

# ALGEBRAIC CURVES

TSE-YU SU

21<sup>st</sup> November 2025

---

## CONTENTS

1	AFFINE ALGEBRAIC SETS	1
1.1	Affine Space and Algebraic Sets . . . . .	1
1.2	The Ideal of a Set of Points . . . . .	2
1.3	The Hilbert Basis Theorem . . . . .	3
1.4	Irreducible Components of an Algebraic Set . . . . .	3
1.5	Algebraic Subsets of the Plane . . . . .	3
1.6	Hilbert's Nullstellensatz . . . . .	5
2	Affine Varieties	6
2.1	Coordinate Rings . . . . .	6
2.2	Polynomial Maps . . . . .	7
2.3	Coordinate Changes . . . . .	7
3	Appendix	7
3.1	Gröbner basis . . . . .	7
3.2	Simplicies & Simplicial Complexes . . . . .	11

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

$F(P) = F(a_1, \dots, a_n) = 0$ . For  $F \neq \text{const}$ , 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  $k[X_1, \dots, X_n]$ , 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 algebraic 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  $k[X_1, \dots, X_n]$  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  $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$ . 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.
- $V(0) = \mathbb{A}^n$ ,  $V(1) = V(k[X_1, \dots, X_n]) = \emptyset$ . And  $V(X_1 - a_1, \dots, X_n - a_n) = \{(a_1, \dots, a_n)\}$ . 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  $k[X_1, \dots, X_n]$  which vanish on  $X$ , these polynomials form an ideal  $\triangleleft k[X_1, \dots, X_n]$ , called the ideal of  $X$ , written  $I(X) = \{F \in k[X_1, \dots, X_n] | F(X) = \{0\}\}$ .

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

- If  $X \subseteq Y$ , then  $I(X) \supseteq I(Y)$
- $I(\emptyset) = k[X_1, \dots, X_n]$ .  $I(\mathbb{A}^n) = 0$ .  $I(\mathbb{A}^n) = 0$  if  $k$  is not finite. A counterexample is  $0 \neq x(x-1) \in I(\mathbb{A}^1(\mathbb{Z}_2)) \triangleleft \mathbb{Z}_2[x]$
- $I(\{a_1, \dots, a_n\}) = (X_1 - a_1, \dots, X_n - a_n)$
- $S \subseteq I(V(S))$  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:

If  $I = I(X)$ , and  $F^n \in I$  for some  $n \in \mathbb{N}$ , 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  $I \triangleleft k[X_1, \dots, X_n]$  is finitely generated by  $(F_1, \dots, F_s)$ , then  $V(I) = V(F_1) \cap V(F_2) \cap \dots \cap V(F_n)$ .

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

### 1.4 Irreducible Components of an Algebraic Set

An algebraic set may be the union of several 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  $k[X_1, \dots, X_n]$  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  $V_1, \dots, V_m$  such that  $V = V_1 \cup V_2 \cup \dots \cup V_m$  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  $V = V_1 \supseteq V_2$ , where  $V_1 \neq V$ . But then  $V_1 \subsetneq V$ , so  $V_1$  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  $V = W_1 \cup \dots \cup W_s$ . Since  $V_i = V \cap V_i = \bigcup_j (W_j \cap V_i)$ , 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.  $\square$

These  $V_1, \dots, V_n$  are called the irreducible components of  $V$ , and  $V = V_1 \cup \dots \cup V_n$  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. AFFINE 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.  $\square$

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.  $\square$

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 infinite, 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  $F = F_1^{n_1} \dots F_r^{n_r}$  be the decomposition of  $F$  into irreducible factors. Then  $V(F) = V(F_1) \cup \dots \cup V(F_r)$  is the decomposition of  $F$  into irreducible components, and  $I(V(F)) = (F_1 F_2 \dots F_r)$ .

*Proof.*  $V(F) = V(F_1) \cup \dots \cup V(F_r)$  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  $I(V(F)) = (F_1 F_2 \dots F_r)$  is also clear.  $\square$

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

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 suffices to show any finite set of points  $\{(a_1, b_1), \dots, (a_r, b_r)\}$  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  $\mathbb{A}^2(\mathbb{R})$ ,  $F = \prod_{i=1}^r ((X - a_i)^2 + (Y - b_i)^2)$  is the desired polynomial.  $\square$

### 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  $k[X_1, \dots, X_n]$ , 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  $k[X_1, \dots, X_n]$  are of the form  $(X_1 - a_1, \dots, X_n - a_n)$ .

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

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

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

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,  $X_1X_{n+1}^3 + X_2^3X_{n+1}^5 \xrightarrow{\times Y^5} X_1Y^2 + X_2^3 = P(\{X_i | i = 1, \dots, n\}, Y)$ )

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

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  $F = F_1^{n_1} \dots F_r^{n_r}$  be the decomposition of  $F$  into irreducible factors, then  $V(F) = V(F_1) \cup \dots \cup V(F_r)$  is the decomposition of  $V(F)$  into irreducible components, and  $I(V(F)) = (F_1 F_2 \dots F_r)$ .

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

Radical ideals  $\leftrightarrow$  Algebraic sets

Prime ideals  $\leftrightarrow$  Irreducible algebraic sets

Irreducible polynomials  $\leftrightarrow$  Irreducible hypersurfaces

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

*Proof.* Assume  $k[X_1, \dots, X_n]/I$  is a finite dimensional vector space over  $k$ , let points  $P_1, \dots, P_r \in V(I)$ , choose polynomials  $F_i \in k[X_1, \dots, X_n], i = 1, \dots, r$  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  $\sum_{i=1}^r \lambda_i F_i \in I$ , so  $\lambda_j = \sum_{i=1}^r \lambda_i F_i(P_j) = 0$ , hence  $\bar{F}_i$  are linearly independent over  $k$ , so  $r \leq \dim_k(k[X_1, \dots, X_n]/I)$ .

Conversely, if  $V(I) = \{P_1, \dots, P_r\}$  is finite, let  $P_i = (a_{i,1}, \dots, a_{i,n})$ , and for  $j = 1, \dots, n$  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  $1, \bar{X}_j^1, \bar{X}_j^2, \dots, \bar{X}_j^{rN-1}$ , and hence so is any positive order  $\bar{X}_j^s$ . Therefore  $\{\bar{X}_1^{m_1} \cdot \bar{X}_2^{m_2} \cdot \dots \cdot \bar{X}_n^{m_n}\}$  generates  $k[X_1, \dots, X_n]/I$  as a vector space over  $k$ .  $\square$

## 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  $k[X_1, \dots, X_n]/I(V)$  is a domain. We denote  $\Gamma(V) = k[X_1, \dots, X_n]/I(V)$  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  $F \in k[X_1, \dots, X_n]$  s.t.  $F(a_1, \dots, a_n) = f(a_1, \dots, a_n)$  for all  $(a_1, \dots, a_n) \in V$ . 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  $\varphi : V \rightarrow W$  is called a **polynomial map** if there are polynomials  $T_1, \dots, T_m \in k[X_1, \dots, X_n]$  s.t.  $\varphi(a_1, \dots, a_n) = (T_1(a_1, \dots, a_n), \dots, T_m(a_1, \dots, a_n))$  for all  $(a_1, \dots, a_n)$ .

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

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

If  $\varphi$  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  $\varphi$  maps  $V$  to  $W$ ,  $g \circ \varphi$  vanished on  $V$ , and the result follows.

If  $V = \mathbb{A}^n, W = \mathbb{A}^m$ , and  $T_1, \dots, T_m$  determine a polynomial map  $T : \mathbb{A}^n \rightarrow \mathbb{A}^m$ , then  $T_i$  are unique determined by  $T$ , i.e. there are no other distinct  $T'_1, \dots, T'_m$  which 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  $\varphi : V \rightarrow W$  and the homomorphisms  $\tilde{\varphi} : \Gamma(W) \rightarrow \Gamma(V)$ . Any such  $\varphi$  is the restriction of a polynomial map from  $\mathbb{A}^n$  to  $\mathbb{A}^m$ .*

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

A polynomial map  $\varphi : V \rightarrow W$  is an isomorphism if there is  $\psi : W \rightarrow V$  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  $k$ .

## 2.3 Coordinate Changes

### 3 APPENDIX

#### 3.1 Gröbner basis

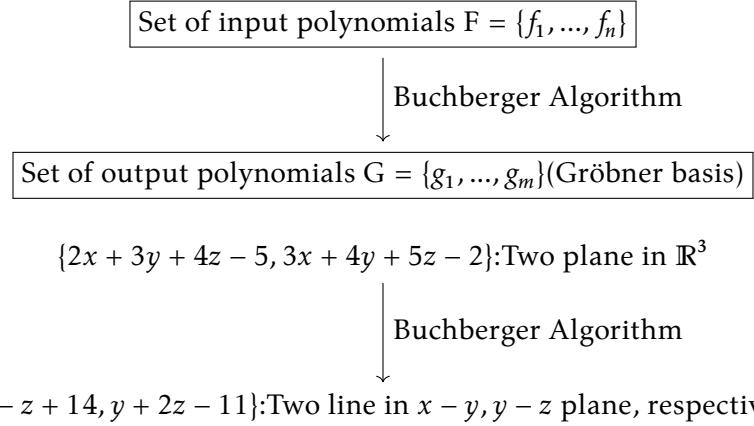
For polynomials with one variable  $f(x), g(X) \in k[X]$ , we have polynomial division algorithm  $f(X) = g(X)q(X) + r(X)$ , where the degree of the remainder  $r(X)$  is less than  $g(X)$ . But for multivariate polynomials, there's no natural ordering of polynomials. So in order to do **generalized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

### 3. APPENDIX

---

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  $X_1 > X_2 > \dots$

**3.1 DEFINITION (Initial Monomial,Ideal).** Let  $>$  be a monomial ordering, define the **initial monomial**  $in_{>}(F)$  to be the leading term of the polynomial  $F \in k[X_1, \dots, X_n]$  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  $k[X_1, \dots, X_n]$ .

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

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:

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

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

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

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

### 3. APPENDIX

---

**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.

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

A monomial  $X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$  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  $in_{>}(I)$ )

**3.4 THEOREM (Fundamental Theorem of Algebra (Generalized)).**

Let  $I = (g_1, \dots, g_m)$ ,  $\{g_i\}$  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  $\in \{X_1, \dots, X_{l-1}, X_l\}$ .

**3.5 DEFINITION ( $l$ -Elimination Ideal).** Let  $I \triangleleft k[X_1, \dots, X_n]$ . The  **$l$ -th elimination ideal**

$I_l$  is the ideal  $\triangleleft k[X_{l+1}, \dots, X_n]$  defined by:

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

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

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

**3.6 THEOREM (Elimination Theorem).** *Let  $I \triangleleft k[X_1, \dots, X_n]$ , and  $G$  : Gröbner basis of  $I$  w.r.t. a  $l$ -elimination type order. Then:*

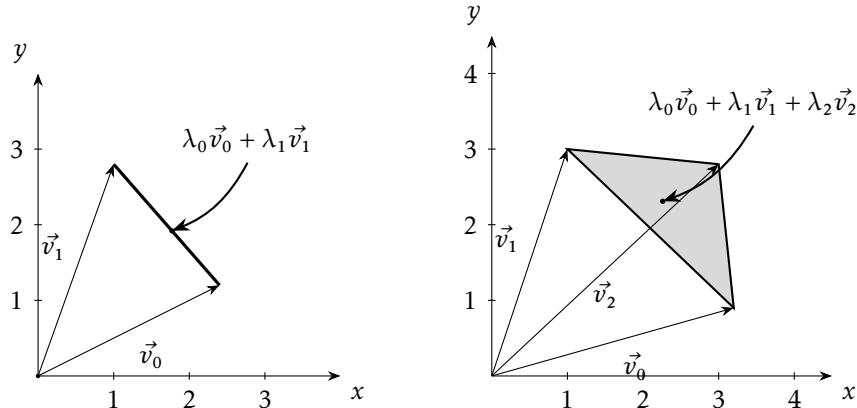
$$G_l = G \cap k[X_{l+1}, \dots, X_n]$$

is a Gröbner basis of the  $l$ -elimination ideal  $I_l$ .

### 3.2 Simplicies & Simplicial Complexes

**Simplices** are the higher-dimensional analogues of triangles.

#### CONVEX COMBINATION



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

In  $\mathbb{A}^n$ , let  $\vec{v}_0, \dots, \vec{v}_n$  be points not lying on same hyperplane, then the  $n$ -simplex  $\Delta_n$ , denoted by  $(\vec{v}_0, \vec{v}_1, \dots, \vec{v}_n)$  is described by:

$$\{\lambda_0 \vec{v}_0 + \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n \mid 0 \leq \lambda_i \leq 1, \sum \lambda_i = 1\}$$

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

#### SIMPLICIAL COMPLEXES

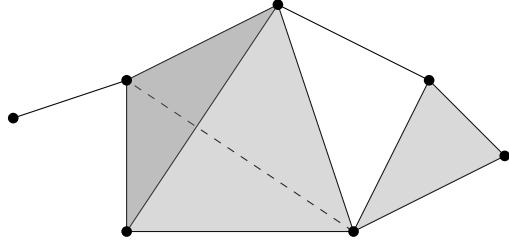
### 3. APPENDIX

---

Building up a space using simplices.

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

A face of a simplices  $(x_1, \dots, x_n)$  is a simplices whose vertices are in  $x_1, \dots, x_n$ . 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-dimensional 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-simplices are all the triangles(including the faces of tetrahedron), 1-simplices are lines, 0-simplices 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  $\Delta_n$ , there are only two orientation.

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

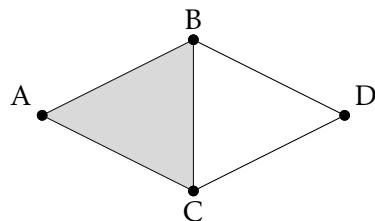
For 2-dimensional  $\Delta_2 = (v_0, v_1, v_2)$ , define

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

For general  $\Delta_n = (v_0, \dots, v_n)$ , we define the boundary  $\partial\Delta_n = \sum_{i=0}^n (-1)^i (v_0, \dots, v_{i-1}, \hat{v}_i, v_{i+1}, \dots, v_n)$ , 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 triangle colored in gray means it's a 2-simplex:

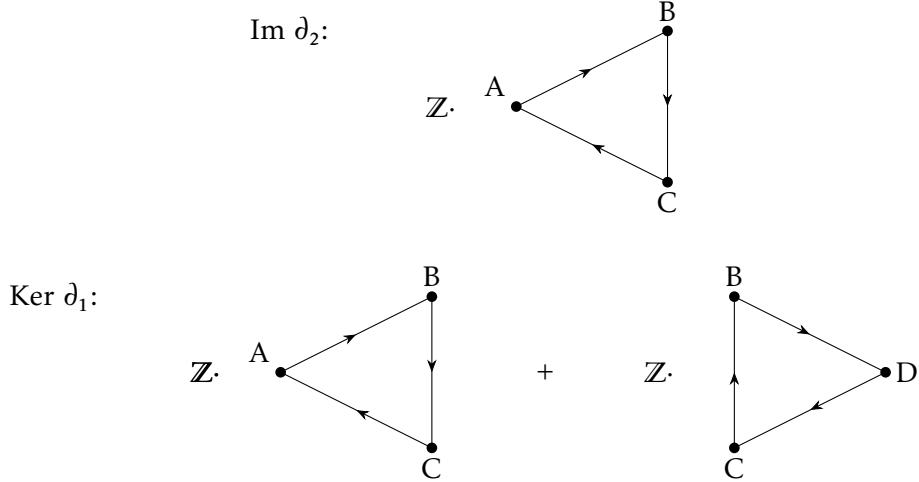


Consider chain complex:

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

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

Easy to see  $\text{Im } \partial_2$  is the  $\mathbb{Z}$ -linear combination of  $(A, B) + (B, C) + (C, A)$ , and  $\text{Ker } \partial_1$  is the  $\mathbb{Z}$ -linear combination of  $(A, B) + (B, C) + (C, A)$  and  $(B, D) + (D, C) + (C, B)$ .



$\ker \partial_i$  is called the  $i$ -th cycle, and  $\text{im } \partial_{i+1}$  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:

$$\text{im } \partial_{i+1} \subseteq \ker \partial_i$$

Notices that in general the inclusion is strict, a boundary is itself a cycle, but a cycle need not be a boundary of simplices! Consider the following example, a 2-D torus (surface of donut) consists of simplices, 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  $\ker \partial_i / \text{im } \partial_{i+1}$ .

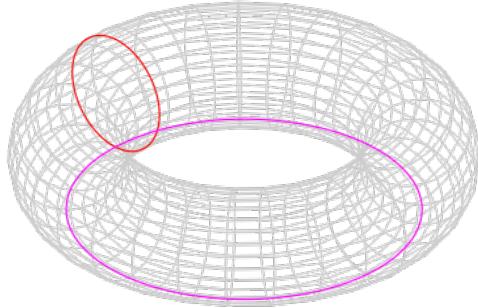


Figure 1: Torus with two closed loops.