Algebraic Curve

Lectured by Prof. Wenchuan Hu and Noted by Xinyu Xiang

Jul. 2025

1 Day 0: Preliminary

Here we will list some preliminary knowledge that we will use in the following lectures.

2 Day I

Definition 2.1 (Polynomial). *The collection of polynomials would denoted by $\mathbb{K}[x_1, \cdots, x_n]$, whose elements are of the form*

$$f = \sum_{i_1,\cdots,i_n} a_{i_1,\cdots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

where $a_{i_1,\cdots,i_n} \in \mathbb{K}$, and $i_1, \cdots, i_n$ are non-negative integers.

Definition 2.2 (Algebraic Closed Field). *If*

Remark 2.1. *Finite field is not algebraic closed: Consider $f = (x - a_1) \cdots (x - a_n) + 1$ which has no zero point.*

Definition 2.3 (Unique Factorization Domain (UFD)).

Proposition 2.1. *(1) $\mathbb{K}[x_1, \cdots, x_n]$ is a commutative ring with unity called the polynomial ring in n variables over $\mathbb{K}$.*

(2) If R is UFD, then $R[X]$ is a UFD, which means that every non-zero polynomial can be factored uniquely into irreducible polynomials, up to order and units.

From here on, we assume that $\mathbb{K}$ is an algebraic closed field.

Definition 2.4 (Affine Variety). *An affine variety is a subset of $\mathbb{K}^n$ defined by the vanishing of a set of polynomials, i.e., it is the solution set of a system of polynomial equations.*

Formally, given a set of polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, the affine variety $V(f_1, \ldots, f_m)$ is defined as:

$$V(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n; f_i(a_1, \ldots, a_n) = 0 \text{ for all } i = 1, \ldots, m\}.$$

Proposition 2.2 (Zariski Topology). *Consider $f, g \in \mathbb{K}[x, y]$*

(1) $V(fg) = V(f) \cup V(g)$,

(2) $V(f, g) = V(f) \cap V(g)$, $V(f_\lambda)_{\lambda\in\Lambda} = \bigcap_{\lambda\in\Lambda} V(f_\lambda)$,

(3) $V(0) = \mathbb{A}^2_{\mathbb{K}}$.

Definition 2.5 (Affine Curve). *Consider $f \in \mathbb{K}[x, y]$, $V(f)$ denotes affine curve.*

(1) $\deg V(f) = \deg f$,

(a) $\deg = 1$: *Line,*

(b) $\deg = 2$: *conic curve (non-degenerate),*

(2) $F = F_1^{n_1} F_2^{n_2} \cdots F_m^{n_m}$, *where F_i irreducible.*

Example 2.1. $(x+y)^2$ *is irreducible, xy is reducible.*

Example 2.2. $y^2 - x^3 + x$ *is irreducible (left as exercise).*

Definition 2.6 (Field of Fractions)**.** *The field of fractions of a UFD R is the smallest field in which R can be embedded, denoted by $K(R)$. It consists of elements of the form $\frac{a}{b}$ where $a, b \in R$ and $b \neq 0 \in R$.*

Formally, if R is a UFD, then the field of fractions $K(R)$ is defined as:

$$Q_{\mathrm{uot}}(R) = \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\},$$

which is indeed a field.

Lemma 2.3. *Consider $f \in \mathbb{K}[x,y]$ and $\deg f > 0$, then*

(1) $V(f)$ has infinitely many points,

(2) $\mathbb{A}^2_{\mathbb{K}} - V(f)$ has infinitely many points.

Theorem 2.4 (Simple Bezout Theorem)**.** *If $F, G \in \mathbb{K}[x,y] \subset \mathbb{K}(x)[y]$ has no common component, then $V(F,G)$ is a finite set $\Leftrightarrow$ $F = 0$, $G = 0$ have finite solutions in $\mathbb{K}^2$.*

Proof. (1) Assume there is an element α such that $F = \alpha F'$ and $G = \alpha G'$, where we consider the ring $\mathbb{K}(x)[y]$, then

$$\begin{cases} aF = HF' \\ bG = HG', \end{cases}$$

where $a \in \mathbb{K}[x]$ and $H \in \mathbb{K}[x,y]$.

(2) TBD

$\square$

Theorem 2.5. *Consider irreducible $F, G \in \mathbb{K}[x,y]$, $F|G \Leftrightarrow V(F) \subset V(G)$.*

Proof. (1) If $F|G$, then $G = FH$ for some $H \in \mathbb{K}[x,y]$, thus $V(F) \subset V(G)$.

(2) If $V(F) \subset V(G)$, by definition $F|G$.

$\square$

3 Day II: Intersection Number (1)

Definition 3.1 (Localized Ring)**.** *Consider $\mathbb{K}[x,y]$ and a prime ideal $P \subset R$, the localized ring $\mathcal{O}_P$ is defined as:*

$$\mathcal{O}_P = \left\{ \frac{f}{g}; f, g \in \mathbb{K}[x,y], g(p) \neq 0 \right\},$$

the maximal ideal $\mathfrak{m}_P$ is defined as:

$$\mathfrak{m}_P = \left\{ \frac{f}{g}; f, g \in \mathbb{K}[x,y], g(p) \neq 0, f(p) = 0 \right\}.$$

which satisfies

$$0 \to \mathfrak{m}_P \to \mathcal{O}_P \to \mathbb{K}.$$

3.1 Definition

Definition 3.2 (Intersection Number). *Consider $F, G \in \mathbb{K}[x, y]$ irreducible, $P = V(F) \cap V(G)$, then the intersection number $I_P(F, G)$ is defined as:*

$$\mu_P(F, G) = \dim_{\mathbb{K}} \mathcal{O}_P / \langle F, G \rangle ,$$

where $\langle F, G \rangle$ is the ideal generated by F and G in the localized ring $\mathcal{O}_P$.

Proposition 3.1. *(1) $\mu_P(F, G) \in \mathbb{N} \cup \{\infty\}$;*

(2) $P \in F \cap G \Leftrightarrow \mu_P(F, G) \geq 1$, $\mu_P(F, G) = 1 \Leftrightarrow \langle F, G \rangle = \mu_P$

(3) $\mu_P(F, G) = \mu_P(G, F)$;

(4) $\mu_P(F, G + FH) = \mu_P(F, G)$;

(5) $\mu_P(FG, H) = \mu_P(F, H) + \mu_P(G, H)$;

(6) $I_{(0,0)}(x, y) = 1$,

Example 3.1. *Consider $F = y - x^2$ and $G = y$.*

Solution. **Use properties to compute**:

$$\begin{aligned}\mu_0(y, y - x^3) =& \mu_0(y, -x^3) \\ =& 2\mu_0(y, x) \\ =& 2\end{aligned}$$

where we used the property (4) to reduce the degree of the polynomial for the given variable, and use the fact that $\mu_0(x, y) = 1$. □

The most important part is to use the property (4) to reduce the degree of the polynomial for the given variable.

Example 3.2. *Consider $F = y^2 - x^3$ and $G = x^2 - y^3$.*

Solution.

$$\begin{aligned}\mu_0(y^2 - x^3, x^2 - y^3) =& \mu_0(y^2 - x^3 + x(x^2 - y^3), y^3 - x^2) \\ =& \mu_0(y^2 - xy^3, y^3 - x^2) \\ =& \mu_0(y^2, y^3 - x^2) + \mu_0(1 - xy, y^3 - x^2) \\ =& 2\mu_0(y, y^3 - x^2) + 0 \\ =& 2\mu_0(y, x^2) \\ =& 4\mu_0(y, x) \\ =& 4\end{aligned}$$

$\mu_0(1 - xy, y^3 - x^2)$ vanished since at $(0, 0)$, $1 - xy \neq 0$ and $y^3 - x^2 = 0$. □

Example 3.3. *Consider $F = y - x - x^2$ and $G = y^2 - x^2 - 3x^2y$.*

Solution.

$$\begin{aligned}\mu_0(y - x - x^2, y^2 - x^2 - 3x^2y) =& \mu_0(y - x - x^2, y^2 - x^2 - 3x^2y - (x + y)(y - x - x^2)) \\ =& \mu_0(y - x - x^2, -2x^2y + x^3) \\ =& \mu_0(y - x - x^2, x^2(x - 2y)) \\ =& 2\mu_0(y - x - x^2, x) + \mu_0(y - x - x^2, x - 2y) \\ =& 3.\end{aligned}$$

Another way to compute is to use definition of intersection number, where we plug the equation $y = x + x^2$ into the second equation, we have

$$\mu_0(y - x - x^2, y^2 - x^2 - 3x^2y) = \mathfrak{m}_0\left((x + x^2)^2 - x^2 - 3x^2(x + x^2)\right) = \mathfrak{m}_0\left(x^3(-1 - 2x)\right) = 0.$$

$\square$

Proposition 3.2. *If the lowest degree of F is x^n and the lowest degree of G is y^m, then the intersection number $I_{(0,0)}(F, G)$ is nm.*

Definition 3.3 (Short Exact Sequence)**.** *A short exact sequence of modules is a sequence of modules and homomorphisms*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,$$

such that the image of f is equal to the kernel of g, i.e., $\mathrm{Im}(f) = \ker(g)$.

We would use the short exact sequence for linear space.

Definition 3.4. *Consider $P \in \mathbb{A}^2$ and $F, G, H \in \mathbb{K}[x, y]$, then*

(1) If F, G has no common component cross P, then

$$0 \to \mathcal{O}_P/\langle F, H\rangle \xrightarrow{\bullet G} \mathcal{O}_p/\langle F, GH\rangle \xrightarrow{\pi} \mathcal{O}_P/\langle F, G\rangle \to 0,$$

where π is the natural projection map.

(2) $\mu_P(F, GH) = \mu_P(F, G) + \mu_P(F, H)$.

Proof. (1) π is surjection;

(2) Consider an element acted by multiplication by G:

$$\bullet G : \frac{f}{g} + aF + bH \mapsto F(aG) + G\left(\frac{f}{g} + bH\right) \in \ker \pi,$$

where $a, b \in \mathbb{K}[x, y]$ and $g \in \mathcal{O}_P$. On the other side, consider $f/g \in \ker \pi$, thus $f/g = aF + bG \to b \in \mathcal{O}_p/\langle F, H\rangle$.

(3) $\bullet G$ is injection.

Note that all the vector spaces are finite dimensional, thus the dimension of the kernel is equal to the dimension of the image, and we can conclude that

$$\mu_P(F, GH) = \mu_P(F, G) + \mu_P(F, H),$$

which proofs the proposition (5). $\square$

3.2 The Algorithm to Compute Intersection Number

Consider $F(x, y) \in \mathbb{K}[x, y]$, in order to compute the insertion number $\mu_0(y, F(x, y))$, we can expand F as $F(x, y) = F(x, 0) + yH(x, y)$, thus

$$\mu_0(y, F(x, y)) = \mu_0(y, F(x, 0) + yH(x, y)) = \mu_0(y, F(x, 0)).$$

Assume $F(x, 0) = x^m f(x)$ where $f(x)$ is no vanishing at $x = 0$, thus

$$\mu_0(y, F(x, y)) = m.$$

Now we shell consider the linear (homogeneous 1 degree part). We denote $F \in \mathbb{K}[x, y]$ as

$$F = F_0 + F_1 + \cdots$$

where F_i is homogeneous degree i part. The F_1 part is important, because of the theorem below:

Theorem 3.3 (2.17 Intersection multiplicity 1). *If $F, G \in \mathbb{K}[x, y]$ pass through the origin, then*

$$\mu_0(F, G) = 1 \Leftrightarrow F, G \text{ Linear Independent}$$

Definition 3.5 (Tangents and multiplicities of points). *Let $F \in \mathbb{K}[x, y]$ be a curve, then*

(1) The smallest $m \in \mathbb{N}$ for which the homogeneous part F_m is non-zero is called the multiplicity $m_0(F)$ of F at the origin. Any linear factor of F_m (considered as a curve) is called a tangent to F at the origin.

(2) For a general point $P = (x_0, y_0) \in \mathbb{A}^2$, tangents at P and the multiplicity $m_P(F)$ are defined by first shifting coordinates to $x' = x - x_0$ and $y' = y - y_0$, and then applying (a) to the origin $(x', y') = (0, 0)$.

4 Day III: Intersection Number (2)

Definition 4.1 (Cusps). *Let P be a point on an affine curve F. We say that P is a cusp if $m_P(F) = 2$, there is exactly one tangent L to F at P, and $\mu_P(F, L) = 3$.*

Definition 4.2 (Singular Curve and Non-singular Curve). *An affine curve $F \in \mathbb{K}[x, y]$ is called singular if it has a point P such that $\mu_P(F) > 1$. If F has no point P such that $\mu_P(F) > 1$, then F is called non-singular.*

where the multiplicity $\mu_P(F)$ is defined as the number of tangents at P.

Proposition 4.1 (Affine Jacobi Criterion). *Let $P = (x_0, y_0)$ be a point on an affine curve F.*

(a) P is a singular point of F if and only if

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = 0,$$

(b) If P is a smooth point of F, the tangent to F at P is given by

$$T_P F = \frac{\partial F}{\partial x}(P) \cdot (x - x_0) + \frac{\partial F}{\partial y}(P) \cdot (y - y_0).$$

Example 4.1. *Consider the tangent $T_P F$ of the curve $F \in \mathbb{K}[x, y]$, compute the intersection number $\mu_P(F, T_P F)$.*

Solution. First, one can consider some basic examples. For example, consider $F = y - x^2$, thus the tangent at $P = (0, 0)$ is $T_P F = y$, so that the intersection number is

$$\mu_0(y, y - x^2) = 2.$$

Moreover, one can prove that $\mu_P(T_P F, F) = 2$ for $F = y - x^2$. □

Theorem 4.2. *Let P be a smooth point on a curve F . Then for any two curves G and H that do not have a common component with F through P we have*

$$\langle F, G\rangle \subset \langle F, H\rangle \text{ in } \mathscr{O}_P \quad \Leftrightarrow \quad \mu_P(F, G) \geq \mu_P(F, H).$$

5 Day IV: Projective Curve (1)

Definition 5.1 (Projective Space). *For $n \in \mathbb{N}$, we define the projective space $\mathbb{P}^n(\mathbb{K})$ as the set of equivalence classes of non-zero vectors in $\mathbb{K}^{n+1}$, where two vectors $(x_0, x_1, \ldots, x_n)$ and $(y_0, y_1, \ldots, y_n)$ are equivalent if there exists a non-zero scalar $\lambda \in \mathbb{K}$ such that*

$$\sim: (x_0, x_1, \ldots, x_n) = \lambda(y_0, y_1, \ldots, y_n).$$

The projective space could thus be defined as:

$$\mathbb{P}^n = \left\{ \mathbb{A}^{n+1}_{\mathbb{K}} - \{0\} \right\} / \sim .$$

Example 5.1. *Consider the projective space $\mathbb{C}P^2 = \mathbb{C}^3 - \{0\} / \sim$, one would induce the fiberation:*

$$\mathbb{S}^1 \to \mathbb{S}^5 \xrightarrow{\pi} \mathbb{C}P^2.$$

Example 5.2. *Consider the curve $F = y - x^2$, in $\mathbb{P}^2$ we can introduce the homogeneous coordinate $[x : y : z]$, thus the curve can be written as:*

$$F = yz - x^2,$$

while $z = 0$ (the point at infinity), we have $[0 : 1 : 0]$, which is the point at infinity of the curve F.

6 Day V: Projective Curve (2)

Consider the local ring $\mathcal{O}_P$ at a point $P \in \mathbb{P}^2$, which could be defined as

$$\mathcal{O}_P = \left\{ \frac{F}{G}; F, G \in \mathbb{K}[x, y, z], G(P) \neq 0 \right\} \cong \left\{ \frac{f}{g}; f, g \in \mathbb{K}[x, y], g(p) \neq 0 \right\}.$$

From projective space to affine space, we could define the map 'homogenization' and 'dehomogenization' as follows:

$$f(x, y) = \sum_{jk} a_{jk} x^j y^k \in \mathbb{K}[x, y] \mapsto f^h = \sum_{i,j} a_{ij} x^i y^j z^{n-i-j} \in \mathbb{K}[x, y, z], \quad \deg f = n,$$
$$F(x, y, z) = \sum_{i,j} a_{ij} x^i y^j z^{n-i-j} \in \mathbb{K}[x, y, z] \mapsto F^i(x, y, 1) = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{K}[x, y].$$

where the first map is called 'homogenization' and the second map is called 'dehomogenization', where we have a bijective correspondence:

$$\{\text{polynomials of degree } d \text{ in } K[x, y]\} \longleftrightarrow \left\{\begin{matrix}\text{homogeneous polynomials of degree } d \text{ in } K[x, y, z] \\ \text{not divisible by } z\end{matrix}\right\}$$
$$f \longmapsto f^{\mathrm{h}}$$
$$f^{\mathrm{i}} \longleftrightarrow f.$$

which showed the isomorphism shown in the begin of this section.

Construction 6.1 (Affine parts and projective closures). *(a) For a projective curve F its affine set of points is $V_p(F) \cap \mathbb{A}^2 = V_a(F(z = 1)) = V_a(F^i)$. We will therefore call F^i the **affine part** of F. The points at infinity of F are given by $V_p(F(z = 0)) \subset \mathbb{P}^1$.*

*(b) For an affine curve F we call F^h its **projective closure**. By Construction 3.13 it is a pro- jective curve whose affine part is again F, and that does not contain the line at infinity as a component.*

However, F^h may contain points at infinity: If $F = F_0 + \cdots + F_d$ is the decomposition into homogeneous parts as in Notation 2.16, we have $F^h = z^d F_0 + z^{d-1} F_1 + \cdots + F_d$ and hence $F^h(z = 0) = F_d$. So the points at infinity of F are given by the projective zero locus of the leading part of F.

Using the discussion above, we could define the intersection number of a projective curve F and G as

$$\mu_P(F, G) = \dim_{\mathbb{K}} \mathcal{O}_P / \langle F, G \rangle,$$

where $P \in \mathbb{P}^2$, $\langle F, G \rangle$ is the homogeneous ideal generated by homogeneous F and G, which could be defined as

Definition 6.1 (Homogeneous Ideal)**.** *Let $K[x_1, \ldots, x_n]$ be a polynomial ring. A subset $I \subset K[x_1, \ldots, x_n]$ is called a* ***homogeneous ideal****, which could be constructed below: For homogeneous polynomials $F_1, \ldots, F_k$, we can define the generated homogeneous ideal as:*

$$\langle F_1, \ldots, F_k \rangle = \left\{ \frac{f_1}{g_1} F_1 + \cdots + \frac{f_k}{g_k} F_k : f_i = 0 \text{ or } f_i, g_i \in K[x, y, z] \text{ homogeneous} \right.$$
$$\left. \text{with } g_i(P) \neq 0 \text{ and } \deg(f_i F_i) = \deg g_i \text{ for all } i \right\}$$

another way to compute the intersection number is to use the homogenization and dehomogenization, thus we shell replace the projective curve F and G with their affine parts F^i and G^i, and compute the intersection number at $P \in \mathbb{A}^2_{\mathbb{K}}$.

Example 6.1. *Compute the intersection number of the projective curve $F = yz - x^2$ and $G = z$ at the point $P = [0 : 1 : 0]$.*

Solution. We shell compute the intersection number at the point $P = (x, z) = (0, 0) \in \mathbb{A}^2_{\mathbb{K}}$, thus we have

$$\begin{aligned} \mu_P(F, G) &= \dim_{\mathbb{K}} \mathcal{O}_P / \left\langle F^i, G^i \right\rangle \\ &= \dim_{\mathbb{K}} \mathcal{O}_P / \left\langle z - x^2, z \right\rangle \\ &= \dim_{\mathbb{K}} \mathcal{O}_P / \left\langle z, x^2 \right\rangle \\ &= 2. \end{aligned}$$

□

7 Day V: Bézout Theorem

Recall that a field $\mathbb{K}$ is called **algebraically closed** if every univariate polynomial $f \in \mathbb{K}[x]$ without a zero in $\mathbb{K}$ is constant.

Theorem 7.1 (Hilbert's Nullstellensatz)**.** *TBD.*

Theorem 7.2 (Bézout Theorem)**.** *Let $F, G \in \mathbb{K}[x, y]$ be two projective curves of degrees d_F and d_G, respectively. If F and G have no common component, $\mathbb{K}$ is algebraically closed, then the number of intersection points of F and G in $\mathbb{P}^2_{\mathbb{K}}$ is given by*

$$\sum_{P \in F \cap G} \mu_P(F, G) = d_F \cdot d_G,$$

where $P \in \mathbb{P}^2_{\mathbb{K}}$. If $\mathbb{K}$ is not algebraically closed, then the intersection number is satisfied

$$\sum_{P \in F \cap G} \mu_P(F, G) < \deg F \cdot \deg G.$$

Lemma 7.3 (Finiteness of the intersection multiplicity)**.** *Let F and G be two curves without a common component that passes through the origin, then:*

(1) There is a number $n \in \mathbb{N}$ such that $x^n = y^n = 0$ in $\mathcal{O}_0 / \langle F, G \rangle$,

(2) Every element of $\mathcal{O}_0 / \langle F, G \rangle$ can be written as a polynomial in x and y of degree less than n.

Proof. TBD. □

Lemma 7.4. *Consider $F, G \in \mathbb{K}[x, y]$, consider $P \in F \cap G$, then diagram*

$$\begin{tikzcd} \mathbb{K}[x,y] \arrow[r] \arrow[d] & \mathcal{O}_P \arrow[d] \\ \mathbb{K}[x,y]/\langle F,G\rangle \arrow[r] & \prod_{P\in F\cap G}\mathcal{O}_P/\langle F,G\rangle, \end{tikzcd}$$

is commutative, where the vertical maps are the natural projection maps. Moreover, if $\mathbb{K}$ is algebraically closed, then the natural ring homomorphism

$$\varphi : \mathbb{K}[x,y]/\langle F,G\rangle \ni f \mapsto \prod_{P\in F\cap G} f(P) \in \prod_{P\in F\cap G}\mathcal{O}_P/\langle F,G\rangle,$$

is an isomorphism. If $\mathbb{K}$ is not algebraically closed, then the map is surjective.

Proof. Let $F\cap G = \{P_1,\cdots,P_2\}$ where $P_i = (x_i,y_i)$. Consider

$$f = \prod_{i:x_i\neq x_0}(x-x_i)^n \prod_{i:y_i\neq y_0}(y-y_i)^n \in \mathbb{K}[x,y],$$

TBD. □

Lemma 7.5. *F, G are two projective curves, if $F_{\deg F}$ and $G_{\deg G}$ has no common component, then for all $f\in\langle F,G\rangle\subset\mathbb{K}[x,y]$ of degree d can be written as $f = aF+bG$, where $\deg a\leq d-m$ and $\deg b\leq d-n$.*

Corollary 7.6 (Max Noether's Theorem)**.** *Let F be a smooth projective curve over an algebraically closed field. Moreover, let G and H be two projective curves that do not have a common component with F. If $\mu_P(F,G)\leq\mu_P(F,H)$ for all points $P\in F\cap G$ then there are homogeneous polynomials A and B (of degrees $\deg H-\deg F$ resp. $\deg H-\deg G$ if non-zero), such that*

(a) $H = AF+BG$;

(b) $\mu_P(F,H) = \mu_P(F,G)+\mu_P(F,B)$ *for all* $P\in\mathbb{P}^2$.

Proof. Where the second part of the corollary is trivial. □