ALGEBRAIC CURVES

TSE-YU SU

21st November 2025

CONTENTS

1 AFFINE ALGEBRAIC SETS

1.1 *Affine Space and Algebraic Sets*

1.1 DEFINITION. Let k be a field, we define the **affine n-space** $\mathbb{A}^n(k)$,or $\mathbb{A}^n$ if k is clear, to be the set of n-tuples of elements of k.

If $F \in k[X_1, ..., X_n]$, a point $P = (a_1, ..., a_n)$ is said to be a **zero** of F if

$F(P) = F(a_1, ..., a_n) = 0$. For $F \neq const$, the set of zeros of F is called the **hypersurface** defined by F, and is denoted by V(F). If F is of degree 1, V(F) is called a **hyperplane** in $\mathbb{A}^n$.

For S: a set of polynomials in $k[X_1, ..., X_n]$, define V(S) to be the set of all common zeros of $F \in S$.

A subset $X \subseteq \mathbb{A}^n(k)$ is called an **affine algebraic set**, or simply **algebraic set**, if $X = V(S)$ for some S.

Can verify that the set of all algebraice sets in $\mathbb{A}^n$ forms a topology, called **Zariski topology**, where the closed sets are exactly the algebraic sets.

Here are some facts about algebraic sets:

- If I is the ideal in $k[X_1, ..., X_n]$ generated by S, then $V(S) = V(I)$. Therefore we can restrict to the case V(I).
- If $\{I_\alpha\}$ is **any** collection of ideals, then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$. So the intersection of **any** collection of algebraic sets is also an algebraic set.
- If $I \subseteq J$, then $V(I) \supseteq V(J)$.
- For polynomials F, G, $V(F) \cup V(G) = V(FG)$, and for ideals I, J, $V(I) \cup V(J) = V(IJ)$. So any **finite union** of algebraic sets is also algebraic.
- $V(0) = \mathbb{A}^n$, $V(1) = V(k[X_1, ..., X_n]) = \varnothing$. And $V(X_1 - a_1, ..., X_n - a_n) = \{(a_1, ..., a_n)\}$. So any finite subset of $\mathbb{A}^n$ is algebraic.
- $V(IJ) = V(I \cap J)$. The $\supseteq$ is clear, now prove $\subseteq$. Let $P \in V(IJ)$, then for every $F \in I, G \in J$, $FG(P) = 0$. Hence for $H \in I \cap J$, $H^2(P) = 0$, so $H(P) = 0$.

1.2 *The Ideal of a Set of Points*

For any $X \subseteq \mathbb{A}^n$, consider those polynomials in $k[X_1, ..., X_n]$ which vanish on X, these polynomials form an ideal $\lhd k[X_1, ..., X_n]$, called the ideal of X, written $I(X) = \{F \in k[X_1, ..., X_n] | F(X) = \{0\}\}$.

The following properties show some relation between ideals and algebraic sets.

- If $X \subseteq Y$, then $I(X) \supseteq I(Y)$
- $I(\varnothing) = k[X_1, ..., X_n]$. $I(\mathbb{A}^n) = 0$. $I(\mathbb{A}^n) = 0$ if k is not finite. A counterexample is $0 \neq x(x-1) \in I(\mathbb{A}^1(\mathbb{Z}_2)) \lhd \mathbb{Z}_2[x]$

- $I(\{a_1, ..., a_n\}) = (X_1 - a_1, ..., X_n - a_n)$
- $S \subseteq I(V(S))$ and $X \subseteq V(I(X))$
- $V(I(V(S))) = V(S)$ and $I(V(I(X))) = I(X)$.

An ideal which is the ideal of an algebraic set, satisfies the following property:

$$\text{If } I = I(X), \text{ and } F^n \in I \text{ for some } n \in \mathbb{N}, \text{ then } F \in I.$$

Consequently, $I(X) = \text{Rad}(I(X)) = \sqrt{I(X)}$ is radical.

1.3 *The Hilbert Basis Theorem*

We defined an algebraic set by any set of polynomials, but in fact finitely many will suffice.

1.2 THEOREM. *Every algebraic set is the intersection of a finite number of hypersurfaces.*

In order to prove this theorem, it suffices to show any ideal $I \lhd k[X_1, ..., X_n]$ is finitely generated by $(F_1, ..., F_s)$, then $V(I) = V(F_1) \cap V(F_2) \cap ... \cap V(F_n)$.

1.3 THEOREM (Hilbert Basis Theorem). *If* R *is a Noetherian ring, then* $R[X]$ *is also Noetherian. Consequetly,* $R[X_1, ..., X_n]$ *is Noetherian.*

1.4 *Irreducible Components of an Algebraic Set*

An algebraic set may be the union of serveral smaller algebraic sets. An algebraic set $V \subseteq \mathbb{A}^n$ is said to be **reducible** if $V = V_1 \cup V_2$, where $V_1 \neq V \neq V_2$ are algebraic. Otherwise V is **irreducible**.

1.4 PROPOSITION. *An algebraic set* V *is irreducible if and only if* $I(V)$ *is prime.*

We want to show that an algebraic set is the union of finitely many irreducible algebraic sets. If V is reducible, write $V = V_1 \cup V_2$, if V_2 is reducible, write $V_2 = V_3 \cup V_4$, need to show this process stops.

Since $k[X_1, ..., X_n]$ is Noetherian, each set of ideals has an maximal element, consequently, any collection of algebraic sets in $\mathbb{A}^n$ has an minimal element.

1.5 THEOREM. *Let* V *be an algebraic set in* $\mathbb{A}^n(k)$*, then there are unique irreducible algebraic sets* $V_1, ..., V_m$ *such that* $V = V_1 \cup V_2 \cup ... \cup V_m$ *and* $V_i \not\subseteq V_j$ *for* $i \neq j$.

Proof. Let $\mathcal{S}$ be the set of all algebraic sets $V \subseteq \mathbb{A}^n$ which is not the union of a finite number of irreducible. Choose an minimal element V in $\mathcal{S}$, clearly V is reducible, say $V = V_1 \sup V_2$, where $V_i \neq V$. But then $V_i \subsetneq V$, so V_i is a union of finitely many irreducible algebraic sets, hence so is $V = V_1 \cup V_2$, a contradiction. To show $V_i \not\subseteq V_j$ for $i \neq j$, simply delete every algebraic set which is contained in another bigger algebraic set.

To show uniqueness, let $V = W_1 \cup ... \cup W_s$. Since $V_i = V \cap V_i = \cup_j (W_j \cap V_i)$, and V_i is irreducible, $V_i \subseteq W_{j(i)}$ for some $j(i)$. Similarly, $W_{j(i)} \subseteq V_{k(j(i))}$ for some $k(j(i))$, but then $V_i \subseteq V_{k(j(i))}$, hence $i = k(j(i))$ and $V_i = W_{j(i)}$. Likewise $W_j = V_{i(j)}$ for some $i(j)$, so $s = n$ and $W_i = V_i$ after renumbering. □

These $V_1, ..., V_n$ are called the irreducible components of V, and $V = V_1 \cup ... \cup V_n$ is the decomposition of V into irreducible components.

1.5 *Algebraic Subsets of the Plane*

Will classify all irreducible algebraic sets of $\mathbb{A}^2(k)$ in this subsection. Once this classification has been done, by Theorem 1.2 we have found all algebraic sets.

1.6 PROPOSITION. *Let* $F, G \in k[X, Y]$ *with no common factors. Then* $V(F, G) = V(F) \cap V(G)$ *is a finite set of points.*

Proof. Consider $A = (F, G) \cap k[X]$, A is an ideal of $k[X]$. Since $k[X]$ is PID, $A = (f(X))$. So $FH + GK = f(X)$ for some $H, K \in k[X, Y]$. Thus the X−component of points in $V(F, G)$ are roots of $f(X)$, which is finitely many. Similarly, the Y−component of points in $V(F, G)$ are roots of some $g \in k[Y]$. Hence $V(F, G) \subseteq \{(a, b) | f(a) = g(b) = 0\}$, which is finite. □

1.7 COROLLARY. *If* F *is irreducible in* $k[X, Y]$, *and if* V(F) *is infinite, then* $I(V(F)) = (F)$ *and* V(F) *is irreducible.*

Proof. Take $G \in I(V(F))$, clearly $G(V(F)) = \{0\}$, hence $V(F) \subseteq V(F, G)$, and $V(F, G)$ is infinite. By the previous proposition F, G must have common factor, since F is irreducible this common factor can only be F, so $G \in (F)$, and thus $I(V(F)) = (F)$, and by proposition 1.4 V(F) is irreducible. □

1.8 COROLLARY. *Suppose k is infinite, then the irreducible algebraic subsets of* $\mathbb{A}^2(k)$ *are:*

$\mathbb{A}^2(k)$,

$\emptyset$,

points,

irreducible plane curves V(F)

where F *is an irreducible polynomial and* V(F) *is infinite.*

Note: Not all zero sets of irreducible polynomial in $k[X, Y]$ is infinte, for example $X^2 + Y^2 \in \mathbb{R}[X, Y]$ is irreducible, but the zero set $\{(0, 0)\}$ is finite.

1.9 COROLLARY. *Assume k is algebraically closed, and* $F \in k[X, Y]$. *Let* $F = F_1^{n_1} ... F_r^{n_r}$ *be the decomposition of* F *into irreducible factors. Then* $V(F) = V(F_1) \cup ... \cup V(F_r)$ *is the decomposition of* F *into irreducible components, and* $I(V(F)) = (F_1 F_2 ... F_r)$.

Proof. $V(F) = V(F_1) \cup ... \cup V(F_r)$ is clear. Since k is algebraically closed, $V(F_i)$ is infinite, and by the previous corollary $V(F_i)$ is irreducible.

(Note: The cases such as $X^2 + Y^2 \in \mathbb{R}[X, Y]$, which is irreducible but has finite zero set, won't happen.)

Also, since $F_i \nmid F_j$, there's no inclusion relation among $V(F_i)$.

The next part $I(V(F)) = (F_1 F_2 ... F_r)$ is also clear.

□

The following problem shows why we usually require k to be algebraically closes.

QUESTION. Show that every algebraic subset of $\mathbb{A}^2(\mathbb{R})$ is equal to some $V(F)$, where $F \in \mathbb{R}[X, Y]$.

Proof. It suufices to show any finite set of points $\{(a_1, b_1), ..., (a_r, b_r)\}$ in $\mathbb{A}^2(\mathbb{R})$ can be written as $V(F)$ for some $F \in \mathbb{R}[X, Y]$.

Since $(X - a)^2 + (Y - b)^2$ has only one zero (a, b) in $\mathbb{A}^2(\mathbb{R})$, $F = \prod_{i=i}^{r}((X - a_i)^2 + (Y - b_i)^2)$ is the desired polynomial. □

1.6 *Hilbert's Nullstellensatz*

we assume k is algebraically closed in this subsection.

Want to find the exact relation between algebraic sets and ideals. Will first prove a weaker theorem:

1.10 THEOREM (Weak Nullstellensatz). *If* I *is a proper ideal in* $k[X_1, ..., X_n]$, *then* $V(I) \neq \emptyset$.

Proof. Since I is contained in some maximal ideal $\mathfrak{m}$, and $V(\mathfrak{m}) \subseteq V(I)$, it suffices to show for every maximal ideals $\mathfrak{m}$, $V(\mathfrak{m}) \neq \emptyset$.

Will use the following fact:

Fact: If k is algebraically closed, then maximal ideals of $k[X_1, ..., X_n]$ are of the form $(X_1 - a_1, ..., X_n - a_n)$.

By the above fact $V(X_1 - a_1, ..., X_n - a_n) = \{(a_1, ..., a_n)\} \neq \emptyset$. □

1.11 THEOREM (Hilbert's Nullstellensatz). *Let* I *be an ideal in* $k[X_1, ..., X_n]$, k *is algebraically closed. Then* $I(V(I)) = Rad(I)$.

Proof. $Rad(I) \subseteq I(V(I))$ is easy. For another direction, suppose $G \in I(V(F_1, ..., F_r))$, $F_i \in k[X_1, ..., X_n]$, let $J = (F_1, ..., F_r, X_{n+1}G - 1) \subseteq k[X_1, ..., X_n, X_{n+1}]$, can see $\emptyset = V(J) \subseteq \mathbb{A}^{n+1}$. Apply Weak Nullstellensatz to J, $J = k[X_1, ..., X_n, X_{n+1}]$. So $1 = \sum A_i(X_1, ..., X_{n+1})F_i + B(X_1, ..., X_{n+1}) \cdot (X_{n+1}G - 1)$.

Let $Y = \frac{1}{X_{n+1}}$, multiply the above equation sufficiently many times by Y, that the X_{n+1}-degree of each monomial terms is negative. (For example, $X_1X_{n+1}^3 + X_2^3X_{n+1}^5 \xrightarrow{\times Y^5} X_1Y^2 + X_2^3 = P(\{X_i|i = 1, ..., n\}, Y)$)

Then we get an equation $Y^N = \sum C_i(X_1, ..., Y)F_i + D(X_1, ..., X_n, Y)\cdot(G-Y) \in k[X_1, ..., X_n, Y]$, substitute $Y = G$, it follows that $G^N \in (F_1, ..., F_r)$. □

Here are some immediate corollary, for k : algebraically closed:

1.12 COROLLARY. *There is a one-to-one correspondence between* ***radical ideals*** *and* ***algebraic sets****.*

1.13 COROLLARY. *If* I *is prime, then* V(I) *is irreducible. There is a one-to-one correspondence between* ***prime ideals*** *and* ***irreducible algebraic sets****. The maximal ideals correspond to points.*

1.14 COROLLARY. *Let* $F = F_1^{n_1}...F_r^{n_r}$ *be the decomposition of* F *into irreducible factors, then* $V(F) = V(F_1) \cup ... \cup V(F_r)$ *is the decomposition of* V(F) *into irreducible components, and* $I(V(F)) = (F_1F_2...F_r)$.

There is a one-to-one correspondence between ***irreducible polynomials****(up to multiplying by a unit) and* ***irreducible hypersurfaces*** *in* $\mathbb{A}^n(k)$*. Remenber that a hypersurface is the zero set of a polynomial.*

$$\text{Radical ideals} \leftrightarrow \text{Algebraic sets}$$
$$\text{Prime ideals} \leftrightarrow \text{Irreducible algebraic sets}$$
$$\text{Irreducible polynomials} \leftrightarrow \text{Irreducible hypersurfaces}$$

1.15 COROLLARY. *Let* I *be an ideal in* $k[X_1, ..., X_n]$*, then* V(I) *is a finite set if and only if* $k[X_1, ..., X_n]/I$ *is a finite dimensional vector space over* k*. In this case the number of points in* V(I) *is less or equal to* $dim_k(k[X_1, ..., X_n]/I)$.

Proof. Assume $k[X_1, ..., X_n]/I$ is a finite dimensional vector space over k, let points $P_1, ..., P_r \in V(I)$, choose polynomials $F_i \in k[X_1, ..., X_n], i = 1, ..., r$ s.t. $F_i(P_i) = 1$ and $F_i(P_j) = 0$ for $i \neq j$. Want to show I−redidue classes $\bar{F}_i$ are linearly independent over k. If $\sum_{i=1}^r \lambda_i\bar{F}_i = 0$, then $\sum_{i=1}^r \lambda_iF_i \in I$, so $\lambda_j = \sum_{i=1}^r \lambda_iF_i(P_j) = 0$, hence $\bar{F}_i$ are linearly independent over k, so $r \leq \dim_k(k[X_1, ..., X_n]/I)$.

Conversely, if $V(I) = \{P_1, ..., P_r\}$ is finite, let $P_i = (a_{i,1}, ...a_{i,n})$, and for $j = 1, ..., n$ define $F_j = \prod_{s=1}^r(X_j - a_{s,j})$, clearly $F_j \in V(I)$, so by Nullstellensatz $F_j^N \in I$ for some N, WLOG take N so large that it holds for all F_j. Consequently $\bar{F_j^N} = 0$, for all j and since $F_j^N \in I$ is a polynomial in X_j of degree rN, $\bar{X_j}^{rN}$ is a k−linear combination of $1, X_j^1, X_j^2, ..., X_j^{rN-1}$, and hence so is any positve order X_j^s. Therefore $\{\bar{X_1}^{m_1}\cdot\bar{X_2}^{m_2}\cdot...\cdot\bar{X_n}^{m_n}\}$ generates $k[X_1, ..., X_n]/I$ as a vector space over k. □

2 AFFINE VARIETIES

2.1 *Coordinate Rings*

Recall that if $V \subseteq \mathbb{A}^n$ is a variety, then $I(V)$ is a prime ideal and $k[X_1, ..., X_n]/I(V)$ is a domain. We denote $\Gamma(V) = k[X_1, ..., X_n]/I(V)$ and call it the **coordinate ring** of V.

For any $S \neq \emptyset$, let $\mathcal{F}(V, k)$ be the ring of all functions from V to k, with the obvious addition and multiplication $f \cdot g(x) = f(x) \cdot g(x)$.

If $V \in \mathbb{A}^n$ is a variety, $f \in \mathcal{F}(V, k)$ is called a **polynomial function** if there is a polynomial $F \in k[X_1, ..., X_n]$ s.t. $F(a_1, ..., a_n) = f(a_1, ..., a_n)$ for all $(a_1, ..., a_n) \in V$. These polynomial functions form a subring of $\mathcal{F}(V, k)$ containing k (the identity functions), and two polynomial F, G determine the same function iff $F - G$ vanishes on V, i.e. $F - G \in I(V)$. Thus we consider $\Gamma(V)$ as a subring of $\mathcal{F}(V, k)$ consisting of all polynomial functions on V.

2.2 *Polynomial Maps*

Let $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m$, a mapping $\varphi : V \to W$ is called a **polynomial map** if there are polynomials $T_1, ..., T_m \in k[X_1, ..., X_n]$ s.t. $\varphi(a_1, ..., a_n) = (T_1(a_1, ..., a_n), ..., T_m(a_1, ..., a_n))$ for all $(a_1, ..., a_n)$.

Any mapping $\varphi : V \to W$ induces a homomorphism $\tilde{\varphi} : \mathcal{F}(W, k) \to \mathcal{F}(V, k)$, by letting $\tilde{\varphi}(f) = f \circ \varphi$.

$$\begin{array}{ccc} W & \xrightarrow{f} & k \\ {\scriptstyle\varphi}\uparrow & \nearrow_{f \circ \varphi} & \\ V & & \end{array}$$

If φ is a polynomial map, then $\tilde{\varphi}(\Gamma(W)) \subseteq \Gamma(V)$, i.e. $\tilde{\varphi}$ sends polynomial functions on W to polynomial functions on V. To show this, need only to check that $\tilde{\varphi}$ is well defined on residue class $f + I(W) \in \Gamma(W)$. Let $g \in I(W)$, $\tilde{\varphi}(g) = g \circ \varphi$, since φ maps V to W, $g \circ \varphi$ vanished on V, and the result follows.

If $V = \mathbb{A}^n$, $W = \mathbb{A}^m$, and $T_1, ..., T_m$ determine a polynomial map $T : \mathbb{A}^n \to \mathbb{A}^m$, then T_i are unique determined by T, i.e. there are no other distinct $T_1', ..., T_m'$ whcih induced the same polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$.

2.1 PROPOSITION. *Let $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m$ be affine varieties. There is a natural one-to-one correspondence between the polynomial maps $\varphi : V \to W$ and the homomorphisms $\tilde{\varphi} :] = \Gamma(W) \to \Gamma(V)$. Any such φ is the restriction of a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$.*

Proof. Let $\alpha : \Gamma(W) \to \Gamma(V)$ be a homomorphism, choose $T_1, ..., T_m \in k[X_1, ..., X_n]$ s.t. $T_i + I(V) = \alpha(X_i + I(W)) + I(V)$ in $\Gamma(V)$, then $T = (T_1, ..., T_m)$ is a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$, which induces $\tilde{T} : k[X_1, ..., X_m] \to k[X_1, ..., X_n]$. To check T restrict to $V \to W$, observe that for $f(X_1, ..., X_m) \in I(W)$, $\tilde{T}(f) = f \circ T = f(T_1, ..., T_m) \equiv \alpha(f(X_1, ..., X_m)) \equiv 0$ in $\Gamma(V)$, thus $T(V) \subseteq W$. Finally, it is easy to verify $\widetilde{T|_V} = \alpha$. □

A polynomial map $\varphi : V \to W$ is an isomorphism if there is $\psi : W \to V$ s.t. $\varphi \circ \psi$ and $\psi \circ \varphi$ are identities on W, V respectively. The previous proposition shows that two affine variety are isomorphic iff their coordinate rings are isomorphic over k.

A useful test for irrducibily: Let $\varphi : V \to W$ be a polynomial map, and $X \subseteq W$ is a algebraic subset, then $\varphi^{-1}(X)$ is also an algebraic subset in V. Moreover, if $\varphi^{-1}(X)$ is irreducible and X is contained in the image $\varphi(V)$, then $\varphi^{-1}(X)$ is also irreducible.

For example, $V = V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y) = \{(t^3, t^4, t^5) | t \in k\}$ is the image of $\varphi : \mathbb{A}^1 \to \mathbb{A}^3$, $\varphi(t) = (t^3, t^4, t^5)$, since $\mathbb{A}$ is irreducible, so is V.

2.3 *Coordinate Changes*

If $T = (T_1, ..., T_m)$ is a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$, and $F \in k[X_1, ..., X_m]$, we denote $F^T = \tilde{T}(F) = F(T_1, ..., T_m) \in k[X_1, ..., X_n]$. For ideal I and algebraic set V in $\mathbb{A}^m$, I^T denote the ideal $\lhd k[X_1, ..., X_n]$ generated by F^T, $F \in I$, and V^T the algebraic set $V(I^T)$, where $I = I(V)$. If V is the hypersurface of F, then V^T is the hypersurface of F^T, for $F \neq$ constant.

An **affine change** of coordinates on $\mathbb{A}^n$ is a **invetible** polynomial map $T = (T_1, ..., T_n) : \mathbb{A}^n \to \mathbb{A}^n$ s.t. each T_i is a polynomial **of degree 1**. Not hard to see that T is a composition of a linear map $\tilde{T} : X_j \to \sum_i a_{ij} X_i$ and a translation $T_a : v \mapsto v + a$. Since any translation has inverse, it follows that $\tilde{T}$ is also invertible.

2.4 *Rational Functions and Local Rings*

Let $\varnothing \neq V \subseteq \mathbb{A}^n$, $\Gamma(V)$ the coordinate ring. Since $\Gamma(V)$ is a domain, may form its quotient field, called the **field of rational functions** on V, and is written $k(V)$.

Let $f \in k(V)$ and $P \in V$, we say that f is defined at P if $f = h/g$for some $h, g \in \Gamma(V)$, $g(P) \neq 0$, in other words, find a "denominator" for f that doesn't vanish at P. If $\Gamma(V)$ is UFD, then there is an unique representation $f = h/g$, where $h, g \in \Gamma(V)$ have no common factors, and f is defined at P iff $g(P) \neq 0$.

Fix $P \in V$, define $\mathcal{O}_P(V)$ to be the set of rational functions on V that are defined at P. It is easy to verify that $\mathcal{O}_P(V)$ forms a subring of $k(V)$ containing $\Gamma(V)$:

$$k \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset k(V)$$

The ring $\mathcal{O}_P(V)$ is called the local ring of V at P.

For a rational function $f \in k(V)$, the set of points $P \in V$ where f is not defined is called the **pole set** of f.

2.2 PROPOSITION.

(1) The pole set of a rational function is an algebraic subset of V.

(2) $\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V)$

Proof. For $f \in k(V)$, $G \in k[X_1, ..., X_n]$, $\bar{G}$ denotes the residue class in $\Gamma(V)$. Let $J_f = \{G \in k[X_1, ..., X_n] | \bar{G}f \in \Gamma(V)\}$. J_f is an ideal $\lhd k[X_1, ..., X_n]$ containing $I(V)$, and the points of $V(J_f)$ are exactly those where f is not defined, this proves (1). For (2), if $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$, then $V(J_f) = \varnothing$, since f is defined on every point of V. So $J_f = k[X_1, ..., X_n]$ by Nullstellensatz, thus $1 \cdot f \in \Gamma(V)$, which proves (2). □

Suppose $f \in \mathcal{O}_P(V)$, can define the value of f at P, written $f(P)$. Consider the kernel $\mathfrak{m}_P(V)$ of the evaluation map $f \mapsto f(P)$, called the maximal ideal of V at P. Since $\mathcal{O}_P(V)/\mathfrak{m}_P(V) \cong k$ is a field, and an element $f \in \mathcal{O}_P(V)$ is an unit in $\mathcal{O}_P(V)$ iff $f(P) \neq 0$, therefore $\mathfrak{m}_P(V) = \{\text{non-unit of } \mathcal{O}_P(V)\}$.

2.3 LEMMA. *The following conditions on a ring* R *are equivalent:*

(1) The set of non-unit in R *forms an ideal.*

(2) R *has a unique maximal ideal that contains every proper ideal of* R.

Proof. (1) $\Rightarrow$ (2) : Cleary every proper ideal must be contained in the set of all non-units.

(2) $\Rightarrow$ (1) : Let z be non-unit, consider the ideal (z) generated by z, by assumption this ideal is contained in the unique maximal ideal $\mathfrak{m}$, so $z \in \mathfrak{m}$. Clearly $\mathfrak{m}$ contains no unit, so the non-units form an ideal. □

2.4 PROPOSITION. $\mathcal{O}_P(V)$ *is a Noetherian local domain.*

Proof. Must show any ideal $I \lhd \mathcal{O}_P(V)$ is finitely generated.

By the following fact:

FACT: For a short exact sequence of R−mods:

$$0 \to M_3 \to M_2 \to M_1 \to 0$$

TFAE:

(1) M_2 is a Noetherian R−mod.

(2) M_1 and M_3 are Noetherian R−mod.

Since $I(V), k[X_1, ..., X_n], \Gamma(V)$ can be viewed as $k[X_1, ..., X_n]$−mods, and by Hilberts's Basis Theorem and the above fact, $\Gamma(V)$ is Noetherian.

Consider $I \cap \Gamma(V)$ as an ideal of $\Gamma(V)$, then $I \cap \Gamma(V)$ is generated by $f_1, ..., f_r$ in $\Gamma(V)$. Now show these $f_1, ..., f_r$ actually generates I in $\mathcal{O}_P(V)$ — for if $f \in \mathcal{O}_P(V)$, then $f = h/g$ for some $h, g \in \Gamma(V)$, and thus $f \cdot g \in \Gamma(V) = \sum a_i f_i$, therefore $f = \sum \frac{a_i}{g} f_i$. □

2.5 *Discrete Valuation Ring*

2.5 PROPOSITION. *Let* R *be a domain that is not a field, then TFAE:*

(1) R *is* ***Noetherian*** *and* ***local****, and the maximal ideal is* ***principal****.*

(2) There is an irreducible element $t \in \mathrm{R}$ *.st. every nonzero* $z \in \mathrm{R}$ *may be written uniquely in the form* $z = ut^n$*, where* u *is an unit in* R, $n \in \mathbb{N}$.

Proof. Will use the following theorem:

> THEOREM (Krull Intersection Theorem). If R is a local Noetherian ring with maximal ideal $\mathfrak{m}$, then:
> $$\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = \{0\}$$

(1) $\Rightarrow$ (2) : Let $\mathfrak{m} = (m)$. Using Krull Intersection Theorem, there is a unique $n \in \mathbb{N}$ s.t. $z \in (m^n)$ but $z \notin (m^{n+1})$. Write $z = u \cdot m^n$. Since if u is a non-unit, then $u \in (m)$, thus $m^{n+1} \mid z$, so u is a unit, done.

(2) $\Rightarrow$ (1): Easy to see (t) is principal and consits of all non-unit, and all ideals are principal of the form (t^n), so R is PID, hence Noetherian. □

A ring satisfies the above conditions is called a **discrete valuation ring**, written DVR. An element t as in (2) is called a **uniformizing parameter** for DVR R.

Let K be the fraction field of R, then any nonzero $z \in \mathrm{K}$ has an unique expression $z = ut^n$, where u is unit and $n \in \mathbb{Z}$, n is called the order of z. We define $\mathrm{ord}(0) = \infty$. Note that $\mathrm{R} = \{z \in \mathrm{K} | \mathrm{ord}(z) \geq 0\}$ and $\mathfrak{m} = \{z \in \mathrm{K} | \mathrm{ord}(z) > 0\}$.

NOTE: Consider fraction field $k(\mathrm{X})$ of $k[\mathrm{X}]$, the DVR's containing k are:

1. Localization at point $a \in k$: $\mathcal{O}_a = \{\mathrm{F/G} \in k(\mathrm{X}) | \mathrm{G}(a) \neq 0\}$
2. Localization "at infinity": $\mathcal{O}_\infty = \{\mathrm{F/G} \in k(\mathrm{X}) | \deg(\mathrm{G}) \geq \deg(\mathrm{F})\}$

The second one cannot be expressed as a localization of the form $\mathrm{S}^{-1}k[\mathrm{X}]$. In fact, it doesn't even contain $k[\mathrm{X}]$.

This motivates the concept of projective varieties in Chapter 4.

2.6 *Forms*

2.6 DEFINITION (Forms). A polynomial $f \in k[\mathrm{X}_1, ..., \mathrm{X}_n]$ is called a **form** of degree d if:

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

i.e. every monomial in f is of degree d.

Let R be a domain, if $F \in R[X_1, ..., X_{n+1}]$ is a form, we define $F_* \in R[X_1, ..., X_n]$ by letting $F_* = F(X_1, ..., X_n, 1)$. Conversely, for any polynomial $f \in R[X_1, ..., X_n]$ of degree d, write $f = f_0 + f_1 + ... + f_d$, where f_i is a form of degree i, then define $f^* \in R[X_1, ..., X_n, X_{n+1}]$ by setting:

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + ... + f_d = X_{n+1}^d f(X_1/X_{n+1}, ..., X_n/X_{n+1})$$

Then f^* is a form of degree d. These processes are described as "dehomogenizing" and "homogenizing" polynomials with respect to X_{n+1}.

2.7 PROPOSITION.

(1) $(FG)_* = F_* G_*$; $(fg)^* = f^* g^*$.

(2) If $F \neq 0$ *and r is the highest power of* X_{n+1} *that divides* F, *then* $X_{n+1}^r (F_*)^* = F$; $(f^*)_* = f$.

(3) $(F + G)_* = F_* + G_*$; $X_{n+1}^t (f+g)^* = X_{n+1}^r f^* + X_{n+1}^s g^*$, *where* $r = deg(g)$, $s = deg(f)$, *and* $t = r + s - deg(f+g)$.

2.8 COROLLARY. *Up to powers of* X_{n+1}, *factoring a form* $F \in R[X_1, ..., X_{n+1}]$ *is the same as factoring* $F_* \in R[X_1, ..., X_n]$. *In particular, if* $F \in k[X, Y]$ *is a form, where k is algebraically closed, then* F *factors into pa product of linear factors.*

EXAMPLE. Let $F \in \mathbb{C}[X, Y]$, then $F_* \in \mathbb{C}[X]$ factors into linears factors $(X - a_i)$, and it follows that $\prod (X - a_i Y) = F \in \mathbb{C}[X, Y]$.

2.7 *Ideals with a Finite Number of Zeros*

The proposition of this section will be used to relate local questions (in terms of the local rings $\mathcal{O}_P(V)$) with global ones (in terms of coordinate rings).

2.9 PROPOSITION. *Let* I *be an ideal in* $k[X_1, ..., X_n]$, *k is algebraically closed, and suppose* $V(I) = \{P_1, ..., P_N\}$ *is finite. Let* $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$. *Then there is a natural isomorphism of* $k[X_1, ..., X_n]/I$ *with* $\prod_{i=1}^N \mathcal{O}_i / I\mathcal{O}_i$.

The proof is omitted.

2.10 COROLLARY. $dim_k(k[X_1, ..., X_n]/I) = \sum_{i=1}^N dim_k(\mathcal{O}_i / I\mathcal{O}_i)$

2.11 COROLLARY. *If* $V(I) = \{P\}$, *then* $k[X_1, ..., X_n]/I$ *is isomorphic to* $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)$.

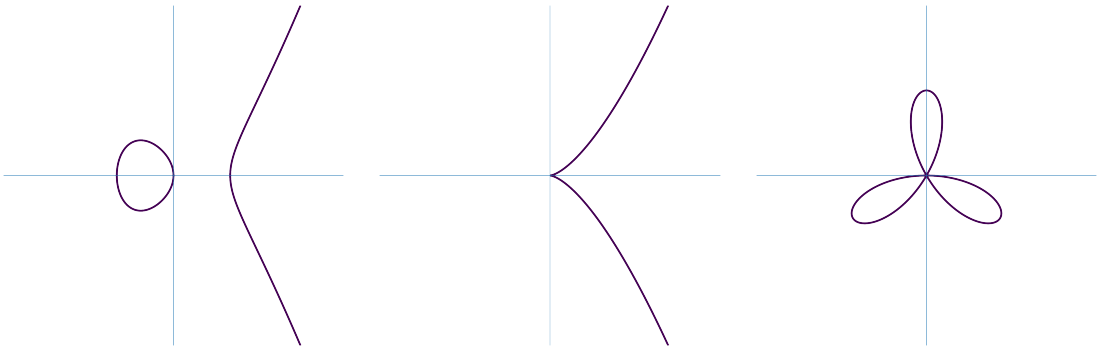
3 LOCAL PROPERTIES OF PLANE CURVES

3.1 *Multiple Points and Tangent Lines*

When considering an affine plane curve, for some purposes it is useful to allow F to have multiple factors.

If $F = \prod F_i^{e_i}$, where F_i are irreducible factors, we call e_i the **multiplicity** of the **component** F_i. F_i is said to be **simple** if $e_i = 1$, and **multiple** otherwise. The components can be recovered by V(F), but the multiplicities cannot.

A point P on the curve F is called a **simple point** of F if either derivative $F_X(P) = \frac{\partial F(P)}{\partial X}$ or $F_Y(P) = \frac{\partial F(P)}{\partial Y}$ is not 0. In this case the tagent line to F at P is $F_X(P)(X-a)+F_Y(P)(X-b) = 0$. A point that isn't simple is called **multiple** or **singular**. A curve with only simple points is called a **nonsingular curve**.



A: $y^2 - x^3 + x = 0$ **B:** $y^2 - x^3 = 0$ **C:** $(x^2 + y^2)^2 + 3x^2y - y^3 = 0$

Figure 1: Some algebraic curves in $\mathbb{R}^2$

Let F be any curve, P = (0, 0), wirte $F = F_m + F_{m+1} + ... + F_n$, where $F_i \neq 0$ is a form of degree i. We call m the **multiplicity** of F at P, and call P a simple, double, triple, ... point if $m = 1, 2, 3...$. For other $P = (a, b)$, just replace F(X, Y) by F'(X', Y'), where $X' = X - a$, $Y' = Y - b$.

Since F_m is a form in two variables, by Corollary 2.8, F_m can be decomposed into linear factors $F_m = \prod L_i^{r_i}$, where $L_i = \alpha X + \beta Y$ are tangent lines to F at P.

r_i is the **multiplicity** of the tangent, L_i is called simple, double, ... if $r_1 = 1, 2, ...$.

If F has m distince tangents at P (i.e. all tangents are simple), then P is said to be a **ordinary multiple point** of F. An ordinary double point is called a **node**.

In figure 1, a calculation of derivatives shows that A is nonsingular, and B,C are singular, where (0, 0) is the only singular point on B,C. Notice that the lowerst order form in A,B,C has degree 1, 2, 3 respectively. (0,0) is an ordinary multiple point of C with 3 distinct tangent, but is not an ordinary multiple point of B.

If $F = \prod F_i^{e_i}$, then $m_P(F) = \sum e_i m_P(F_i)$; and if L is a tangent line to F_i with multiplicity r_i, for $i = 1, 2, ...$, then L is tangent to F with multiplicity $\sum e_i r_i$.

3.2 *Multiplicities and Local Rings*

Let $F \in k[X_1, ..., X_n]$ be irreducible. We can find the multiplicity of P on F in terms of the local ring $\mathcal{O}_P(F)$. In this section we denote the residue class of $G \in k[X_1, ..., X_n]$ in $\Gamma(F) = k[X_1, ..., X_n]/(F)$ by $\bar{G}$.

3.1 THEOREM. P *is a simple point of* F *iff* $\mathcal{O}_P(F)$ *is a discrete valuation ring. In this case, if* L *is any line through* P *that is not tangent to* F *at* P*, then* $\bar{L} \in \mathcal{O}_P(F)$ *is a uniformizing parameter.*

Proof. By making a affine change of coordinates, we may assume WLOG that $L = X$, Y is the tangent line, and $P = (0,0) \in F$. Then it suffices to show that $\mathfrak{m}_P(F)$ is generated by $\bar{X}$.

Note that regardless of the multiplicity, $\mathfrak{m}_P(F) = (\bar{X}, \bar{Y})$.

By above assumption, $F = Y + (\text{terms of order } \geq 2)$, and can write $F = YG + X^2H$, where $G = 1 + (\text{terms of order } \geq 1)$. Oberserve that $G(0,0) = 1$, so $\bar{G} \in \Gamma(F) \subseteq \mathcal{O}_P(F)$ is a unit in $\mathcal{O}_P(F)$. By abuse of notation, let $\bar{G}^{-1}$ be the inverse, then $\bar{Y}\bar{G} = \bar{X^2}\bar{H}$, so $\bar{Y} = X^2\bar{H}\bar{G}^{-1}$ in $\mathcal{O}_P(F)$, thus $m_P(F) = (\bar{X}, \bar{Y}) = (\bar{X})$.

Now suppose $\mathcal{O}_P(F)$ is DVR, define a valuation function ord_P on $\mathcal{O}_P(F)$. Suppose L is a line through P, if L is tengent to F at P, then $\mathrm{ord}_P(L) > 1$ (recall that $\mathrm{ord}_P(0) = \infty$), and $\mathrm{ord}_P(L) = 1$ if L is tengent to F at P, for since L passing P, L is nonunit in $\mathcal{O}_P(F)$, and by the same argument on the previous part, L is a uniformizing parameter, hence $\mathrm{ord}_P(L) = 1$. The rest of the proof follows from the next therem. □

3.2 THEOREM. *Let* P *be a point on an irreducible curve* F*, then for all sufficiently large n:*

$$m_P(F) = dim_k(\mathfrak{m}_P(F)^n / \mathfrak{m}_P(F)^{n+1})$$

So the multiplicity of F *at* P *depends only on the local ring* $\mathcal{O}_P(F)$.

Proof. Write $\mathcal{O} = \mathcal{O}_P(V)$, $\mathfrak{m} = \mathfrak{m}_P(V)$ for convenience.

From the exact sequence of $k[X,Y]$–mods:

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \mathcal{O}/\mathfrak{m}^{n+1} \to \mathcal{O}/\mathfrak{m}^n \to 0$$

It follows that it is enough to show $\dim_k(\mathcal{O}/\mathfrak{m}^n) = n \cdot m_P(F) + s$ for some constant s and all $n \geq m_P(F)$. WLOG may assume $P = (0,0)$, so $\mathfrak{m} = (X,Y)\mathcal{O}$.

By the following fact:

Fact:

$$S^{-1}R/S^{-1}I \cong S^{-1}(R/I),$$

where $S^{-1}R$ is the localization of R at S, S is a multiplicative subset, $I \cap S = \varnothing$.

We have:

$$\mathcal{O}/\mathfrak{m}^n \cong S^{-1}\Gamma(V)/S^{-1}(X,Y)^n \cong S^{-1}(k[X,Y]/(F,(X,Y)^n))$$

For $k[X,Y]/(F,(X,Y)^n)$ is already local at the point $(0,0)$, $S^{-1}(k[X,Y]/(F,(X,Y)^n)) \cong k[X,Y]/(F,(X,Y)^n)$, so the problem is reduced to calculating the dimension of $k[X,Y]/(F,(X,Y)^n)$. Since the multiplicity $m = m_P(F)$ is the smallest degree of monomial terms, it follows that

$F(X,Y)^{n-m} \subseteq I^n$, so we have a k-linear map:

$$\begin{array}{rccc} \psi\colon & k[X,Y]/(X,Y)^{n-m} & \longrightarrow & k[X,Y]/(X,Y)^n \\ & \bar{G} & \longmapsto & \overline{FG} \end{array}$$

Now consider the short exact sequence:

$$0 \to k[X,Y]/(X,Y)^{n-m} \xrightarrow{\psi} k[X,Y]/(X,Y)^n \xrightarrow{\pi} k[X,Y]/(F,(X,Y)^n) \to 0$$

Since the k–dimension of $k[X,Y]/(X,Y)^n$ is $\sum_{k=1}^{n-1} k = \frac{n(n-1)}{2}$, it follows the k–dimension of $k[X,Y]/(F,(X,Y)^n)$ is:

$$\frac{n(n-1)}{2} - \frac{(n-m)(n-m-1)}{2} = nm - \frac{m(m-1)}{2}$$

for all $n \geq m$. □

Note that if $\mathcal{O}_P(F)$ is DVR, then Theorem 3.2 implies that $m_P(F) = 1$, this complete the proof of Theorem 3.1.

3.3 *Intersection Numbers*

We want to define for plane curves F, G and point $P \in \mathbb{A}^2$ the intersection number $\mathrm{int}_P(F,G)$. We shall first list several properties we want this intersection number to have before given the definition.

We say F, G intersect **properly** at P if F, G have no common component that passes through P, i.e. there is no irreducible $H \in k[X,Y]$ s.t. $P \in H$ and $H \mid F, G$.

(1) $\mathrm{int}_P(F,G)$ is a nonnegative integer if F, G intersect properly at P. $\mathrm{int}_P(F,G) = \infty$ if F, G intersect but not properly at P (if F, G share a irr component containing P).

(2) $\mathrm{int}_P(F,G) = 0$ iff $P \notin F \cap G$. $\mathrm{int}_P(F,G)$ depends only on the components of F, G passing through P.

(3) If T is a affine change of coordinates on $\mathbb{A}^2$ and $T(Q) = P$, then $\mathrm{int}_P(F,G) = \mathrm{int}_Q(F^T, G^T)$.

(4) $\mathrm{int}_P(F,G) = \mathrm{int}_P(G,F)$.

Two curves F, G are said to intersect transversally at P if P is a simple point both on F, G and the tangent line to F, G at P are different.

(5) $\mathrm{int}_P(F,G) \geq m_P(F) m_P(G)$, with equality occurring iff F, G have no common tagent at P.

(6) If $F = \prod F_i^{r_i}$, $F = \prod G_j^{s_j}$, then $\mathrm{int}_P(F,G) = \sum_{i,j} \mathrm{int}_P(F_i, G_j)$.

The last requirement says that the intersection number should depend only on the image of G in $\Gamma(F)$.

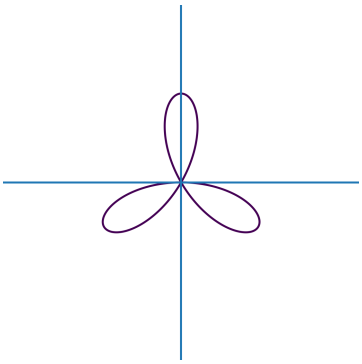
(7) $\mathrm{int}_P(F,G) = \mathrm{int}_P(F, G + AF)$ for any $A \in k[X,Y]$.

3.3 THEOREM. *There is a* ***unique*** *intersection number defined for all plane curve* F, G *and point* P *satisfying properties (1)-(7):*

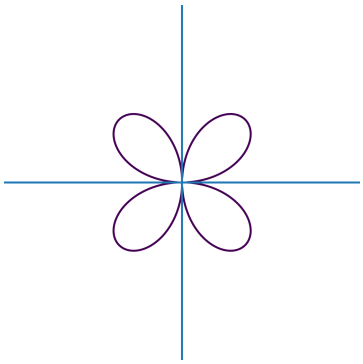
$$int_P(F, G) = dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G))$$

The proof is omited.

Property (7) is very useful for calculating intersection numbers, for example, $\text{int}_{(0,0)}(D, E)$ can be reduced to $2\text{int}_{(0,0)}(D, Y) + \text{int}_{(0,0)}(D, H)$, where $H = 5X^2 - 3Y^2 + 4Y^3 + 4X^2Y$, and D, E as belows:

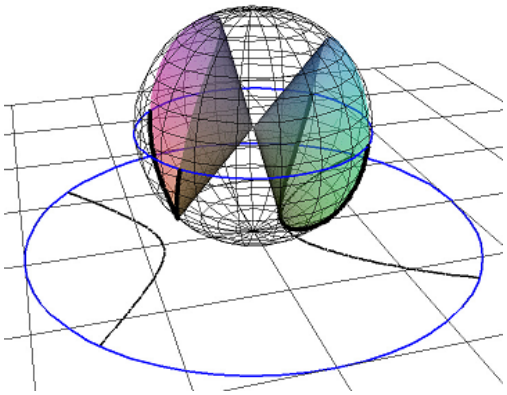


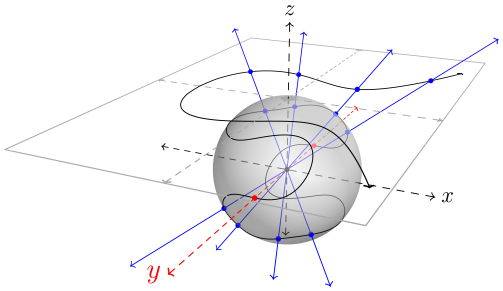
D: $(X^2 + Y^2)^2 + 3X^2Y - Y^3$



E: $(X^2 + Y^2)^3 - 4X^2Y^2$

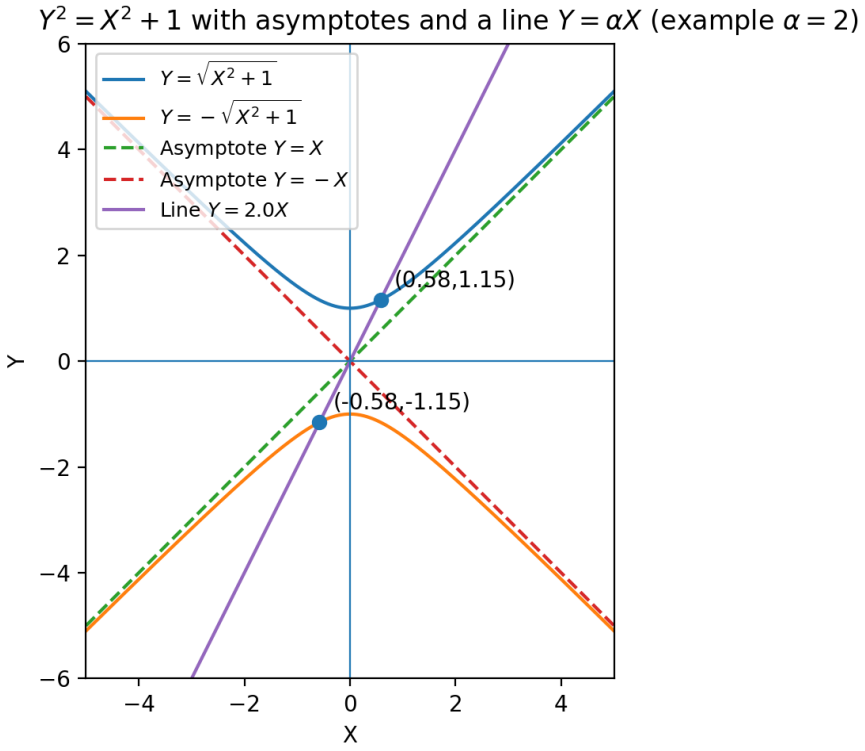
4 PROJECTIVE VARIETIES





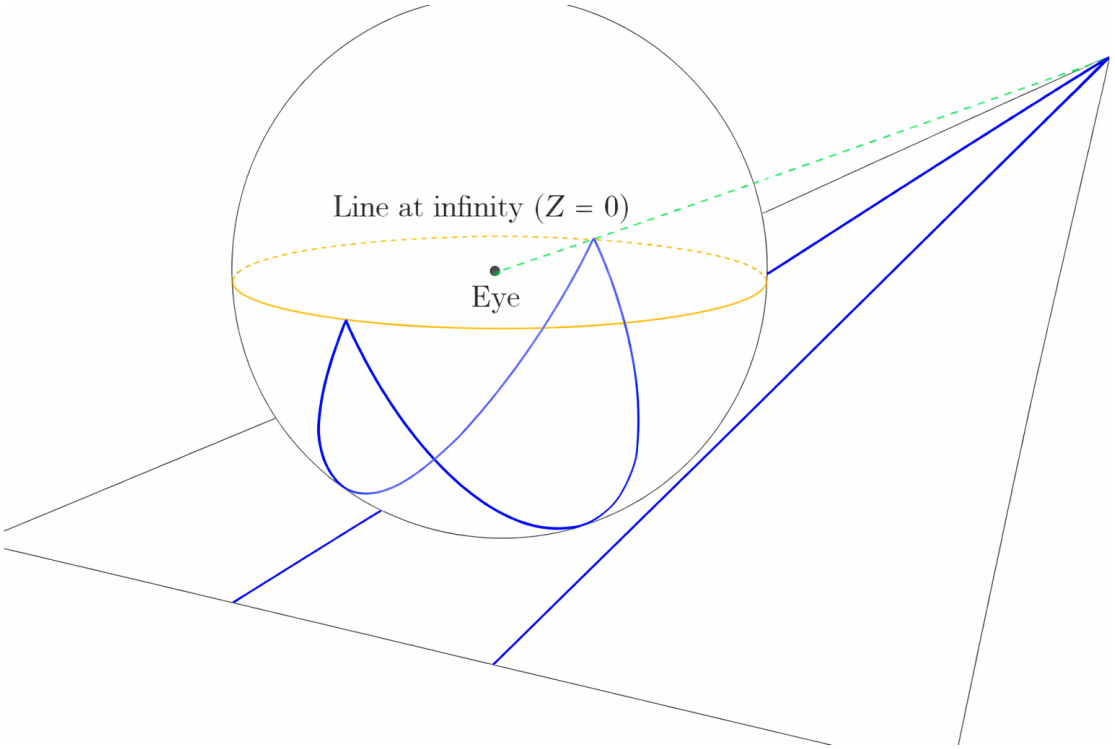
4.1 *Projective Space*

Consider two plane curve $Y^2 = X^2 + 1$ and $Y = \alpha X$, $\alpha \in k$.If $\alpha \neq \pm 1$, they intersect in two points. When $\alpha = \pm 1$, they do not intersect, but the curve is asymptotic to the line. We want to enlarge the plane in such way that two such curves intersect "at infinity".



To achieve this, we introduce the notion of **Projective n-space**:

DEFINITION (Projective n–space). Let k be any field. The **Projective n-space** over k, written $\mathbb{P}^n(\mathrm{K})$ is defined to be the set of all lines through $(0, 0, ..., 0)$ in $\mathbb{A}^{n+1}(k)$. Notice that $(a_1, ..., a_{n+1}) \neq 0$ and $(\lambda a_1, ..., \lambda a_{n+1})$ determine the same line if $\lambda \neq 0$, so an element in $\mathbb{P}^n(k)$ is a equivalence class, or equivalently, can be viewed as points on a semishpere with boundary.



Elements of $\mathbb{P}^n$ will be called points, a point P determined by $(x_1, ..., x_{n+1}) \neq 0$ is denoted by $P = [x_1, ..., x_{n+1}]$.

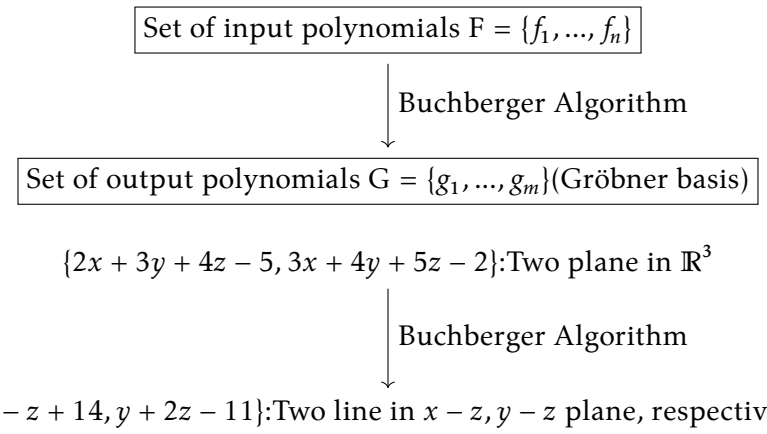
5 APPENDIX

5.1 *Gröbner basis*

For polynomials with one variable $f(x), g(X) \in k[X]$, we have polynomial division algorithm $f(X) = g(X)q(X) + r(X)$, where the degree of the remainder $r(X)$ is less than $g(X)$. But for multivariate polynomials, there's no natural ordering of polynomials. So in order to do **generalized polynomial division**, we need an **monomial ordering**, usually the lexico order $x_1 > x_2 > ...$ or some permutation $x_{\alpha_1} > x_{\alpha_2} > ....$

We also need another tool called Gröbner basis to perform generalized polynomial division, Gröbner basis is strongly related to some well-known algorithm, such as:

- Gaussian Elimination
- Euclidean Algorithm for Computing gcd
- Simplex Algorithm
- ...



Now give the definition of Gröbner basis, first fix a lexico ordering $X_1 > X_2 > ....$

5.1 DEFINITION (Initial Monomial,Ideal). Let $>$ be a monomial ordering, define the **initial monomial** $in_>(F)$ to be the leading term of the polynomial $F \in k[X_1, ..., X_n]$ i.e. the monomial in F of maximal degree.

Consider the ideal consists of every initial monomial of polynomial in I, called the **initial ideal**, denoted by $in_>(I)$. Can see $in_>(I)$ is indeed an ideal in $k[X_1, ..., X_n]$.

5.2 DEFINITION (Gröbner basis). Given polynomials $f_1, ..., f_r$ and monomial ordering $>$, a finite set of generators $\{g_1, g_2, ..., g_m\}$ of ideal $I = (f_1, ..., f_r) \in k[X_1, ..., X_n]$ is called a **Gröbner basis** of I if $in_>(I) = (in_>(g_1), ..., in_>(g_m))$.

Will show an combinatory application of Gröbner basis:

QUESTION. Minimize linear function $P + N + D + Q$, while $P, N, D, Q \in \mathbb{N} \cup \{0\}$, with constraint $P + 5N + 10D + 25Q = 117$.

Answer: Consider polynomial ring $\mathbb{Q}[C, P, N, D, Q]$, can represent a combination of coins by a monomial $C^n P^{n_P} N^{n_N} D^{n_D} Q^{n_Q}$, where $n = \sum_\alpha n_\alpha$.

Now define relations:

$$f_1 = CN - C^5P^5$$

$$f_2 = CD - C^{10}P^{10}$$

$$f_3 = CQ - C^{25}P^{25}$$

These three polynomial represent all the exchange rules of coins, which are:

$$1 \text{ nickel } = 5 \text{ pennies}$$

$$1 \text{ dime } = 10 \text{ pennies}$$

$$1 \text{ quarter } = 25 \text{ pennies}$$

The C–degree of each monomial in the relations represents the number of coins.

Now choose an ordering C > P > N > D > Q, then apply Buchberger Algorithm to these three polynomials, will get a unique **reduced Gröbner basis** consists of nine polynomials (computed by program, might be wrong):

$$g_1 : C^5P^5 - CN$$

$$g_2 : C^2N^2 - CD$$

$$g_3 : C^3ND^2 - CQ$$

$$g_4 : C^4P^5D - CN^3$$

$$g_5 : C^2D^3 - CNQ$$

$$g_6 : CN^3Q - CD^4$$

$$g_7 : C^3P^5D^2 - CN^5$$

$$g_8 : CP^5Q - CN^6$$

$$g_9 : CP^5D^4 - CN^9$$

In order to minimize total number of coins, we apply generalized polynomial division to $C^{117}P^{117}$(represents 117 coins of penny), and calculate the remainder, which is:

$$\boxed{C^8P^2NDQ^4}$$

The multi-degree $(8, 2, 1, 1, 4)$ means total of 8 coins, with 2 pennies, 1 nickel, 1 dime, and 4 quarters.

Here are some total amount of cents and its minimal number of coins represented with monomials:

Dividend	Remainder
$C^{30}P^{30}$	C^2NQ
$C^{567}P^{567}$	$C^{26}P^2NDQ^{22}$
$C^{9999}P^{9999}$	$C^{405}P^4D^2Q^{399}$
$C^{35857}P^{35857}$	$C^{1437}P^2NQ^{1434}$
$C^{8679031}P^{8679031}$	$C^{347163}PNQ^{347161}$

Note: The additional variable C for counting number of coins is crucial, one may try to work under $\mathbb{Q}[P, N, D, Q]$ and compute Gröbner basis for:

$$f_1' = N - P^5$$

$$f_2' = D - P^{10}$$

$$f_3' = Q - P^{25}$$

with ordering P > N > D > Q, this is the only reasonable choice of lexico order, since generalized polynomial division tend to make the remainder as small as possible, and the least favorite coin is penny, otherwise the remainder of, for example Q may be P^{25}, in which case the total number of coins increases. Similarly for N, D, Q. But one observes that:

$$QN \sim D^3$$

Which the degree on the left-hand-side is greater, but the right one has much number of coins.

5.3 THEOREM (Standard Monomials). *Let* $I \lhd k[X_1, ..., X_n]$, $>$: *monomial order.*

A monomial $X_1^{a_1} X_2^{a^2} ... X_n^{a_n}$ *is said to be* ***standard*** *if it is not in the initial ideal* $in_>(I)$.

EXAMPLE. n=3, $in_>(I) = (X_1^3, X_2^4, X_3^5)$, then the standard monomials are $X_1^{a_1} X_2^{a^2} X_3^{a_3}$, where $a_1 = 0, 1, 2$, $a_2 = 0, 1, 2, 3$, $a_3 = 0, 1, 2, 3, 4$, totally 60 standard monomials.

On the other hand, if $in_>(I) = (X_1^3, X_2^4, X_1 X_3^4)$, then there're infinitely many standard monomials. (Since all X_3^t are not in $in_>(I)$)

5.4 THEOREM (Fundamental Theorem of Algebra (Generalized)).

Let $I = (g_1, ..., g_m)$, $\{g_i\}$ *forms a Gröbner basis under monomial order* $>$,

then $|V(I)|$ *(counted with multiplicity) is equal to the number of standard monomial w.r.t.* I.

EXAMPLE. Consider an ideal I generated by Gröbner basis $\{x - 2yz + 2y + z, y^2 + yz + y - z - \frac{2}{3}, z^2 + z - 1\}$ in $k[x, y, z]$, the leading terms are x, y^2, z^2 respectively, so there are $1 \cdot 2 \cdot 2 = 4$ standard monomials, hence by Fundamental Theorem of Algebra, V(I) = 4.

Note that the theorem also holds for $|V(I)| = \infty$ or exists infinitely many standard monomials.

Solving a system of polynomials involves elimination of variables. We begin by eliminating all polynomials involving any variable $\in \{X_1, ..., X_{l-1}, X_l\}$.

5.5 DEFINITION (l–Elimination Ideal). Let $I \lhd k[X_1, ..., X_n]$. The l–**th elimination ideal** I_l is the ideal $\lhd k[X_{l+1}, ..., X_n]$ defined by:

$$I_l = I \cap k[X_{l+1}, ..., X_n]$$

For a fix $l \in \mathbb{N}$ s.t. $1 \leq l \leq n$, we say a monomial order $>$ on $k[X_1, ..., X_n]$ is of l–**elimination type**, if any monomial invloving any of $X_1, ..., X_{l-1}, X_l$ is greater than all other monomial in $k[X_{l+1}, ..., X_n]$.

For example, the lexico ordering is of l–elimination type.

5.6 THEOREM (Elimiation Theorem). *Let* $I \lhd k[X_1, ..., X_n]$, *and* G : *Gröbner basis of* I *w.r.t.*

a l−elimination type order. Then:

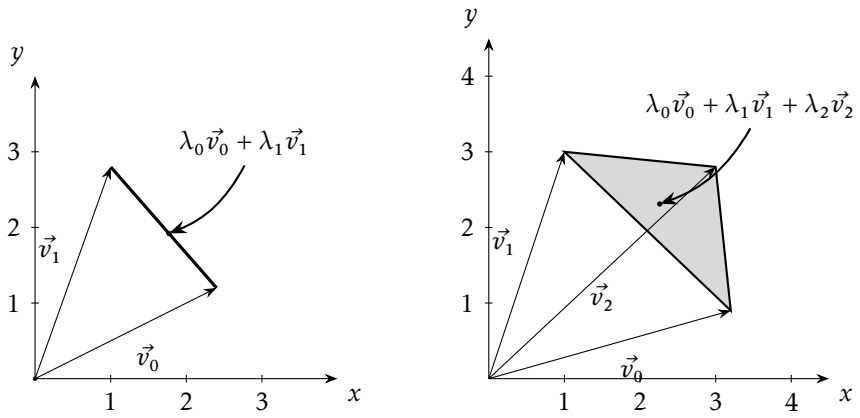
$$G_l = G \cap k[X_{l+1}, ..., X_n]$$

is a Gröbner basis of the l−elimination ideal I_l.

5.2 *Simplicies & Simplicial Complexes*

Simplices are the higher-dimensional analogues of triangles.

Convex Combination



Points in triangle are uniquely determined by $(\lambda_0, ..., \lambda_n)$, $\lambda_i \geq 0$ and $\sum_{i=0}^{n} \lambda_i = 1$. These $(\lambda_0, ..., \lambda_n)$ are called the barycentric coordinates for simplcies.

In $\mathbb{A}^n$, let $\vec{v_0}, ..., \vec{v_n}$ be points not lying on same hyperplane, then the n−simplex Δ_n, denoted by $(\vec{v_0}, \vec{v_1}, ..., \vec{v_n})$ is described by:

$$\{\lambda_0\vec{v_0} + \lambda_1\vec{v_1} + ... + \lambda_n\vec{v_n} | 0 \leq \lambda_i \leq 1, \sum \lambda_i = 1\}$$

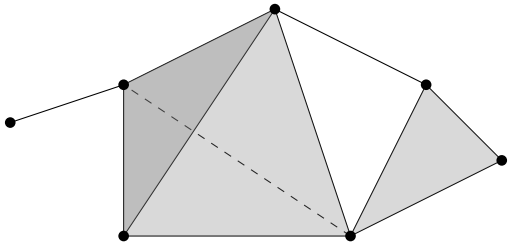
A n−**dimensional standard form** of simplex is the simplex defined by $(e_1, ..., e_{n+1})$ in $\mathbb{A}^{n+1}$, which lies in the hyperplane $x_1 + x_2 + ... + x_{n+1} = 1$.

Simplicial Complexes

Building up a space using simplicies.

Any 2 simplicies in a simplicial complex are either disjoint or meet in a common face.

A face of a simplicies $(x_1, ...x_n)$ is a simplcies whose vertices are in $x_1, ..., x_n$. For example $(x_2, x_3, x_4), (x_1, x_3, x_4), (x_1, x_2, x_4), (x_1, x_2, x_3)$ are 4 different 2-dimesional faces, $(x_i, x_j), i \neq j$ are 1-dimensional(edges) faces of (x_1, x_2, x_3, x_4).



3-simplex is the tetrahedron, 2-simplcies are all the triangles(including the faces of tetrahedron), 1-simplecies are lines, 0-simplcies are points.

ORIENTATION A simplex is oriented by choosing an ordering of its vertices; two orderings give the same orientation iff they differ by an even permutation. So for any n–dimensional simplex Δ_n, there are only two orientation.

BOUNDARY For a 1-dimensional oriented simplex $\Delta_1 = (v_0, v_1)$, define the boundary $\partial\Delta_1 = v_1 - v_0$.

For 2-dimensional $\Delta_2 = (v_0, v_1, v_2)$, define

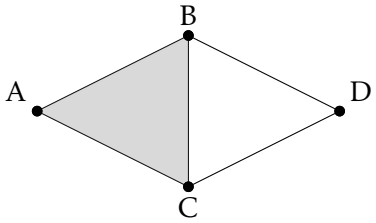
$\partial\Delta_2 = (v_0, v_1) + (v_1, v_2) + (v_2, v_0) = (v_0, v_1) - (v_0, v_2) + (v_1, v_2)$.

For general $\Delta_n = (v_0, ..., v_n)$, we define the boundary $\partial\Delta_n = \sum_{i=0}^{n}(-1)^i(v_0, ..., v_{i-1}, \hat{v_i}, v_{i+1}, ..., v_n)$,

where the hat means 'omit', for example $(v_0, \hat{v_1}, v_2) = (v_0, v_2)$.

SIMPLICIAL CHAIN Will give an example to show how is chain complex useful.

Consider the following diagram of a two triangles sharing an edge, where one trianle colored in gray means it's a 2-simplex:

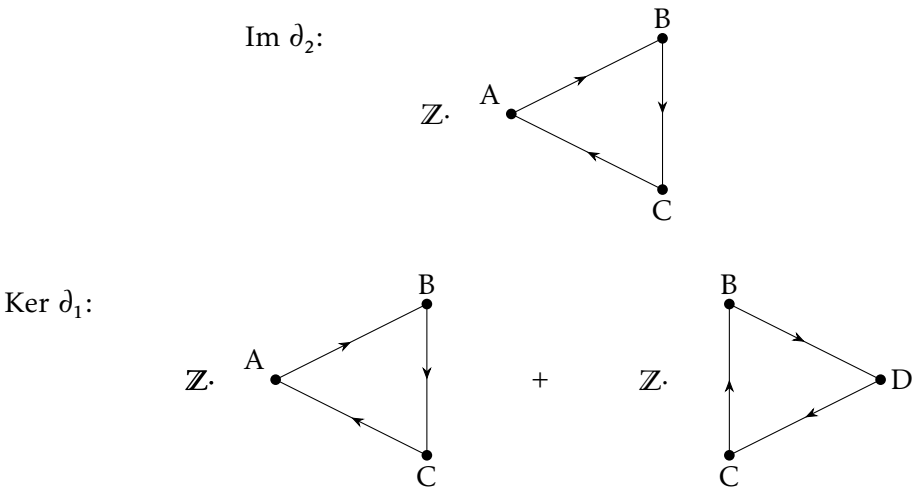


Consider chain complex:

$$\mathbb{Z}[\mathrm{F}] \xrightarrow{\partial_2} \mathbb{Z}[\mathrm{E}] \xrightarrow{\partial_1} \mathbb{Z}[\mathrm{V}]$$

Where F, E, V are sets of faces, edges, points, repectively.

Easy to see Im ∂_2 is the $\mathbb{Z}$–linear combination of (A, B) + (B, C) + (C, A), and Ker∂_1 is the $\mathbb{Z}$–linear combination of (A, B) + (B, C) + (C, A) and (B, D) + (D, C) + (C, B).



ker ∂_i is called the i–th cycle, and im ∂_{i+1} is called the $(i+1)$–th boundary. Can see in above diagram, the 2-th boundary (the boundary of triangles) is in 1-th cycle (all 'loops' consists of edges), and this make sense - since any $(i+1)$–th boundary must as well be a cycle.

So for simplicial chain complex $\mathcal{C}_\bullet$, we have:

$$\text{im } \partial_{i+i} \subseteq \ker \partial_i$$

Notices that in general the inclusion is strict, a boundary is itself a cycle, but a cycle need not be a boundary of simplicies! Consider the following example, a 2-D torus (surface of donut) consists of simplcies, We can construct a closed 1-cycle that winds around the hole of the torus, but this cycle is not a boundary of any 2-D surface on the torus!

To measure the difference between boundaries and cycles, we define the **n-th Homology** by the quotient $\mathbb{Z}$–module $\ker \partial_i / \text{im } \partial_{i+1}$.

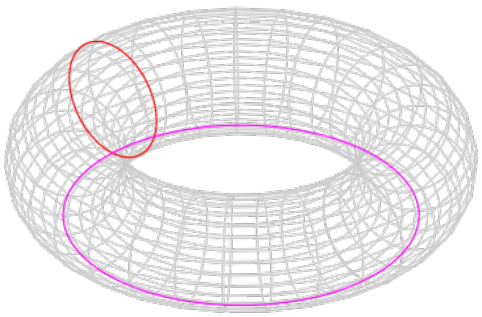


Figure 2: Torus with two closed loops which are not boundaries.