , is:

$$\prod_{i=1}^e \left(1 - (t^n)^{d'(Q_i)}\right)^{-1} = \left(1 - t^{n \cdot d(P)/e}\right)^{-e}$$

. The contribution from the point  $P$  to the RHS,  $\prod_{\eta^n=1} Z(\eta t, C)$ , is:

$$\prod_{\eta^n=1} \left(1 - (\eta t)^{d(P)}\right)^{-1}$$

. The theorem follows from the algebraic identity:

$$(1 - X^{n/e})^e = \prod_{\eta^n=1} (1 - (\eta Y)^{d/e})$$

where  $X = t^{d(P)}$ ,  $Y = t$ ,  $d = d(P)$ . Let  $u = t^{d(P)}$  and  $m = d(P)$ . We need to prove

that  $(1 - u^{n/e})^e = \prod_{\eta^n=1} (1 - \eta^m u)$ . A standard identity is  $\prod_{\zeta^k=1} (1 - \zeta x) = 1 - x^k$ . Let  $d = d(P)$ . As  $\eta$  runs through the  $n$ -th roots of unity,  $\eta^d$  runs through the  $(n/e)$ -th roots of unity, with each root appearing  $e$  times. Therefore,

$$\prod_{\eta^n=1} (1 - (\eta t)^d) = \prod_{\eta^n=1} (1 - \eta^d t^d) = \left( \prod_{\zeta^{n/e}=1} (1 - \zeta t^d) \right)^e = (1 - (t^d)^{n/e})^e = (1 - t^{nd/e})^e$$

Taking the reciprocal of both sides proves that the factors are equal, and thus the identity holds.  $\square$

## GCD of Point Degrees

**Corollary 4.4.1: GCD of Degrees is 1** The integer  $\delta = \gcd_{P \in C} \{d(P)\}$  must be 1.

*Proof Sketch.* The poles of  $Z(t, C)$  are related to the roots of  $(1 - t^\delta)$  and  $(1 - (qt)^\delta)$ . If  $\delta > 1$ , the poles would be at the  $\delta$ -th roots of unity (and  $1/q$  times these roots). Consider the base change to  $k_\delta = \mathbb{F}_{q^\delta}$ . From the theorem:

$$Z(t^\delta, C_\delta) = \prod_{\eta^\delta=1} Z(\eta t, C) = \prod_{\eta^\delta=1} \frac{L(\eta t, C)}{(1 - \eta t)(1 - q\eta t)}$$

The product in the denominator is  $(1 - t^\delta)(1 - (qt)^\delta)$ . This implies that  $Z(T, C_\delta)$ , with  $T = t^\delta$ , has poles at  $T = 1$  and  $T = 1/q$ . This means the gcd of degrees of points on  $C_\delta$  is 1. By construction, for any point  $P$  on  $C$  of degree  $d(P)$ , its split components on  $C_\delta$  have degree  $d(P)/\gcd(\delta, d(P))$ . Since  $\delta$  divides all  $d(P)$ , this degree is  $d(P)/\delta$ . The gcd of these new degrees is  $\frac{1}{\delta} \gcd(d(P)) = \frac{\delta}{\delta} = 1$ . This is consistent. The Weil bounds imply the existence of a rational point over some finite extension, which can be used to show  $\delta = 1$  if the base field is chosen appropriately (e.g., large enough). The notes suggest this is a direct corollary of the base change formula itself, likely by analyzing and comparing the pole structures.  $\square$

# CHAPTER 5

## WEIL BOUNDS, COHOMOLOGY & L-FUNCTIONS

---

### 5.1 L-Functions and Zeta Functions

#### Zeta Function and L-Functions

On the other hand,

$$\begin{aligned} Z(t, c_\delta) &:= \frac{L'(t)}{(1 - t^8) \cdot (1 - qt^9)} \\ \Rightarrow Z(t^8, c_\delta) &= \frac{L'(t^8)}{(1 - t^{88}) \cdot (1 - q^8 \cdot t^{88})} \end{aligned}$$

which has only simple poles.

$\Rightarrow$  The two expressions imply  $\delta = 1$ .

- Note that  $L(0) = Z(0) = 1$ .
- Also,  $(q - 1) \cdot Z(t) \cdot (t - 1)|_{t=1} = h(c)$  [as ??=1].  
 $(-1) \cdot \frac{L(t)}{qt-1}|_{t=1} = h(c) \Rightarrow L(1) = h(c)$ .

#### Theorem 5.1.1: L-function

(i) We've an exact sequence

$$\mathrm{Pic}^0(C) \rightarrow \mathbb{Z} \rightarrow 0.$$

(ii)  $Z(t, C) = L(t)/((1 - t)(1 - qt))$

where  $L(t) \in \mathcal{Z}[t]$  has  $\deg = 2g$  &

$$L(t) = (qt^2)^g \cdot L(1/qt)$$

(iii)  $L(0) = 1$  &  $L(1) = h(C)$ .

#### Computational Questions

Qn. Can we compute  $D \in \mathcal{C}^{-1}(1)$ ?

Qn. Can we compute  $L(t)$  efficiently, given  $C/k$ ?

## 5.2 Point Counting via Zeta Functions

### Euler Product and Log-Derivative

Consequences to counting pts.

- Euler product:  $Z = Z(t, C) = \prod_{P \in C} (1 - t^{\deg(P)})^{-1}$ .
- Idea: Use dlog (log-derivative operator). [ $\text{dlog } f = f'/f$ ]

$$\begin{aligned} d \log Z &= \sum_{P \in C} d \log(1 - t^{\deg(P)})^{-1} \\ &= \sum_{P \in C} \frac{\deg(P) \cdot t^{\deg(P)-1}}{(1 - t^{\deg(P)})} \\ &= t^{-1} \cdot \sum_{P \in C} \deg(P) \cdot \sum_{n \geq 1} t^{n \cdot \deg(P)} \\ &= t^{-1} \cdot \sum_{m \geq 1} t^m \left( \sum_{P \in C: \deg(P) | m} \deg(P) \right) = t^{-1} \cdot \sum_{m \geq 1} N_m \cdot t^m \end{aligned}$$

### Zeta Function Log Formula

- Definite integration  $\int_0^t$  gives:

#### Proposition 5.2.1: Zeta Function Log Formula

$$\log Z(t) = \sum_{m \geq 1} N_m \frac{t^m}{m}.$$

### L-Function Factorization

- $Z(t) = \exp \left( \sum_{m \geq 1} N_m \cdot \frac{t^m}{m} \right)$ .
  - Now, use
- $$Z(t) = \frac{L(t)}{(1-t)(1-qt)} = \frac{\prod_{i=1}^{2g} (1 - \alpha_i t)}{(1-t)(1-qt)}$$
- $(L(0) = 1, \text{ reciprocal roots of } L \text{ are } \alpha_i)$
- Plugging in the first formula above, we get:

$$\log Z(t) = \sum_{i=1}^{2g} \log(1 - \alpha_i t) - \log(1 - t) - \log(1 - qt)$$

Comparing the series expansion of this with  $\log Z(t) = \sum_{m \geq 1} N_m \cdot \frac{t^m}{m}$  yields:

$$N_m = q^m + 1 - \sum_{i=1}^{2g} \alpha_i^m$$

The term  $\sum_{i=1}^{2g} \alpha_i^m$  is viewed as the error-term.

## Error Term Analysis

Qn. How big can the error be?

- By functional equation symmetry we get: We can label  $\alpha_i$ 's s.t.  $\alpha_i \cdot \alpha_{i+g} = q$ ,  $\forall i \in \{1, \dots, g\}$ .

## 5.3 Riemann Hypothesis for Curves over Finite Fields

### The Riemann Hypothesis Conjecture

- RH conjectures a strong symmetry, namely

$$|\alpha_i| = \sqrt{q} = q^{1/2}$$

- In terms of  $Z(s, C) = Z(q^{-s}, C)$ , it means that the zeros of  $Z$  are on the line  $Re(s) = \frac{1}{2}$  [just like the original unproved RH!]
- It means:  $|N_m - (q^m + 1)| = |\sum_{i=1}^{2g} \alpha_i^m| \leq \sum_{i=1}^{2g} |\alpha_i|^m \leq 2g \cdot q^{m/2}$ .

### Hasse-Weil Bound

RH  $\Rightarrow$  #pts on a curve (smooth projective) are in the range  $q + 1 \pm 2g\sqrt{q}$ .

- We'll prove RH by doing a sequence of reductions, and finally using the  $l(D)$ -sheaf.

### Base-Change Reduction

#### Proposition 5.3.1: Base-change

RH is true for  $Z(t, C)$  iff RH is true for  $Z(t, C_n)$ , for  $n > 1$ .

*Proof.* We know  $Z(t, C)$  ...

We've:  $(1 - \beta t)$  is a factor of  $Z(t, C_n) \iff (1 - \beta^{1/n}t)$  is a factor of  $Z(t^n, C_n)$ .  $\square$

- Thus, RH for  $C_n \Rightarrow |\beta| = q^{n/2}$
- $\Rightarrow |\beta^{1/n}| = (q^{n/2})^{1/n} = q^{1/2}$
- $\Rightarrow$  All roots of  $Z(t, C)$  satisfy  $|\alpha| = \sqrt{q}$   
 $\Rightarrow$  RH for  $C$ .
- Conversely, assume RH for  $Z(t, C)$ .

- As,  $(1 - \alpha t)$  is a factor of  $Z(t, C)$
- We deduce,  $\prod_{\eta^n=1} (1 - \alpha \eta t)$  are the factors of  $Z(t^n, C_n)$ .
- $(1 - \alpha^n t^n)$  is a factor of  $Z(t^n, C_n) \Rightarrow (1 - \alpha^n t)$  is a factor of  $Z(t, C_n)$ .
- $|\alpha^n| = |\alpha|^n = (q^{1/2})^n = q^{n/2} \Rightarrow$  RH for  $C_n$ .

## Equivalent Formulation of RH

### Proposition 5.3.2: Equivalent Formulation of RH

The following are equivalent (TFAE):

- (i) RH for  $Z(t, C)$ . [i.e.,  $|\alpha_i| = q^{1/2}, \forall i$ ]
- (ii)  $|N_d - (q^d + 1)| \leq A + B \cdot q^{d/2}$  for some constants  $A, B, N \in \mathbb{Z}$  & for all multiples  $d$  of  $N$ . (independent of  $d$ )

*Proof.* (i)  $\Rightarrow$  (ii): We've proved this already ( $\forall d$ ).

(ii)  $\Rightarrow$  (i): Replace the base field  $\mathbb{F}_q$  by  $\mathbb{F}_{q^N}$ . As we vary  $d$  (over multiples of  $N$ ), we can rename  $\mathbb{F}_{q^N}$  to be the new base field  $\mathbb{F}_q$ . The hypothesis becomes  $|N_d - (q^d + 1)| \leq A + B \cdot q^{d/2}$  for all  $d \geq 1$ .

We've  $\prod_{i=1}^{2g} \alpha_i = \prod_{i=1}^g (\alpha_i \cdot \alpha_{i+g}) = q^g$  (by symmetry).  $\square$

## Proof Strategy: Bounding the Roots

It suffices to show:  $\forall i, |\alpha_i| \leq \sqrt{q}$ . (The original text had "Kils" here).

Recall  $L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$ .

$$\Rightarrow \log \frac{1}{L(t)} = \sum_{d \geq 1} \left( \sum_{i=1}^{2g} \alpha_i^d \right) \cdot \frac{t^d}{d}$$

Let's consider the curve  $C_N$  over  $\mathbb{F}_{q^N}$ . Let  $q' = q^N$  and its roots be  $\alpha'_i = \alpha_i^N$ .

$$\begin{aligned} \left| \log \frac{1}{L(t)} \right| &\leq \sum_{d \geq 1} (A + B \cdot (q')^{d/2}) \cdot \frac{|t|^d}{d} \\ &= A \cdot \log \frac{1}{1 - |t|} + B \cdot \log \frac{1}{1 - |t|\sqrt{q'}} \end{aligned}$$

The LHS converges for  $t \in \mathbb{C}$  if  $|t| < 1/\sqrt{q'}$ .

$\Rightarrow$  Zeros of  $L(t)$  (which are  $1/\alpha'_i$ ) must have norm  $\geq 1/\sqrt{q'}$ .

$\Rightarrow |1/\alpha'_i| \geq 1/\sqrt{q'}$ , which implies  $|\alpha'_i| \leq \sqrt{q'}$ .

Combining with the functional equation (which implies  $|\alpha'_i| \geq \sqrt{q'}$ ), we get

$$\forall i \in [2g], \quad |\alpha'_i| = \sqrt{q'}.$$

RH for  $Z(t, C_N)$  holds. By the base-change proposition, RH holds for  $Z(t, C)$ .

## 5.4 Galois Covers and Point Counting

### Introduction to Galois Covers

Next reduction that we need is to make the Cover Galois;

$$C \rightarrow \mathbb{P}^1; \quad k(x_1)[x_2]/\langle F \rangle \supseteq k(x_1)$$

, we want  $k(C)$  to have all roots of  $F$  wrt  $x_2$  (think of  $x_1$  fixed in  $k$ ).

#### Example: Specific Galois Cover

Move to the Galois Cover of  $C$ . Let  $C$  (in affine patch  $x_0 = 1$ ) be

$$x_2^3 - x_2 - x_1^2 = 0 \quad \text{over } k = \mathbb{F}_q.$$

$\Rightarrow k(C) =: K = k(x_1)[x_2]/\langle x_2^3 - x_2 - x_1^2 \rangle$  is a  $\deg = 3$  extension of  $k(x_1) = k(\mathbb{P}^1)$  which may not be a splitting field.

- We correct this by moving to the splitting field  $K'$  of  $x_2^3 - x_2 - x_1^2$  over  $k(x_1)$ .  $[K' : k(x_1)]$  is typically  $3! = 6$ . For this specific polynomial, the Galois group is  $S_3$ .

$$K' \supset K \supset k(x_1) \supset k = \mathbb{F}_q$$

$K'/K$  &  $K'/k(x_1)$  are Galois extensions (i.e., they're separable & normal.)

Let  $C'$  be the curve defined by  $K'$  (as it's a function field in 1 variable over  $k$ ).

$$C' \rightarrow C \rightarrow \mathbb{P}^1$$

is called the Galois Cover of  $C$ .

### Fiber Analysis and Frobenius Action

Let  $f(y) = y^3 - y - x_1^2$ . If  $x_2$  is a root, we can divide  $f(y)$  by  $(y - x_2)$ . The fiber over a point  $x_1 \in k(x_1)$  corresponds to the roots of  $y^3 - y - x_1^2 = 0$ .

$$\begin{array}{ccc} P_0, P_1, P_2 & \in & k(x_1)[x_2, y_2]/\langle \dots \rangle \cong k(C') \\ \downarrow & & \\ P \in C & \in & k(x_1)[x_2]/\langle \dots \rangle \cong k(C) \\ \downarrow & & \\ x_1 & \in & k(x_1) \end{array}$$

$P_0 := (x_1, x_2)$ ,  $P_1 := (x_1, y_2)$  &  $P_2 := (x_1, -x_2 - y_2)$  are the three roots, given  $x_1$ .

Let  $F$  be the Frobenius &  $\sigma$  be a Galois automorphism of  $k(C')$  over  $k(C)$ . For instance, an element  $\sigma \in \text{Gal}(K'/K)$  would fix  $P_0$  and permute  $P_1, P_2$ .

$$P_0^\sigma = P_0, \quad P_1^\sigma = P_2, \quad P_2^\sigma = P_1.$$

E.g., for  $(x_1, x_2) \in \mathbb{F}_q \times \mathbb{F}_q$  s.t.  $x_2^3 - x_2 - x_1^2$  has only one root in  $\mathbb{F}_q$ .

The other two roots are in  $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ . The Frobenius  $F$  acts as  $F(P_0) = P_0$ ,  $F(P_1) = P_2$ ,  $F(P_2) = P_1$ .

$P_1, P_2$  are conjugates over  $\mathbb{F}_q(C)$ , via  $F$ .

- $P_1 = P_2$  for some  $x_1 \in \mathbb{F}_q$  implies  $x_1$  is a zero of the discriminant of the polynomial, or  $\text{Res}_{x_2}(f(x_2, x_1), \frac{\partial f}{\partial x_2}(x_2, x_1))$ .
- Thus,  $P_1 = P_2$  happens for  $\leq (\deg f)^2$  many  $x_1$ 's.

## Definition and Properties of Galois Group

### Definition 5.4.1: Galois Cover

Let  $G = \text{Gal}(k(C')/k(C))$  be the group of  $k(C)$ -automorphisms of  $K' := k(C')$ .

### Proposition 5.4.1: Size of Galois Group

Let  $C$  be a smooth projective curve over  $k$  & let  $C'$  be a Galois cover.

$$|\text{Gal}(k(C')/k(C))| = [k(C') : k(C)]$$

*Proof.*  $k(C')/k(C)$  is a finite Galois extension. By the primitive element theorem,  $k(C') = k(C)(\alpha)$ .  $\deg(\text{minpoly}_\alpha) = [k(C') : k(C)]$ .

&  $k(C')$  is the splitting-field of  $\text{minpoly}_\alpha$ . & so it has all its conjugates.

$$|\text{Gal}(k(C')/k(C))| = \# \text{ conjugates} = [k(C') : k(C)].$$

□

## Action on Points and Geometric Frobenius

$\forall \sigma \in \text{Gal}(k(C')/k(C))$ , can be seen to act on pts.  $P' \in C'$  via its action on  $k(C')$ . Say, pt.  $P' = (x_1, x_2)$ .

- $\sigma(x_1)$  &  $\sigma(x_2)$  can be seen as functions in  $k(C')$ .
- Use them to define  $\sigma(P')$ .
- Qn: What about poles of  $\sigma(x_2)$ ?

Frobenius  $F: k(C) \rightarrow k(C)$ ;  $f(x_1, x_2) \mapsto f(x_1^q, x_2^q)$ . This induces a map on points (the geometric Frobenius):  $(\alpha, \beta) \mapsto (\alpha^{q^{-1}}, \beta^{q^{-1}})$ .

$F$  is injective. ( $k$ -Monomorphism).

## 5.5 Bombieri-Stepanov Method: Proof of Weil Bounds

### Introduction and Setup

This document outlines a proof of the Hasse-Weil bound (also known as the Riemann Hypothesis for curves over finite fields). The method presented is based on the work of Bombieri and Stepanov. The core idea is to bound the number of rational points on a curve by constructing a function with specific properties related to its zeros and poles.

Let  $C_0$  be a curve defined over a finite field  $\mathbb{F}_q$ . Let  $k_0 = \mathbb{F}_q(C_0)$  be its function field. We consider the curve  $C$  over the algebraic closure  $k = \mathbb{k}$ , with function field  $K = k_0 \cdot k$ . The points of  $C$  rational over  $\mathbb{F}_q$ , denoted  $C(\mathbb{F}_q)$ , are the points fixed by the geometric Frobenius endomorphism  $F$ .

- The Frobenius map  $F$  acts on the coordinates of points. For a point  $P = (x_1, \dots, x_n)$ ,  $F(P) = (x_1^q, \dots, x_n^q)$ .
- Consequently, the set of  $\mathbb{F}_q$ -rational points is precisely the set of fixed points of Frobenius:

$$C(\mathbb{F}_q) = \{P \in C \mid F(P) = P\}$$

The number of these points is denoted  $N_1(C) = |C(\mathbb{F}_q)|$ .

- The action of Frobenius on functions in the function field  $K(C)$  is given by raising the coefficients to the  $q$ -th power. For example, the action on a function  $(x_1 - \alpha)$  is  $F^*(x_1 - \alpha) = x_1^q - \alpha^q$ .
- This action relates the order of vanishing of a function at a point  $P$  to the order of vanishing of its image at the point  $F(P)$ . Specifically,  $\text{ord}_P(f \circ F) = q \cdot \text{ord}_{F(P)}(f)$ .

### Galois Covers and Averaging

The proof strategy involves relating the point count on an arbitrary curve  $C$  to the point count on a related curve  $C'$  which is a Galois cover.

Let  $\phi: C' \rightarrow C$  be a Galois cover, with  $G = \text{Gal}(k(C')/k(C))$  being the Galois group of the corresponding function field extension. For any  $\sigma \in G$ , we define a set of "twisted" fixed points on  $C'$ :

$$\bar{N}_1(C', \sigma) := \{P \in C' \mid \sigma^{-1} \circ F(P) = P\}$$

The number of such points is denoted  $N_1(C', \sigma)$ . The standard set of rational points corresponds to the case where  $\sigma$  is the identity element,  $N_1(C') = N_1(C', 1)$ .

A key tool is the following proposition, which connects the number of rational points on  $C$  to the average of these twisted point counts on  $C'$ .

**Proposition 5.5.1: Averaging over  $G$**

The number of  $\mathbb{F}_q$ -rational points on  $C$  is given by:

$$N_1(C) = \frac{1}{|G|} \sum_{\sigma \in G} N_1(C', \sigma) + O_\delta(1)$$

where the error term  $O_\delta(1)$  depends on the degree  $\delta$  of the extension defining  $C$ , specifically on the number of ramified points.

*Proof Sketch.*

- For any point  $P \in C$ , consider its fiber under the cover,  $\phi^{-1}(P) = \{Q_1, \dots, Q_r\}$ . The size of the fiber,  $r$ , is equal to  $|G|$  if  $P$  is unramified, and  $r < |G|$  if  $P$  is ramified. The number of ramified points is bounded, e.g., by  $\delta^2$ , contributing the  $O_\delta(1)$  term.
- If  $P \in C(\mathbb{F}_q)$  is an unramified point, then for any  $Q \in \phi^{-1}(P)$ , the point  $F(Q)$  is also in the fiber  $\phi^{-1}(P)$  because  $F(P) = P$ . The group  $G$  acts transitively on the fiber. For any  $Q_i, Q_j$  in the fiber, there is a unique  $\sigma \in G$  such that  $Q_j = \sigma(Q_i)$ .
- Let's count the size of the sum  $\sum_{\sigma \in G} N_1(C', \sigma)$ . A point  $Q' \in C'$  contributes to this sum if there exists some  $\sigma \in G$  such that  $\sigma^{-1}(F(Q')) = Q'$ .
- If  $Q'$  contributes to the sum, let  $P' = \phi(Q')$ . Then  $\phi(\sigma^{-1}(F(Q'))) = \phi(Q')$ , which implies  $\phi(F(Q')) = \phi(Q')$ . This simplifies to  $F(\phi(Q')) = \phi(Q')$ , meaning  $P' = \phi(Q')$  is an  $\mathbb{F}_q$ -rational point on  $C$ .
- So, the sum only counts points  $Q'$  that lie above the  $\mathbb{F}_q$ -rational points of  $C$ .
- For each unramified point  $P \in C(\mathbb{F}_q)$ , and for each  $Q \in \phi^{-1}(P)$ , the set  $\{\sigma^{-1}(F(Q)) \mid \sigma \in G\}$  is precisely the fiber  $\phi^{-1}(P)$ . Therefore, for each  $Q$  in the fiber, there is exactly one  $\sigma$  that fixes it in this twisted sense. This means each unramified rational point  $P \in C(\mathbb{F}_q)$  contributes exactly  $|G|$  to the total sum  $\sum_{\sigma \in G} N_1(C', \sigma)$ .
- Summing over all unramified points, we get  $\sum_{\sigma \in G} N_1(C', \sigma) \approx |G| \cdot N_1(C)$ . Including the error from ramified points gives the proposition.

□

## Main Theorem: Weil-Bombieri-Stepanov Bound

The proof hinges on the following theorem, which provides a bound for the number of twisted fixed points on a Galois cover of the projective line  $\mathbb{P}^1$ .

### Theorem 5.5.1: Weil, Bombieri-Stepanov

Let  $C \rightarrow \mathbb{P}$  be a Galois cover over  $\mathbb{F}_q$ . Let  $g$  be the genus of  $C$ . Assume  $q = p^\alpha$  with  $\alpha$  even, and that  $q > (g + 1)^4$ . Then, for any  $\sigma \in \text{Aut}(C/\mathbb{P})$ , we have the bound:

$$N_1(C, \sigma) \leq q + 1 + (2g + 1)\sqrt{q}$$

This theorem for a special case (Galois covers of  $\mathbb{P}^1$ ) can be leveraged to prove the Riemann Hypothesis for any curve  $C_0$ .

## Application to General Curves

### Implication for General Curves

Let  $C_0$  be an arbitrary curve.

1. Construct the smallest Galois extension  $K'$  of the function field  $K = k(C_0)$  and let  $C'$  be the corresponding curve. This gives a Galois cover  $C' \rightarrow C_0$ . Let  $H = \text{Gal}(K'/K)$ .
2. By the Averaging Proposition:  $N_1(C_0) = |H|^{-1} \sum_{h \in H} N_1(C', h) + O_\delta(1)$ .
3. Now view  $C'$  as a cover of the projective line  $\mathbb{P}^1$ . Let  $G = \text{Gal}(K'/\mathbb{F}_q(x))$  be the full Galois group, where  $G \geq H$ .
4. We know  $N_1(\mathbb{P}) = q + 1$ . Applying the Averaging Proposition to the cover  $C' \rightarrow \mathbb{P}$ :

$$q + 1 = N_1(\mathbb{P}) = |G|^{-1} \sum_{\sigma \in G} N_1(C', \sigma) + O_\delta(1)$$

5. The theorem gives an upper bound on each term in the sum:  $N_1(C', \sigma) \leq q + 1 + O(g\sqrt{q})$ . Combining this with the equality from the previous step implies that the terms  $N_1(C', \sigma)$  must be close to  $q + 1$  on average. This forces a lower bound as well, leading to the two-sided estimate:

$$N_1(C', \sigma) = q + 1 + O(g\sqrt{q} + \delta^2)$$

6. Substituting this estimate back into the formula for  $N_1(C_0)$  from step 2 (noting that  $H$  is a subset of  $G$ ), we get:

$$N_1(C_0) = \frac{1}{|H|} \sum_{h \in H} (q + 1 + O(g\sqrt{q} + \delta^2)) = q + 1 + O(g\sqrt{q} + \delta^2)$$

This is the celebrated Hasse-Weil bound, which is the statement of the Riemann Hypothesis for the curve  $C_0$ .

## Construction of the Auxiliary Function

We now focus on proving the theorem for a Galois cover  $C \rightarrow \mathbb{P}$ . Let  $\phi$  be the composite map  $\sigma^{-1} \circ F$ . We want to bound the number of points  $P \in C$  such that  $\phi(P) = P$ .

If  $N_1(C, \sigma)$  is empty, the theorem is trivial. Otherwise, pick a point  $P \in C$  such that  $\phi(P) = P$ . For an integer  $a > 2g - 2$ , consider the Riemann-Roch space  $L_a = L(aP)$ , which is the vector space of functions  $f \in k(C)$  whose only poles are at  $P$  with order at most  $a$ . By the Riemann-Roch theorem, its dimension is  $l_a = \dim(L_a) = a + 1 - g$ .

We will construct a non-zero function that vanishes at many of the points we want to count. The argument relies on two actions on these function spaces:

1. The map  $\phi = \sigma^{-1} \circ F$ . If  $f \in L_a$ , then  $f \circ \phi$  has a pole of order at most  $qa$  at  $P$  (since  $\phi(P) = P$ ). This defines a linear map  $L_a \rightarrow L_{aq}$ .
2. The absolute Frobenius map  $F_{abs} : x \mapsto x^p$ . Let  $q = p^\alpha$ . For an integer  $\mu$ , we consider the map  $f \mapsto f \circ F_{abs}^\mu = f^{p^\mu}$ . If  $f \in L_b$ , then  $f^{p^\mu}$  has a pole of order at most  $bp^\mu$  at  $P$ . This gives a linear map  $L_b \rightarrow L_{bp^\mu}$ .

Now, consider the multiplication map on the tensor product of these transformed spaces:

$$\Psi : L_b^{p^\mu} \otimes L_a^q \rightarrow L_{bp^\mu + aq}$$

$$(s \circ F_{abs}^\mu) \otimes (f \circ \phi) \mapsto (s \circ F_{abs}^\mu) \cdot (f \circ \phi)$$

### Lemma 5.5.1: Claim 1: Injectivity of $\Psi$

The multiplication map  $\Psi$  is injective provided that  $bp^\mu < q$ .

*Proof of Claim 1.* Let  $\{f_i\}_{i=1}^{l_a}$  be a basis of  $L_a$  such that the pole orders at  $P$  are strictly increasing:  $v_P(f_i) < v_P(f_{i+1})$ , where  $v_P = -\text{ord}_P$ . An arbitrary element in the tensor product space is  $G = \sum_i (s_i \circ F_{abs}^\mu) \otimes (f_i \circ \phi)$ , where  $s_i \in L_b$ . Suppose its image under  $\Psi$  is zero:

$$\sum_i (s_i \circ F_{abs}^\mu) \cdot (f_i \circ \phi) = 0$$

Let  $h$  be the smallest index for which  $s_h \neq 0$ . We can write:

$$(s_h \circ F_{abs}^\mu) \cdot (f_h \circ \phi) = - \sum_{i>h} (s_i \circ F_{abs}^\mu) \cdot (f_i \circ \phi)$$

Now we compare the pole orders at  $P$  for both sides. The valuation  $v_P$  transforms as

$$v_P(g \circ \phi) = q \cdot v_P(g) \text{ and } v_P(g \circ F_{abs}^\mu) = p^\mu \cdot v_P(g).$$

$$\begin{aligned} v_P(\text{LHS}) &= p^\mu v_P(s_h) + q v_P(f_h) \\ v_P(\text{RHS}) &\geq \min_{i>h} \{p^\mu v_P(s_i) + q v_P(f_i)\} \end{aligned}$$

Since  $v_P(f_i) > v_P(f_h)$  for  $i > h$ , and  $v_P(s_i) \leq b$  for all  $i$ , we get:

$$p^\mu v_P(s_h) + q v_P(f_h) \geq \min_{i>h} \{p^\mu v_P(s_i) + q v_P(f_i)\} > p^\mu v_P(\text{some } s_i) + q v_P(f_h)$$

$p^\mu(v_P(s_h) - v_P(s_i)) > q(v_P(f_h) - v_P(f_i))$  (This step in the notes seems slightly off, let's follow the note)

The logic in the notes leads to  $p^\mu v_P(s_h) \geq -bp^\mu + q(v_P(f_i) - v_P(f_h))$ . Since  $v_P(f_i) - v_P(f_h) > 0$ , if we have  $q - bp^\mu > 0$ , a contradiction arises, implying that our assumption (that some  $s_h \neq 0$ ) must be false. Thus, all  $s_i = 0$  and the map is injective.  $\square$

## Counting Argument and Zero Divisor

To create our desired function, we need a non-zero element in the kernel of some map. The previous map is injective under the condition  $bp^\mu < q$ . So instead, we consider a different map and find an element in its kernel. Let's consider the space  $L_b \otimes L_a$ . We require its dimension,  $l_b \cdot l_a$ , to be greater than the dimension of the target space  $L_{bp^\mu + aq}$ . This will guarantee the existence of a non-zero function in the kernel of a related map.

Let  $G_0 = \sum_i s_i \otimes f_i$  be a non-zero element in  $L_b \otimes L_a$ . We construct the function

$$G = \sum_i (s_i \circ F_{abs}^\mu) \cdot (f_i \circ \phi)$$

We can choose  $G_0$  such that a related function  $\tau(G_0) = \sum_i s_i^{p^\mu} f_i$  is identically zero. The function  $G$  is not identically zero (by a modification of Claim 1's argument). By construction,  $G$  lies in the space  $L_{bp^\mu + aq}$ , so the degree of its pole divisor is at most  $bp^\mu + aq$ .

Now let's find the zeros of  $G$ . Let  $Q$  be any point in our target set, i.e.,  $Q \in N_1(C, \sigma)$  and  $Q \neq P$ . By definition,  $\phi(Q) = Q$ . At such a point:

$$G(Q) = \sum_i s_i(F_{abs}^\mu(Q)) \cdot f_i(\phi(Q)) = \sum_i s_i(Q)^{p^\mu} \cdot f_i(Q) = \tau(G_0)(Q) = 0$$

So,  $G$  vanishes at every point in  $N_1(C, \sigma) \setminus \{P\}$ .

The argument in the notes is that the related function  $\tau(G_0)$  is a  $p^\mu$ -th power, and thus vanishes with high multiplicity. This high order of vanishing at the points  $Q$  is crucial. The degree of the zero divisor of  $G$  must be at least  $p^\mu \cdot (|N_1(C, \sigma)| - 1)$ . Since

the degree of the zero divisor equals the degree of the pole divisor:

$$p^\mu(N_1(C, \sigma) - 1) \leq \deg((G)_\infty) \leq bp^\mu + aq$$

Rearranging this inequality gives our initial bound:

$$N_1(C, \sigma) \leq 1 + b + \frac{aq}{p^\mu}$$

## Parameter Optimization

The final step is to choose the integer parameters  $a, b, \mu$  to make this bound as strong as possible, while satisfying the necessary conditions for the proof to work.

### Lemma 5.5.2: Claim 2: Parameter Choices

Let  $q = p^\alpha$  with  $\alpha$  even. Choose the parameters as follows:

- $\mu = \alpha/2$ , which implies  $p^\mu = \sqrt{q}$ .
- $a = \lfloor \sqrt{q} \rfloor + 2g$ .
- $b = \left\lfloor \frac{g\sqrt{q}}{g+1} \right\rfloor + g + 1$ .

Then for  $q > (g+1)^4$ , the following conditions hold:

- (i)  $bp^\mu < q$ .
- (ii)  $l_b \cdot l_a > l_{bp^\mu+a}$  (a slightly different target space from the notes to ensure a non-zero element).
- (iii) The bound becomes  $1 + b + a\sqrt{q} \leq q + 1 + (2g + 1)\sqrt{q}$ .

*Proof of Claim 2.* • **For (i):**  $b = \left\lfloor \frac{g\sqrt{q}}{g+1} \right\rfloor + g + 1 \leq \frac{g\sqrt{q}}{g+1} + g + 1 = \frac{g\sqrt{q} + (g+1)^2}{g+1}$ . Since we assume  $q > (g+1)^4$ , we have  $\sqrt{q} > (g+1)^2$ .  $b < \frac{g\sqrt{q} + \sqrt{q}}{g+1} = \frac{(g+1)\sqrt{q}}{g+1} = \sqrt{q}$ . Therefore,  $b \cdot p^\mu = b\sqrt{q} < \sqrt{q} \cdot \sqrt{q} = q$ . The condition holds.

- **For (ii):** We need to show  $\dim(L_b \otimes L_a) > \dim(L_{bp^\mu+a})$ . Using Riemann-Roch for large degrees, this is approximately  $(b - g + 1)(a - g + 1) > bp^\mu + a - g + 1$ . The notes show that this is equivalent to  $b(a + 1 - g - p^\mu) > g(a + 1 - g)$ . Substituting  $a \approx \sqrt{q}$  and  $p^\mu = \sqrt{q}$ , this is roughly  $b(\sqrt{q} - \sqrt{q}) > g\sqrt{q}$ , which doesn't seem right. Let's follow the derivation in the notes: the condition becomes  $b > g + \frac{g\sqrt{q}}{g+1}$ . Our choice for  $b$  is  $b = \lfloor \frac{g\sqrt{q}}{g+1} \rfloor + g + 1$ , which is indeed greater than  $g + \frac{g\sqrt{q}}{g+1}$ . The condition holds.

- **For (iii):** We substitute our choices into the bound  $1 + b + aq/p^{-\mu} = 1 + b + a\sqrt{q}$ .

$$\begin{aligned}
 N_1(C, \sigma) &\leq 1 + \left( \left\lfloor \frac{g\sqrt{q}}{g+1} \right\rfloor + g + 1 \right) + (\lfloor \sqrt{q} \rfloor + 2g)\sqrt{q} \\
 &\leq 1 + \frac{g\sqrt{q}}{g+1} + g + 1 + (\sqrt{q} + 2g)\sqrt{q} \\
 &= 1 + \frac{g\sqrt{q}}{g+1} + g + 1 + q + 2g\sqrt{q} \\
 &= q + g + 2 + \sqrt{q} \left( 2g + \frac{g}{g+1} \right) \\
 &= q + g + 2 + \sqrt{q} \left( \frac{2g(g+1) + g}{g+1} \right)
 \end{aligned}$$

This simplifies to  $q + 1 + \sqrt{q}(2g + \frac{g}{g+1}) + g + 1$ . For large  $q$ , this is bounded by  $q + 1 + (2g + 1)\sqrt{q}$ .

This completes the proof of the theorem.  $\square$

## 5.6 Conclusion and Results

Thus, we've shown for any Smooth proj. curve  $C$  over  $\mathbb{F}_q$ , genus  $g$ , the roots of  $L(t)$  satisfy  $|\alpha| = \sqrt{q}$ .

$$-2g\sqrt{q} \leq N_1(C) - (q + 1) \leq 2g\sqrt{q}$$

For large  $q$ ,  $N_1(C) \approx q + 1 = N_1(\mathbb{P}^1)$ .

## Applications to Character Sums

RH has tons of implications. For ex. in CS we use

### Proposition 5.6.1: Corollary: Weil Estimate for $\chi$ -sums

Let  $\chi = \chi_2 : \mathbb{F}_q \rightarrow \{-1, 0, +1\}$  be the character.

$a^{(q-1)/2} \equiv 1$  iff  $a$  is square in  $\mathbb{F}_q^*$ .

Let  $f(x)$  be deg- $d$  polynomial. Then,

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (d-1)\sqrt{q}$$

*Proof.* Consider the curve  $C$  for  $K := \mathbb{F}_q(x)[y]/\langle y^2 - f(x) \rangle$ .

$$\begin{aligned} \sum_{\alpha \in \mathbb{F}_q} \chi(f(\alpha)) &= \sum_{\alpha; \chi(f(\alpha))=1} 1 - \sum_{\alpha; \chi(f(\alpha))=-1} 1 \\ &= (\# \text{ of points with 2 preimages}) - (\# \text{ of points with 0 preimages}) \\ &\approx N_1(C) - (q + 1) \quad (\text{ignoring points at infinity, roots of } f) \\ &= N_1(C) - q + O_d(1). \end{aligned}$$

□

## Further Exercises and Questions

**Exercise:** Do this for other exponential sums.

**Questions:**

- (i) Given  $C/\mathbb{F}_q$ , how do we compute  $N_r(C)$  in  $\text{poly}(\log q, \dots)$ -time?
- (ii) Is there another interpretation of  $L(t)$  that can help in computing?

## 5.7 Cohomological Interpretation of L-Functions

### Isogeny and the Frobenius Endomorphism

See Frob ( $q$ -th) as an isogeny on Jacobian.

#### Definition 5.7.1: Isogeny

Isogeny  $\alpha : J_C(k) \rightarrow J_C(k)$  is a surjective morphism with finite  $\ker(\alpha)$ . (respecting the group & the variety)  
 $\deg(\alpha) := |\ker(\alpha)|$ .

- $\pi : J \rightarrow J$  is an isogeny with  $\deg(\pi) = q^g$ .
- For  $n \in \mathbb{Z}$ ,  $[n] : J \rightarrow J; D \mapsto nD$  is an isogeny.

### Torsion Points and Tate Module

What's  $\deg([n]) = ?$

#### Definition 5.7.2: Torsion points

For prime  $l \in \mathbb{N}$  we call  $\ker([l])$  the  $l$ -torsion of  $J$ , denoted  $J[l]$ .  
 $T_l J := \varprojlim_i J[l^i]$  is the  $l$ -adic Tate module of  $J$ . ( $T_l J$  is built from  $\bigcup_{i \geq 1} J[l^i]$  which is the  $l$ -adic torsion of  $J$ .)

Any isogeny  $\alpha : J \rightarrow J$  gives an isogeny  $T_l \alpha : T_l J \rightarrow T_l J; D \mapsto \alpha(D)$ .

Now, we can study  $T_l \alpha$  for  $\alpha$  coming from  $\pi$  &  $[n]$ .

## Weil Theorem on Torsion and Characteristic Polynomial

**Theorem 5.7.1: Theorem (Weil):**

- (a) Linear map  $T_l(\pi)$  on  $T_l J$  has Charpoly  $t^{2g} L(1/t)$ . (Assume  $l \neq p = \text{char}(\mathbb{F}_q)$ .)
- (b)  $T_l J \cong (\mathbb{Z}_l)^{2g}$ , i.e.  $T_l J$  is a finite rank  $\mathbb{Z}_l$ -module.
- (c) For any  $n \in \mathbb{N}$ ,  $\deg([n]) = n^{2g}$  &  $J[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ .

## Proof of Weil Theorem

**Pf:** Recall,  $\deg(\pi - 1) = |J(\mathbb{F}_q)| = |\text{Cl}_0(C)| = h(C) = L(1) = \prod(\alpha_i - 1)$ .

Similarly,  $\forall m \in \mathbb{N}$ ,  $\deg(\pi^m - 1) = |J(\mathbb{F}_{q^m})| = \prod(\alpha_i^m - 1)$  [Base-change of  $L(t)$ ].

Going to  $\mathbb{Z}_l$ , we can view  $\pi$  in  $M_{2g}(\mathbb{Z}_l)$ .

Let  $\pi$  act on  $T_l J$  with eigenvalues  $\beta_i, i \in \{1, \dots, 2g\}$ .

$\Rightarrow \deg(\pi^m - 1) = |T_l J / (\pi^m - 1)T_l J| = \det(T_l(\pi^m - 1)) = \prod_i(\beta_i^m - 1)$ . ( $|\ker| = |\text{coker}| = \det = \prod \text{eigenval}$ )

Since this holds  $\forall m$ , we deduce that  $\{\alpha_i\} = \{\beta_i\}$  as multisets.  $\Rightarrow \text{Charpoly}(\pi|_{T_l J}) = \det(tI - T_l \pi) = \prod(t - \beta_i) = \prod(t - \alpha_i) = t^{2g} L(1/t)$  over  $\mathbb{Z}_l$ .

Also,  $\text{Charpoly}(\pi^{-1}|_{T_l J}) = q^{-g} L(t)$ , over  $\mathbb{Q}_l$ .

(b) & (c) are implied by  $\deg(L) = 2g$  &  $l$ -torsion resp.  $n$ -torsion of  $J$ .

→ These properties are computationally useful, as one can work with the Frobenius action on torsion points.

## Computational Complexity

Current time-complexity for  $L(t)$  is the min of:

- $\text{poly}(p, g, \log q)$  [Kedlaya, 2001] (by computing  $L(t)$   $p$ -adically.)
- $\text{poly}(\log q, g^{O(g)})$  [Pila, 1990]

## REFERENCES

---

- [1] Carlos J. Moreno. *Algebraic Curves over Finite Fields*, volume 97 of *Cambridge Tracts in Mathematics*. Cambridge University Press, 1991.