An Introduction to Computational Algebraic Geometry

Chi Zhang

E-mail: zhangchi2018@itp.ac.cn

Abstract: These are notes I took when I previously attended the *Introduction to Computational Algebra*, by Prof. Dingkang Wang in Spring 2021. The course covers the definition and computation of Groebner bases, Hilbert's Nullstellensatz, and dimensional theory in affine algebraic geometry. All errors in the notes are mine.

Contents

1 Hilbert's Nullstellensatz

1.0.1 Weierstrass Form

Definition 1.1. Let $f \in K[X]$ and $\deg_{x_1}(f) = m > 0$. We say that f has **Weierstrass form** in x_1, if the coefficient of x_1^m in f is constant. More precisely, the expansion of f has the form

$$f = \lambda x_1^m + a_{m-1}x_1^{m-1} + \cdots + a_0, \tag{1.1}$$

where $\lambda \in K$ and $a_i \in K[x_2, \ldots, x_n]$ for all $0 \leq i \leq m-1$.

Proposition 1.1. Let $f \in K[X]$ be a non-constant polynomial. Then there exists a Weierstrass transformation $\omega : K[X] \to K[X]$ such that $\omega(f)$ has Weierstrass form in x_1.

1.0.2 Projections and Extensions

For any $1 \leq j < n$, we first introduce the projections

$$\begin{aligned} \mathrm{pr}_j : \overline{K}^n &\to \overline{K}^{n-j}, \\ (c_1, \ldots, c_n) &\mapsto (c_{j+1}, \ldots, c_n) \end{aligned}$$

on $\overline{K}^n$. For any algebraic variety $V \subset \overline{K}^n$, we say the image $\mathrm{pr}_j(V)$ to be the j**th projection** of V.

The algebraic correspondence of projection maps pr_j in the category of ideals in $K[X]$ is **elimination ideals**. For any $\mathfrak{a} \subset K[X]$, we say that the ideal $\mathfrak{a} \cap K[x_{j+1}, \ldots, x_n]$ is the j**th elimination ideal** of $\mathfrak{a}$, denoted by $\mathfrak{a}^{(j)}$.

Let $\mathbb{V}(\mathfrak{a})$ be an affine variety. It's easy to see that $\mathrm{pr}_j(\mathbb{V}(\mathfrak{a})) \subseteq \mathbb{V}(\mathfrak{a}^{(j)})$. But they are not necessarily equal in general. In some cases[1], $\mathrm{pr}_j\mathbb{V}(\mathfrak{a})$ need not be an algebraic variety.

[1] *"In some cases" is a grammatically correct expression, but "in some case" is not.*

Example. Let $\mathfrak{a} = (x_1x_2 - 1)$ be an ideal of $K[x_1, x_2]$. So $\mathfrak{a}^{(1)} = \mathfrak{a} \cap K[x_2] = (0)$. Then $\mathbb{V}(\mathfrak{a}^{(1)}) = \mathbb{V}(0) = \overline{K}^2$. But $\mathrm{pr}_1\mathbb{V}(\mathfrak{a}) = \overline{K}\backslash\{0\}$ is not a variety in $\overline{K}^2$.

Proposition 1.2 (Extension Theorem)**.** Let $\mathfrak{a} \subseteq K[X]$ be an ideal, and let $c \in \mathbb{V}(\mathfrak{a}^{(1)}) \subseteq \overline{K}^{n-1}$ be a point. Suppose that $f \in \mathfrak{a}$ is a polynomial satisfying

$$\deg_{x_1} f > 0,$$

then $c \in \mathrm{pr}_1\mathbb{V}(\mathfrak{a})$.

1.1 The Nullstellensatz

Proposition 1.3. Let $V \subseteq \overline{K}^n$ be an affine variety, and $S \subseteq V$ a subvariety of V. Then $V = \overline{S}$ iff $\mathbb{I}(V) = \mathbb{I}(S)$.

2 Gröbner Bases

We denote M_n by the set of all mononomials of $K[X]$. For $u, v \in M_n$, if there exists $w \in M_n$ such that $u = wv$, we say that v is a **divisor** of u, denoted by $v \mid u$.

Lemma 2.1 (Dickson's Lemma)**.** Let $A \subseteq M_n$ be a non-empty subset of M_n. There exists a finite subset $B \subseteq A$, such that for all $u \in A$ there exists some $v \in B$ satisfying

$v \mid u$.

Proof. We prove the lemma by induction on n.
When $n = 1$, note that for two monic monomials u, v, $u \mid v$ iff $\deg u \leq \deg v$. Let a be the element of A of smallest degree, then let $B \coloneqq \{a\}$. We are done.
Now we assume that the lemma holds for all M_k with $1 < k < n$, we need to show that the lemma also holds for M_n. For any $w \in A$, we define the subset C_0 of A by

$$C_0 \coloneqq \{\, v \in A \mid w \text{ divides } v \,\}.$$

And for each $1 \leq i \leq n$ and each $0 \leq j \leq \deg_{x_i} w - 1$, we define the subsets $C_{i,j}$ of A by

$$C_{i,j} \coloneqq \left\{\, v \in A \;\middle|\; \deg_{x_i} v = j \,\right\}.$$

Note that the subsets $C_{i,j}x_i^{-j}$ consist of monomials in indeterminates $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ for each $1 \leq i \leq n$, where the notations are self-explanary. By the induction hypothesis, there exist finite subsets $B_{i,j} \subset C_{i,j}x_i^{-j}$ such that all elements of $C_{i,j}x_i^{-j}$ are divided by elements of $B_{i,j}$. Let

$$B \coloneqq (\bigcup_{i=1}^{n} \bigcup_{j=0}^{\deg_{x_i} w - 1} B_{i,j}x_i^j) \cup \{\, w \,\},$$

then we see that B is a finite subset of A as each $B_{i,j}x_i^j$ is finite. Also note that every element in the set

$$(\bigcup_{i=1}^{n} \bigcup_{j=0}^{\deg_{x_i} w - 1} C_{i,j}) \cup C_0$$

is divided by some element in B. Now if we can prove that

$$A = (\bigcup_{i=1}^{n} \bigcup_{j=0}^{\deg_{x_i} w - 1} C_{i,j}) \cup C_0, \tag{2.1}$$

we are done. The $\supseteq$ direction is trivial, since C_0 and $C_{i,j}$ are all subsets of A. Now we show the $\subseteq$ direction. Take any $v \in A$, then either $w \mid v$ or $w \nmid v$. If the former holds, $v \in C_0$. If the latter holds, $v \notin C_0$, then there exists $1 \leq i' \leq n$ such that $\deg_{x_{i'}}(v) < \deg_{x_{i'}} w$. Let $j \coloneqq \deg_{x_{i'}} v$, then $v \in C_{i',j}$. So (2.1) holds and the proof is complete. □

Remark. Note that the relation of divisibility on M_n makes M_n a partially ordered set $(M_n, \preceq)$. Explicitly, for any $u, v \in M_n$, $u \preceq v$ iff $u \mid v$.
Now consider the set $\mathbb{N}^n$, which is $\mathbb{N}$ copied by n times. Note that there is a natural partial order $\leq$ on $\mathbb{N}^n$, $x \leq y$ iff each component of x is less than y's, for any $x, y \in \mathbb{N}^n$. Moreover, one can easily show that $(M_n, \preceq) \simeq (\mathbb{N}^n, \leq)$ as partially ordered sets.

We say the finite subset B in the above lemma to be a **Dickson basis** of A. Dickson bases are not necessarily unique. But if we put some constraints on those bases, they can be unique. A subset $S \subseteq M_n$ is said to be **reduced**, if for any two $u, v \in S$, neither $u \mid v$ nor $v \mid u$ holds, unless $u = v$.

Proposition 2.2. Let $A \subseteq M_n$ and B be a Dickson basis of A, the following[2] are equivalent:

(i) B is contained in all other Dickson bases of A;

(ii) $|B|$ is less than the cardinality of any other Dickson bases of A;

(iii) B is a reduced Dickson basis.

[2] *Note that "following" is not an adjective, but rather a pronoun. Although it lacks an "s" at the end, it should always be counted as plural when it refers to multiple types of items. So "TFAE" stands for "the following are equivalent".*

Proof. (i) $\implies$ (ii) is trivial.
(ii) $\implies$ (iii) Suppose that B is not reduced, then there are elements $u \neq v$ of B such that $u \mid v$. By definition, $B\backslash\{v\}$ is a Dickson basis of A. But $|B\backslash\{v\}| = |B| - 1$, which contradicts (ii). So B must be reduced.
(iii) $\implies$ (i) Let C be another Dickson basis of A. Then $\forall u \in B$, there $\exists v \in C$ such that $v \mid u$ since C is Dickson. But since B is also Dickson, there $\exists w \in B$ such that $w \mid v$. Given that $w \mid u$ with w, u both elements of B, we conclude $w = u$. Thus $u = v = w$, and $u \in C$, showing that $B \subseteq C$. □

If a Dickson basis B of A is reduced, we say that B is a **canonical** Dickson basis of A. Proposition 2.2 shows that canonical Dickson bases are minimal, hence are unique.

2.1 Monomial Orders on M_n

Before we start, let us recall the concept of partial order. Let S be a set, a **binary relation** (or simply a **relation**) R on S is just a subset $R \subset S \times S$.

Definition 2.1. A relation R on S is a **partial order**, if it satisfies the following conditions:

(i) for all $u \in S$, $(u, u) \in R$.

(ii) If $(u, v) \in R$ and $(v, w) \in R$, then $(u, w) \in R$.

(iii) If $(u, v) \in R$, $(v, u) \in R$, then $u = v$.

We say R is a **total order**, if for any $u, v \in S$ we have either $(u, v) \in R$ or $(v, u) \in R$.

For simplicity, we often denote a partial order R by $\succeq$ and use the notation $u \succ v$ when $(u, v) \in R$ but $u \neq v$. A partial order $\succeq$ on S is **Noetherian**, if any descending chain stabilizes. Explicitly, for any chain

$$u_1 \succeq u_2 \succeq u_3 \succeq \cdots$$

there exists an integer $m > 0$ such that $u_m = u_{m+1} = \cdots$.

Definition 2.2. A total order $\succeq$ on M_n is a **monomial order**, if

(i) for all $u \succeq v$ in M_n and any $w \in M_n$, $uw \succeq vw$; and

(ii) if $1 \neq u \in M_n$, $u \succ 1$.

In the following example we introduce some frequently used monomial orders.

Example. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, and we use the notation for $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, $x^\beta = x_1^{\beta_1}$. Conversely, it's clear that any element of M_n has the form x^α, $\alpha \in \mathbb{N}^n$. So we can identify the set M_n and the set $\mathbb{N}^n$, and the

partial orders on M_n that are compatible with addition and having a smallest element $(0, 0, \ldots, 0)$ induce monomial orders on M_n. Here are some:

(i) the **lexicographic order** $\succ_{\text{lex}}$ is defined by

$$x^\alpha \succ_{\text{lex}} x^\beta \iff \text{the rightmost non-zero entry of } \alpha - \beta \text{ is positive.}$$

(ii) The **graded lexicographic order** $\succ_{\text{grlex}}$ is defined by

$$x^\alpha \succ_{\text{grlex}} x^\beta \iff |\alpha| > |\beta|, \text{ or } x^\alpha \succ_{\text{lex}} x^\beta \text{ whence } |\alpha| = |\beta|.$$

(iii) The **graded reverse lexicographic order** $\succ_{\text{grevlex}}$ is defined by

$$x^\alpha \succ_{\text{grevlex}} x^\beta \iff |\alpha| > |\beta|, \text{ or } x^\beta \succ_{\text{lex}} x^\alpha \text{ whence } |\alpha| = |\beta|.$$

Proposition 2.3. Any monomial order on M_n is Noetherian.

Proof. Let $\succeq$ be a monomial order on M_n, and let $u_1 \succeq u_2 \succeq u_3 \succeq \cdots$ be a descending chain in M_n. By Dickson's Lemma 2.1, the set $\{ u_1, u_2, u_3, \ldots \}$ has a Dickson basis B. Let $B = \{ u_{i_1}, u_{i_2}, \ldots, u_{i_s} \}$, and $m \coloneqq \max\{ i_1, \ldots, i_s \}$. For any $j \geq m$, there exists $v_j \in B$ such that $v_j \mid u_j$. Since $\succeq$ is a monomial order, we know by Definition 2.2 that $u_j \succeq v_j$. On the other hand, we have $v_j \succeq u_m$. Thus

$$u_m \succeq u_j \succeq v_j \succeq u_m,$$

implying that $u_m = u_j$ for all $j \geq m$. □

Fixing a monomial order $\succeq$ on M_n, and let $\mathcal{S}$ be the set of all finite subsets of M_n. There is a partial order $\succeq_{\mathcal{S}}$ on $\mathcal{S}$ defined inductively by $\succeq$ on M_n. More precisely

Definition 2.3. Let $A, B \in \mathcal{S}$. We say $A \succeq_{\mathcal{S}} B$, if

(i) $B = \varnothing$; or

(ii) if neither of A, B is empty, then let $u \coloneqq \max_{\succeq} A, v \coloneqq \max_{\succeq} B$, then

  (a) $u \succ v$; or

  (b) $u = v$ and $A \backslash \{u\} \succeq_{\mathcal{S}} B \backslash \{v\}$.

Proposition 2.4. Let $\succeq$ be a monomial on M_n, then $\succeq_{\mathcal{S}}$ on $\mathcal{S}$ induced by $\succeq$ is Noetherian.

Let $f \in K[X]$ be a polynomial, we may expand f as

$$f = \sum_\alpha c_\alpha x^\alpha \tag{2.2}$$

with $c_\alpha \in K$. Fixing a monomial order $\succeq$ on M_n, we can arrange the monomials in (2.2) in an unambiguous way with respect to $\succeq$. The set $\{x^\alpha | c_\alpha \neq 0\}$ is said to be the **support** of f and often denoted by $\operatorname{supp}(f)$. We call the element $\max_{\succeq} \operatorname{supp}(f)$ the **leading monomial** of f, denoted by $\operatorname{lm}(f)$; and call the coefficient of $\operatorname{lm}(f)$ in (2.2) the **leading coefficient** of f, denoted by $\operatorname{lc}(f)$. Note that $\operatorname{lm}(f)$ is always monic and $\operatorname{lc}(f)$ is always an element of K. We should also note that both $\operatorname{lm}(f)$ and $\operatorname{lc}(f)$ depend on the choice of the partial

order $\succeq$.

2.2 Reduction

In this subsection we always fix a monomial order $\succeq$ on M_n.

Let $f, h \in K[X]$ be non-zero polynomials and $g \in K[X]$ be a polynomial not necessarily non-zero. We say that f is **reduced** to g by h, denoted by $f \to_h g$, if there exists some monomial $u \in \operatorname{supp}(f)$ such that

(i) $u = v\operatorname{lm}(h)$, where $v \in M_n$ is a monic polynomial;

(ii) $g = f - \frac{c}{\operatorname{lc}(h)} vh$, where c is the coefficient of u in the expansion of f.

Now we take a closer look. If g is the reduction of f by h, the term cu will not appear in the expansion of g, since

$$\operatorname{lt}(\frac{c}{\operatorname{lc}(h)} vh) = \frac{c}{\operatorname{lc}(h)} \operatorname{lt}(vh) = \frac{c}{\operatorname{lc}(h)} v\operatorname{lt}(h) = cv\operatorname{lm}(h) = cu.$$

So the reduction by h eliminates the term cu in f, but may introduce some smaller (with respect to the monomial order $\succeq$) terms into f, as cu is the leading term of the polynomial $c/\operatorname{lc}(h)vh$.

Lemma 2.5. Let $f, g \in K[X]$ be non-zero polynomials and $h \in K[X]$ be a polynomial. Suppose that f reduces to g by h. Then

(i) $f \succ g$[3];

(ii) f reduces to 0 in finitely many steps. Namely, we can find polynomials $f_1, \ldots, f_n \in K[X]$ with $f_n = 0$ and polynomials $h_1, \ldots, h_n \in K[X]$ such that

$$f \to_{h_1} f_1 \to_{h_2} f_2 \to_{h_3} \cdots \to_{h_n} f_n = 0.$$

[3] *What is this notation really means? $\operatorname{supp}(f) \succ_{\mathcal{S}} \operatorname{supp}(g)$?*

Proof. (i) Suppose that the term eliminated by h in the expansion of f is cu, then $u = v\operatorname{lm}h$, and by definition of the reduction,

$$f = g + \frac{c}{\operatorname{lc}h} vh. \tag{2.3}$$

Set

$$S_1 := \{\, w \in \operatorname{supp}(f) \mid w \succ u \,\}$$

and

$$S_2 := \{\, w \in \operatorname{supp}f \mid w \prec u \,\},$$

then $S_1 \cap S_2 = \varnothing$ and $\operatorname{supp}(f) = S_1 \cup S_2 \cup \{\, u \,\}$. The last identity holds because the monomial order $\succeq$ is a total order on M_n, by Definition 2.2. Since the term cu doesn't appear in the expansion of g, thus $u \notin \operatorname{supp}(g)$. By (2.3),

$$\begin{aligned} \operatorname{supp}(g) &\subseteq (\operatorname{supp}(f) \cup \operatorname{supp}(vh)) \setminus \{\, u \,\} \\ &= (\operatorname{supp}(f) \setminus \{\, u \,\}) \cup (\operatorname{supp}(vh) \setminus \{\, u \,\}) \\ &= S_1 \cup S_2 \cup (\operatorname{supp}(vh) \setminus \{\, u \,\}). \end{aligned}$$

Since u is the leading monomial of vh, the monomials in the set $\operatorname{supp}(vh) \setminus \{\, u \,\}$ are all $\prec u$. Thus the set $S_2 \cup (\operatorname{supp}(vh) \setminus \{\, u \,\})$ contains monomials that are strictly $\prec u$, whilst the set S_1 consists of the monomials strictly $\succ u$. Then $\max_{\succeq} \operatorname{supp}(g) \in S_1$.

But $S_1 \subseteq \operatorname{supp}(f)$, so we have $\max_{\succeq} \operatorname{supp}(f) \succeq \max_{\succeq} \operatorname{supp}(g)$.By Definition 2.3, $\operatorname{supp}(f) \succeq_{\mathcal{S}} \operatorname{supp}(g)$, we are done.
(ii) Suppose $\exists f$ that cannot be reduced to 0 in finitely many steps. Then for any $h_1, h_2, \ldots, h_n, \ldots$, the chain

$$f \to_{h_1} f_1 \to_{h_2} f_2 \to_{h_3} \cdots \to_{h_n} f_n \to_{h_{n+1}} \cdots$$

never stabilizes. By (i),

$$\operatorname{supp}(f) \succ \operatorname{supp}(f_1) \succ \operatorname{supp}(f_2) \succ \cdots$$

is a strictly descending chain in $\mathcal{S}$, which contradicts to Proposition 2.4. □

We have just described how a polynomial f reduces to a polynomial g by a single polynomial h. Now we do a little bit of generalization. Let $H \subset K[X]$ be a non-empty subset, we say that f is **reduced** to g by H, denoted by $f \to_H g$, if we can find finitely many $h_1, \ldots, h_m \in H$ such that

$$f \to_{h_1} f_1 \to_{h_2} f_2 \to_{h_3} \cdots \to_{h_m} g.$$

Definition 2.4. Let $f \in K[X]$ be a polynomial and $H \subseteq K[X]$ be a non-empty subset. We say that f is **reduced** with respect to H, if $f = 0$ or there is no such $g \in K[X]$ that is the reduction of f by H.

By definition, a non-zero polynomial f can be reduced to 0 modulo H iff $\forall u \in \operatorname{supp}(f)$, u is the multiple of some element in $\operatorname{lm}(H)$. Here $\operatorname{lm}(H) \coloneqq \{\operatorname{lm}(h) | h \in H\}$.

Lemma 2.6. A non-zero polynomial f is reduced modulo H iff

$$\operatorname{supp}(f) \cap (\operatorname{lm}(H))_{M_n} = \varnothing.$$

Proof. Let $0 \neq f$ be a polynomial reduced with respect to H. Thus □

If f reduces to 0 by a subset $H \subseteq K[X]$, then $f \in (H)$.

Conversely, suppose that $\mathfrak{a} \subseteq K[X]$ is an ideal generated by $H = \{ h_1, \ldots, h_m \}$, which is always true since $K[X]$ is Noetherian. Given an arbitrary polynomial $f \in K[X]$, can we determine whether f is an element of $\mathfrak{a}$ using reduction by H? If we don't put any other constraint on $H = \{ f_1, \ldots, f_m \}$, reduction by H is hardly a good criterion for the ideal membership problem. As the following example shows, if we do different reductions on f, *exempli gratia*,

$$f \to_{h_1} f_1 \to_{h_2} \cdots \to_{h_m} f_m$$

and

$$f \to_{h_m} \tilde{f}_1 \to_{h_{m-1}} \cdots \to_{h_1} \tilde{f}_m,$$

we may get f_m different from $\tilde{f}_m$, whilst f_m and $\tilde{f}_m$ are both reduced with respect to H.

Example. Let $f = xyz, h_1 = xy + y$ and $h_2 = xz$, then let $H \coloneqq \{ h_1, h_2 \}$. Under the lexicographic order $x \succ y \succ z$, both 0 and yz are reduced with respect to H. Indeed, as $\operatorname{lm}(H) = \{ xy, xz \}$, $\operatorname{supp}(yz) \cap (\operatorname{lm}(H))_{M_n} = \{ yz \} \cap (\{ xy, xz \})_{M_n} = \varnothing$. Thus by Lemma 2.6, yz is reduced with respect to 0.
It's easy to verify that

$$f \to_{h_2} = 0, \tag{2.4}$$

as $f - yh_2 = 0$, and

$$f \to_{h_1} (-yz), \tag{2.5}$$

as $f - zh_1 = -yz$. The reduction (2.4) tells us that $f \in (H)$, whilst the reduction (2.5) tells us that $f \notin (H)$

However, as we'll see in the next section, if we pick H to be the Gröbner basis of the ideal $\mathfrak{a}$, $f \in \mathfrak{a}$ iff $f \to_H 0$.

2.3 Gröbner Bases

In this subsection, we fix a monomial order $\succeq$ on M_n.

Definition 2.5. Let $\mathfrak{a} \subseteq K[X]$ be a proper ideal. We say a finite subset $G \subseteq \mathfrak{a}$ is a **Gröbner basis** of $\mathfrak{a}$, if $\mathrm{lm}(G)$ is a Dickson basis of $\mathrm{lm}(\mathfrak{a})$.

There is another equivalent description of a Gröbner basis of a proper ideal $\mathfrak{a}$. $G \subseteq \mathfrak{a}$ is a Gröbner basis of $\mathfrak{a}$ iff $(\mathrm{lt}(G)) = (\mathrm{lt}\mathfrak{a})$.

By Dickson's Lemma 2.1, the Gröbner basis of an ideal always exists.

Theorem 2.7. Let $\mathfrak{a} \subset K[X]$ be a proper ideal and G be a Gröbner basis of $\mathfrak{a}$. Then

(i) for any $f \in \mathfrak{a}$, f is reduced modulo G iff $f = 0$;

(ii) if $f \to_G f_1, f \to_G f_2$ and f_1, f_2 are reduced modulo G, then $f_1 = f_2$.

Proof. (i) By Lemma 2.6, f is reduced modulo G iff

$$\mathrm{supp}(f) \cap (\mathrm{lm}(G))_{M_n} = \varnothing,$$

iff

$$\mathrm{supp}(f) \cap (\mathrm{lm}(\mathfrak{a}))_{M_n} = \varnothing,$$

by Definition 2.5. But as $f \in \mathfrak{a}$, at least $\mathrm{lm}(f) \in \mathrm{lm}(\mathfrak{a})$, as well as $\mathrm{lm}(f) \in \mathrm{supp}(f)$ trivially. So $\mathrm{supp}(f) \cap (\mathrm{lm}(\mathfrak{a}))_{M_n}$ must not be empty, unless $f = 0$.
(ii) Since $f \to_G f_1$, $(f - f_1) \to_G 0$, which implies $f - f_1 \in (G) \subseteq \mathfrak{a}$ ("=" *de facto*, as we shall see in the next corollary). Similarly $f - f_2 \in \mathfrak{a}$, thus $f_1 - f_2 \in \mathfrak{a}$. Observe that

$$\begin{aligned}\mathrm{supp}(f_1 - f_2) \cap (\mathrm{lm}(G))_{M_n} &\subseteq (\mathrm{supp}(f_1) \cup \mathrm{supp}(f_2)) \cap (\mathrm{lm}(G))_{M_n} \\ &= \mathrm{supp}(f_1) \cap (\mathrm{lm}(G))_{M_n} \cup \mathrm{supp}(f_2) \cap (\mathrm{lm}(G))_{M_n} \\ &= \varnothing,\end{aligned}$$

implying that $f_1 - f_2$ is reduced modulo G by Lemma 2.6. Then $f_1 - f_2 = 0$ by (i). □

Corollary 2.8. Let G be a Gröbner basis of a proper ideal $\mathfrak{a}$ and $f \in \mathfrak{a}$ be a polynomial. $f \in \mathfrak{a}$ iff $f \to_G 0$. Furthermore, $\mathfrak{a} = (G)$.

Proof.

□

Let G be a Gröbner basis of I. If for all $g_i \in G$, g_i is reduced with respect to $G \backslash \{g_i\}$, we say that G is **reduced**. If G is a reduced Gröbner basis and $\mathrm{lm}(G) = \{1\}$, we say that G is **canonical**.

Proposition 2.9. Given an ideal $I \subseteq K[X]$, the canonical Gröbner basis G of I exists uniquely.

2.4 Buchberger's Algorithm

For any monomial $u, v \in M_n$, we use the notation $\mathrm{lcm}(u, v)$ for their least common multiple.

Definition 2.6. Let $f, g \in K[X]$, and $u, v \in M_n$ be the monic monomials satisfying

$$u\mathrm{lm}(f) = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = v\mathrm{lm}(g).$$

We say that the polynomial

$$S(f, g) \coloneqq \mathrm{lc}(g)uf - \mathrm{lc}(f)vg$$

is the S**-polynomial** of f and g.

Our more tediously,

$$\begin{aligned} S(f, g) &\coloneqq \mathrm{lc}(g)uf - \mathrm{lc}(f)vg \\ &= \mathrm{lc}(g)\frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}f} f - \mathrm{lc}(f)\frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}g} g \end{aligned}$$

Theorem 2.10 (Buchberger's Criterion)**.** Let $G \subset K[X]$ be a non-empty finite set. Then G is a Gröbner basis of the ideal (G) iff for any $f, g \in G$,

$$S(f, g) \to_G 0.$$

Proof.

Lemma 2.11. Let $H \subseteq K[X] \setminus \{0\}$ be a non-empty finite subset of $K[X]$, and $0 \neq f \in K[X]$. If $f \to_H 0$, then there are $h_1, \ldots, h_m \in H$ and $q_1, \ldots, q_m \in K[X] \setminus \{0\}$ such that

(i) $f = q_1h_1 + q_2h_2 + \cdots + q_mh_m$, with $\mathrm{lm}(f) \succ \mathrm{lm}q_ih_i$ for all $1 \leq i \leq m$; and

(ii) there exists $1 \leq j \leq m$, such that $\mathrm{lm}(f) = \mathrm{lm}q_jh_j$.

Proof.

□

Lemma 2.12. Let $f, g \in K[X]$ be non-zero polynomials and $u, v \in M_n$. Then there exists $w \in M_n$, such that

$$S(uf, vg) = wS(f, g).$$

Proof. A useful observation is

$$\operatorname{lcm}(\operatorname{lm} f, \operatorname{lm} g) \mid \operatorname{lcm}(\operatorname{lm}(uf), \operatorname{lm}(vg).$$

Denote by $t \coloneqq \operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$, and let

$$\operatorname{lcm}(\operatorname{lm}(uf), \operatorname{lm}(vg)) = wt.$$

Thus

$$\begin{aligned} S(uf, vg) &= \operatorname{lc}(vg)\frac{wt}{\operatorname{lm}(uf)}uf - \operatorname{lc}(uf)\frac{wt}{\operatorname{lm}(vg)}vg \\ &= \operatorname{lc}(g)\frac{wt}{\operatorname{lm}(f)}f - \operatorname{lc}(f)\frac{wt}{\operatorname{lm}(g)}g \\ &= w(\operatorname{lc} g\frac{t}{\operatorname{lm}(f)}f - \operatorname{lc}(g)\frac{t}{\operatorname{lm}(g)}g) \\ &= w(\operatorname{lc}(g)\frac{\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))}{\operatorname{lm}(f)}f - \operatorname{lc}(f)\frac{\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))}{\operatorname{lm}(g)}g) \\ &= wS(f, g). \end{aligned}$$

□

Lemma 2.13. Let $f, h_1, \ldots, h_m \in K[X]$ be non-zero polynomials, and assume that $f = c_1h_1 + \cdots + c_mh_m$ with $c_i \in K$, $1 \leq i \leq m$. Furthermore we assume that

$$\operatorname{lm}(h_1) = \operatorname{lm}(h_2) = \cdots = \operatorname{lm}(h_m) \succ \operatorname{lm}(f),$$

then

$$f = \sum_{1 \leq i < j \leq m} c_{i,j} S(h_i, h_j)$$

for some $c_{i,j} \in K$. In particular, if $S(h_i, h_j) \neq 0$, then $\operatorname{lm}(h_i) \succ \operatorname{lm}(S(h_i, h_j))$.

□

Proposition 2.14. Let $f, g \in K[X]$ be polynomials satisfying $\gcd(\operatorname{lm}(f), \operatorname{lm}(g)) = 1$. Then $S(f, g) \to_{\{f,g\}} 0$, namely, the set $\{f, g\}$ is a Gröbner basis of the ideal (f, g).

2.5 Applications of Gröbner Bases

Let $\mathfrak{a} \subseteq K[X]$ be an ideal. We can determine the K-linear basis of the K-linear space $K[X]/\mathfrak{a}$ via Gröbner bases of the ideal $\mathfrak{a}$. Assume that $G_\mathfrak{a}$ is the (canonical) Gröbner bases of $\mathfrak{a}$, then we define

$$B \coloneqq \{\, \bar{u} \mid u \in M_n \text{ and is reduced with respect to } G_\mathfrak{a} \,\}. \tag{2.6}$$

We claim that

Proposition 2.15. The set B defined by (2.6) is a K-linear basis for the K-linear space $K[X]/\mathfrak{a}$.

Proof. Given any $f \in K[X]$, we can always reduce f to g modulo $G_\mathfrak{a}$, such that g is reduced modulo $G_\mathfrak{a}$. By Corollary (2.8), this holds iff $f - g \in \mathfrak{a}$, or equivalently, $\bar{f} = \bar{g}$ in the quotient ring $K[X]/\mathfrak{a}$. Since g is reduced with respect to $G_\mathfrak{a}$, its image

$\bar{g}$ can be written as a K-linear combination of the elements in B, this shows that B spans $K[X]/\mathfrak{a}$.
Now we show the K-linear independence of B. Suppose there are $c_1, \ldots, c_s \in K$ and $\overline{u_1}, \ldots, \overline{u_s} \in B$, such that

$$c_1\overline{u_1} + \cdots + c_s\overline{u_s} = 0$$

in $K[X]/\mathfrak{a}$, or equivalently

$$c_1u_1 + \cdots + c_su_s \in \mathfrak{a}.$$

Since each $u_j, 1 \leq j \leq s$ is reduced modulo $G_\mathfrak{a}$, we have

$$\mathrm{supp}u_j \cap (\mathrm{lm}(G_\mathfrak{a})_{M_n} = \{\, u_j \,\} \cap (\mathrm{lm}(\mathfrak{a}))_{M_n} = \varnothing,$$

by Lemma 2.6. Thus

$$\mathrm{supp}(c_1u_1 + \cdots + c_su_s) \cap (\mathrm{lm}(G_\mathfrak{a})) = \{\, u_1, \ldots, u_s \,\} \cap (\mathrm{lm}(\mathfrak{a}))_{M_n} = \varnothing,$$

which means that the linear combination $c_1u_1 + \cdots + c_su_s$ is also reduced modulo $G_\mathfrak{a}$. So again by Corollary 2.8, we know that

$$c_1u_1 + \cdots + c_su_s = 0.$$

Since $u_1, \ldots, u_s$ are distinct monic monomials, there must be $c_1 = c_2 = \cdots c_s = 0$. Thus we have shown that B spans $K[X]/\mathfrak{a}$ and is K-linear independent. This completes the proof. □

Theorem 2.16 (Elimination Theorem). Let $\mathfrak{a} \subseteq K[X]$ be a proper ideal, and G a Gröbner basis of $\mathfrak{a}$ under the lexicographic order $x_1 \succ x_2 \succ \cdots \succ x_n$. Then $G \cap K[x_{j+1}, x_{j+2}, \ldots, x_n]$ is a Gröbner basis of $\mathfrak{a}^{(j)}$.

Proof. We denote by $G^{(j)} \coloneqq G \cap K[x_{j+1}, x_{j+2}, \ldots, x_n]$. It's obvious that $G^{(j)}$ is a finite subset of $\mathfrak{a}^{(j)}$. If we can show that for all $f \in \mathfrak{a}^{(j)}$, there is some $g \in G^{(j)}$ such that $\mathrm{lm}(g) \mid \mathrm{lm}(f)$, then by Definition 2.5, $G^{(j)}$ is a Gröbner basis of $\mathfrak{a}^{(j)}$. Indeed, since $f \in K[x_{j+1}, \ldots, x_n] \subset K[X]$, there is some $g \in G$ such that $\mathrm{lm}(g) \mid \mathrm{lm}(f)$, thus $\mathrm{lm}(f) \succ \mathrm{lm}(g)$ since the lexicographic order is a monomial order. However, as $\mathrm{lm}(g) \in K[x_{j+1}, \ldots, x_n]$ is the greatest element of $\mathrm{supp}(g)$, the other elements of $\mathrm{supp}(g)$ cannot contain indeterminates more than $x_{j+1}, \ldots, x_n$. This dictates that $g \in K[x_{j+1}, \ldots, x_n]$, or $g \in G \cap K[x_{j+1}, \ldots, x_n] = G^{(l)}$, as desired. □

Claim 2.17. Let $\mathfrak{a} = (f_1, \ldots, f_l)$ and $\mathfrak{b} = (g_1, \ldots, g_m)$ be two ideals. What are the generators of the ideal $\mathfrak{a} \cap \mathfrak{b}$? Let $\mathfrak{c}$ be the ideal generated by

$$\{\, f_it \mid 1 \leq i \leq l \,\} \cup \{\, (1-t)g_i \mid 1 \leq i \leq m \,\}$$

in the ring $K[X, t]$. Then we claim that $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{c} \cap K[X]$.

Let $\mathfrak{a}, \mathfrak{b}$ be two ideals. The **saturation** of $\mathfrak{a}$ with respect to $\mathfrak{b}$ is defined by

$$\{\, g \in K[X] \mid \forall f \in \mathfrak{b}, gf^m \in \mathfrak{a}, \exists m > 0 \,\},$$

and is often denoted by $\mathfrak{a} : \mathfrak{b}^\infty$. In particular, when $\mathfrak{b} = (f)$ is principal for some $f \in K[X]$, the saturation $\mathfrak{a} : \mathfrak{b}$ is often denoted by $\mathfrak{a} : f^\infty$ for short. Let $\mathfrak{a} = (f_1, \ldots, f_m)$, and let $\mathfrak{c}$ be

the ideal in $K[X,t]$ generated by $\{ f_1, \ldots, f_m, tf-1 \}$. We claim that

$$\mathfrak{a} : f^\infty = \mathfrak{c} \cap K[X].$$

3 Correspondence between Varieties and Ideals

By the powerful Nullstellensatz, we already know that there is a one-to-one correspondence between affine varieties in K^n and radical ideals of $K[X]$. In this section, we will discuss the variety-ideal correspondence in more details.

3.1 Preliminaries

Let $U, V \subseteq \bar{K}^n$ be two algebraic varieties. We say that U is a **subvariety** of V, if $U \subset V$; say that U is a **proper subvariety** of V if $U \subsetneq V$. We say that V is **irreducible**, if V is not a union of its two proper subvarieties.

Lemma 3.1. An affine variety V is irreducible iff for any $f, g \in K[X]$, $fg|_V = 0$ implies either $f|_V = 0$ or $g|_V = 0$.

Proof. $\Longleftarrow$ We want to show that V is irreducible. Let $V = U_1 \cup U_2$ with U_1, U_2 two subvarieties , and suppose that $V \neq U_1$. We must show that $V = U_2$. Since $U_1 \subsetneq V$, by the Nullstellensatz we have $\mathbb{I}(U_1) \supsetneq \mathbb{I}(V)$. So we can choose $g \in \mathbb{I}(U_1)$ but $g \notin \mathbb{I}(V)$. For any $f \in \mathbb{I}(U_2)$, we have $fg|_V = 0$, as $fg|_{U_1} = fg|_{U_2} = 0$ and $V = U_1 \cup U_2$. Since $g|_V \neq$, there must be $f|_V = 0$, by assumption.
$\Longrightarrow$ Let $f, g \in K[X]$ be two polynomials satisfying $fg|_V = 0$. So $V \subseteq \mathbb{V}(fg) = \mathbb{V}(f) \cup \mathbb{V}(g)$. Thus $V = V \cap (\mathbb{V}(f) \cup \mathbb{V}(g)) = (V \cap \mathbb{V}(f)) \cup (V \cap \mathbb{V}(g))$. By assumption, V is irreducible, so either $V = V \cap \mathbb{V}(f)$ or $V = V \cap \mathbb{V}(g)$, or equivalently either $V \subseteq \mathbb{V}(f)$ or $V \subseteq \mathbb{V}(g)$. This shows that either $f|_V = 0$ or $g|_V = 0$ holds, as desired. □

An ideal $I \subseteq K[X]$ is a **prime ideal**, if for any $f, g \in K[X]$, $fg \in I$ implies $f \in I$ or $g \in I$.

Lemma 3.2. An ideal $\mathfrak{a} \subseteq K[X]$ is a prime ideal iff $K[X]/\mathfrak{a}$ is an integral domain.

Proof. C. f. any textbook of undergraduate algebra. □

Corollary 3.3. An affine variety V is irreducible iff $\mathbb{I}(V)$ is a prime ideal.

Proof. This is a direct corollary of the Lemma 3.1. □

Lemma 3.4. An ideal $\mathfrak{m} \subseteq K[X]$ is maximal iff $K[X]/\mathfrak{m}$ is a field.

Proof. C. f. any textbook of undergraduate algebra. □

Let E/K be a field extension, and let $\alpha \in E$ be algebraic over K. Then α satisfies a non-trivial polynomial equation in $K[x]$, with x an indeterminate. Now consider the set of polynomials $f \in K[x]$ such that $f(\alpha) = 0$. It's easy to see that furthermore the set is an ideal. Indeed, it is the kernel of the map

$$\begin{aligned} \phi : K[x] &\to E, \\ x &\mapsto \alpha. \end{aligned}$$

Since $K[x]$ is a PID, there is some $f \in K[x]$ such that $(f) = \ker \phi$. If we assume that p is monic, without loss of generality, then f is uniquely determined.

Definition 3.1. The polynomial f above is called the **minimal polynomial** of α over K.

Corollary 3.5. If an ideal $\mathfrak{m} \subseteq K[X]$ is maximal, then $K[X]/\mathfrak{m}$ is a finite extension over K.

Proof. Obviously, $K[X]/\mathfrak{m}$ is a field. If we can show that $\overline{x_i}$ for all $1 \leq i \leq n$ are algebraic over K, then we can prove the lemma, by Lemma 09GH[4], where the $\overline{x_i}$ are the image of x_i in $K[X]/\mathfrak{m}$. Thus we must find f_i such that $f_i(\overline{x_i}) = 0 \iff f_i(x_i) \in \mathfrak{m}$, where $f_i \in K[y]$ are polynomials of one indeterminate. This holds iff $K[x_i] \cap \mathfrak{m} \neq (0)$ for all $1 \leq i \leq n$.
Now consider $\mathbb{V}(\mathfrak{m})$, and we know that $\mathbb{V}(\mathfrak{m}) \neq \varnothing$ since $\mathfrak{m} \neq K[X]$. Let $c = (c_1, \ldots, c_n) \in \mathbb{V}(\mathfrak{m}) \subseteq \overline{K}^n$. Since $\overline{K}$ is the algebraic closure of K, all c_i are algebraic over K for $1 \leq i \leq n$. So their minimal polynomial exists, and let them be $f_1, \ldots, f_n$, with $f_i(x_i) \in K[x_i]$. We may view each $f_i(x_i)$ a polynomial in $K[X]$ via the natural inclusion $K[x_i] \hookrightarrow K[X]$. Thus $c \in \mathbb{V}(\mathfrak{m} + (f_i(x_i))$. Then $\mathfrak{m} + (f_i(x_i)) \neq K[X]$, by the weak Nullstellensatz. On the other hand, $\mathfrak{m} \subseteq \mathfrak{m} + (f_i(x_i))$, which implies that $f_i(x_i) \in \mathfrak{m}$, by the maximality of $\mathfrak{m}$. This shows that $f_i(x_i) \in \mathfrak{m} \cap K[x_i]$ for all $1 \leq i \leq n$, hence $\mathfrak{m} \cap K[x_i] \neq (0)$, as desired. □

[4] *Prove the lemma later. To do.*

Lemma 3.6. Let $x \in \bar{K}^n$ be a point and $\mathfrak{m} \subset K[X]$ be a maximal ideal, then

(i) $\mathbb{I}(x)$ is a maximal ideal of $K[X]$; and

(ii) for all $y \in \mathbb{V}(\mathfrak{m})$, $\mathfrak{m} = \mathbb{I}(y)$.

Proof. (i) Let $\mathfrak{b} \subseteq K[X]$ be an ideal such that $\mathbb{I}(x) \subsetneq \mathfrak{b}$. Let $f \in \mathfrak{b} \backslash \mathbb{I}(x)$, then $f(x) \neq 0$. Let $p(t)$ be the minimal polynomial of $f(x) \in \overline{K}$ over K. Since p is minimal, it is irreducible in $K[t]$, by Definition 3.1. We claim that $p(0) \neq 0 \in K$. Indeed, if $p(0) = 0$ were true, then $t \mid p(t)$, which is a contradiction.
On the other hand, since $p(f(x)) = p(f)(x) = 0$, we know that $p(f) \in \mathbb{I}(x)$. Thus we have $p(f) - f \in \mathfrak{b}$[5]
(ii) Take any $y \in \mathbb{V}(\mathfrak{m})$. For any $f \in \mathfrak{m}$, $f(y) = 0$, hence $f \in \mathbb{I}(y)$. This shows that $\mathfrak{m} \subseteq \mathbb{I}(y)$. By assumption $\mathfrak{m}$ is maximal, we have $\mathfrak{m} = \mathbb{I}(y)$. □

[5] *There is a gap. To do.*

Corollary 3.7. Let $\mathfrak{a} \subseteq K[X]$ be a proper radical ideal of $K[X]$.Then

$$\mathfrak{a} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m}, \mathfrak{m} \text{ maximal}} \mathfrak{m}$$

with $\mathfrak{m}$ running over maximal ideals containing $\mathfrak{a}$.

Proof. $\subseteq$ is trivial.
$\supseteq$ Let $f \in \bigcap_{\mathfrak{a} \subseteq \mathfrak{m}, \mathfrak{m} \text{ maximal}} \mathfrak{m}$, we must show that $f \in \mathfrak{a}$. To see this, let $x \in \mathbb{I}(\mathfrak{a})$ be an arbitrary point. By Lemma 3.6, $\mathbb{I}(x)$ is maximal and contains $\mathfrak{a}$, so $f \in \mathbb{I}(x)$, hence $f(x) = 0$. Since x is arbitrary, f vanishes on the whole $\mathbb{V}(\mathfrak{a})$, or equivalently, $f \in \mathbb{I}(\mathbb{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{a}$. Where the last equality follows from the assumption that $\mathfrak{a}$ is radical. □

3.2 Decomposition of Affine Varieties

Proposition 3.8. (i) Every affine variety can be written as a union of finitely many irreducible affine varieties.

(ii) Every radical ideal can be written as an intersection of finitely many prime ideals.

Proof. (i) Let V be an affine variety. If V is irreducible, then we are done. Otherwise there is a decomposition $V = V_1 \cup U_1$, where $V_1 \subsetneq V$ and $U_1 \subsetneq V$ are proper subvarieties of V. If V_1, U_1 are both irreducible, we are done. Otherwise, we can decompose V_1, U_1 in a similar manner. If the decomposition doesn't finish in finitely many steps, we must get a strictly descending chain of affine varieties

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots$$

that doesn't stabilize. Then by the Nullstellensatz there is a non-stabilizing strictly ascending chain

$$\mathbb{I}(V) \subsetneq \mathbb{I}(V_1) \subsetneq \mathbb{I}(V_2) \subsetneq \cdots,$$

which is a contradiction to the fact that $K[X]$ is Noetherian.
(ii) Let $\mathfrak{a} \subseteq K[X]$ be a radical ideal. By (i), there are irreducible affine varieties $V_1, \ldots, V_m$ such that $\mathbb{V}(\mathfrak{a}) = V_1 \cup V_2 \cup \cdots \cup V_m$. Since $\mathfrak{a}$ is radical, by the Nullstellensatz we have

$$\mathfrak{a} = \sqrt{\mathfrak{a}} = \mathbb{I}(\mathbb{V}(\mathfrak{a})) = \mathbb{I}(V_1) \cap \mathbb{I}(V_2) \cap \cdots \cap \mathbb{I}(V_m).$$

By Corollary 3.3, each $\mathbb{I}(V_i)$ is a prime ideal. □

The irreducible decomposition of an affine variety need not be unique. The following lemma, however, ensures that the minimal irreducible decomposition is unique, up to reindexing the subscripts.

Lemma 3.9. (i) Let $V, U_1, \ldots, U_m$ be algebraic varieties in $\bar{K}^n$, with V irreducible. If $V \subseteq \cup_{i=1}^m U_i$, then $V \subseteq U_j$ for some $1 \leq j \leq m$.

(ii) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ be ideals of $K[X]$ and $\mathfrak{p} \subseteq K[X]$ be a prime ideal. If $\bigcap_{i=1}^m \mathfrak{a}_i \subseteq \mathfrak{p}$, then $\mathfrak{a}_j \subseteq \mathfrak{p}$ for some $1 \leq j \leq m$.

Proof. We only prove (ii), as (i) can be implied by (ii) with the help of the Nullstellensatz.
We use *reductio ad absurdum*. Now assume that for all $1 \leq i \leq m$, the relations $\mathfrak{a}_i \not\subseteq \mathfrak{p}$ all hold. This means that for all $1 \leq i \leq m$, there exist polynomials $f_i \in \mathfrak{a}_i$ but $f_i \notin \mathfrak{p}$. On the other hand, $f_1 f_2 \cdots f_m \in \bigcap_{i=1}^m \mathfrak{a}_i \subseteq \mathfrak{p}$. But this implies that there exists some $1 \leq j \leq m$ such that $f_j \in \mathfrak{p}$, as $\mathfrak{p}$ is prime by assumption. So we reach a contradiction. □

Let $V_1, \ldots, V_m$ be irreducible algebraic varieties in $\bar{K}^n$ and $V \subseteq \bar{K}^n$ be an algebraic variety. If $V = U_1 \cup \cdots \cup U_m$ and each U_i is irreducible, we say that $U_1, \ldots, U_m$ are **irreducible components** of V. We say the irreducible decomposition $V = U_1 \cup \cdots \cup U_m$ is **minimal**, if $V_i \not\subseteq V_j$ for each $1 \leq i \leq m$ and $i \neq j$. Similarly, for a radical ideal $\mathfrak{a}$, we can also define its prime decomposition and its minimal prime decomposition. By Lemma 3.9, we have

Corollary 3.10. (i) A minimal irreducible decomposition of an irreducible affine variety is essentially unique;

(ii) a minimal prime decomposition of an irreducible ideal is essentially unique.

Proof. We only prove (i), as (ii) and (i) are equivalent.
Let V be an affine variety in $\overline{K}^n$, and $V = U_1 \cup \cdots \cup U_l = V_1 \cup \cdots \cup V_m$ be two minimal irreducible decompositions of V. we may first assume that $l \leq m$, and finally show that $l = m$.
By Lemma 3.9, there exists V_{i_1} such that $U_1 \subseteq V_{i_1}$, similarly there exists U_{j_1} such that $V_{i_1} \subseteq U_{j_1}$. Thus $U_1 \subseteq V_{i_1} \subseteq U_{j_1}$. But since the decomposition $V = U_1 \cup \cdots \cup U_l$ is minimal, the only possibility is that $U_1 = V_{i_1} = U_{j_1}$. The a similar manner, we get $U_s = V_{i_s}$ for $2 \leq s \leq l$. After a reindexing, we may let $U_s = V_s$ for $1 \leq s \leq l$. Then $V = (V_1 \cup \cdots V_l) \cup V_{l+1} \cup \cdots \cup V_m = (U_1 \cup \cdots \cup U_l) \cup V_{l+1} \cup \cdots \cup V_m = V_{l+1} \cup \cdots \cup V_m$, showing that $V = V_{l+1} \cup \cdots \cup V_m$ is another irreducible decomposition of V. This contradicts the assumption that $V = V_1 \cup \cdots \cup V_m$ is a minimal decomposition of V. So $l = m$, and $U_1, \ldots, U_l$ are just $V_1, \ldots, V_m$ after their subscripts reindexed, as desired.

□

3.3 Zariski Closures and Ideal Quotients

Definition 3.2. Let $\mathfrak{a}, \mathfrak{b} \subseteq K[X]$ be ideals of $K[X]$. We define their **ideal quotient** to be

$$(\mathfrak{a} : \mathfrak{b}) \coloneqq \{f \in K[X] | f\mathfrak{b} \subseteq \mathfrak{a}\},$$

which is an ideal of $K[X]$.

We use the notation $(\mathfrak{a} : g^\infty)$ for

$$(\mathfrak{a} : g^\infty) \coloneqq \{\, f \in K[X] \mid fg^m \in \mathfrak{a}, \exists m \in \mathbb{Z}_+ \,\},$$

and the notation $(\mathfrak{a} : g)$ for

$$(\mathfrak{a} : g) \coloneqq \{\, f \in K[X] \mid fg \in \mathfrak{a} \,\}.$$

If $f \in (\mathfrak{a} : g)$, then $fg \in \mathfrak{a}$. But this implies that $hfg = fhg \in \mathfrak{a}$, or namely $f \in (\mathfrak{a} : (g))$, as (g) is principal. So $(\mathfrak{a} : g) \subset (\mathfrak{a} : (g))$. Conversely, if $f \in (\mathfrak{a} : (g))$, then $fhg \in \mathfrak{a}$ for all $h \in K[X]$, this holds in particular when $h = 1$, thus $f \in (\mathfrak{a} : g)$. We have shown that $(\mathfrak{a} : (g)) = (\mathfrak{a} : g)$ for all $g \in K[X]$, so in later use we don't distinguish those notations for simplicity. Immediately we have

$$(\mathfrak{a} : g) \subset (\mathfrak{a} : g^\infty),$$

but the above ideal quotients need not necessarily equal in general.

Proposition 3.11. Let $\mathfrak{a}, \mathfrak{b} \subset K[X]$ be ideals of $K[X]$. Then the followings hold:

(i) $\overline{\mathbb{V}(\mathfrak{a}) \backslash \mathbb{V}(\mathfrak{b})} \subseteq \mathbb{V}((\mathfrak{a} : \mathfrak{b}))$; and

(ii) if $\mathfrak{a}$ is radical, $\overline{\mathbb{V}(\mathfrak{a}) \backslash \mathbb{V}(\mathfrak{b})} = \mathbb{V}((\mathfrak{a} : \mathfrak{b}))$.

Proof. (i) Let $c \in \mathbb{V}(\mathfrak{a})\backslash\mathbb{V}(\mathfrak{b})$ be an arbitrary point, then we can find some $g \in \mathfrak{b}$ such that $g(c) \neq 0$. $\forall f \in (\mathfrak{a} : \mathfrak{b})$, $fg \in \mathfrak{a}$, thus $(fg)(c) = f(c)g(c) = 0$. The last equation shows that $f(c) = 0$, and as both c and f are arbitrary, $c \in \mathbb{V}((\mathfrak{a} : \mathfrak{b})) \implies \mathbb{V}(\mathfrak{a})\backslash\mathbb{V}(\mathfrak{b}) \subseteq \mathbb{V}((\mathfrak{a} : \mathfrak{b})) \implies \overline{\mathbb{V}(\mathfrak{a})\backslash\mathbb{V}(\mathfrak{b})} \subseteq \mathbb{V}((\mathfrak{a} : \mathfrak{b}))$.
(ii) Set $S \coloneqq \mathbb{V}(\mathfrak{a})\backslash\mathbb{V}(\mathfrak{b})$. We are asked to show that $\overline{S} = \mathbb{V}(\mathfrak{a} : \mathfrak{b})$. In (i) we have shown that $\overline{S} \subseteq \mathbb{V}(\mathfrak{a} : \mathfrak{b})$, so what left to us is to show that $\overline{S} \supseteq \mathbb{V}(\mathfrak{a} : \mathfrak{b})$. So it suffices to show that $\mathbb{I}(S) = \mathbb{I}(\overline{S}) \subseteq \mathbb{I}(\mathbb{V}(\mathfrak{a} : \mathfrak{b})) = \sqrt{(\mathfrak{a} : \mathfrak{b})}$. We claim that $\sqrt{(\mathfrak{a} : \mathfrak{b})} = (\mathfrak{a} : \mathfrak{b})$. Indeed, for any $f \in \sqrt{(\mathfrak{a} : \mathfrak{b})}$, there exists some $m > 0$ such that $f^m\mathfrak{b} \subseteq \mathfrak{a} \iff f^m g \in \mathfrak{a}, \forall g \in \mathfrak{b} \implies f^m g^m = (fg)^m \in \mathfrak{a}, \forall g \in \mathfrak{b} \iff fg \in \sqrt{\mathfrak{a}} = \mathfrak{a}, \forall g \in \mathfrak{b} \iff f \in (\mathfrak{a} : \mathfrak{b}) \implies \sqrt{(\mathfrak{a} : \mathfrak{b})} \subseteq (\mathfrak{a} : \mathfrak{b})$. Hence what we need to show is that

$$\mathbb{I}(S) \subseteq (\mathfrak{a} : \mathfrak{b}).$$

For any $f \in \mathbb{I}(S)$ and any $g \in \mathfrak{b}$, we have $fg|_{\mathbb{V}(\mathfrak{a})} = 0$, showing that $fg \in \sqrt{\mathfrak{a}} = \mathfrak{a}$. Since g is arbitrary, the last equation means that $f \in (\mathfrak{a} : \mathfrak{b})$, consequently $\mathbb{I}(S) \subseteq (\mathfrak{a} : \mathfrak{b})$. □

Lemma 3.12. Let $\mathfrak{a} \subseteq K[X]$ be an ideal, and $0 \neq g \in K[X]$. Suppose that $\mathfrak{a} \cap (g)$ is finitely generated and can be generated by $f_1, \ldots, f_m \in \mathfrak{a}$, then $(\mathfrak{a} : g)$ can be generated by

$$f_1/g, \ldots, f_m/g,$$

where the notations $f_1/g, \ldots, f_m/g$ explain themselves manifestly.

Proof. Since all $f_1, \ldots, f_m$ are elements of (g), then $g \mid f_i$ for all $1 \leq i \leq m$. The last condition means that $f_i = gq_i$ for some $q_i \in K[X]$. Obviously, $q_i \in (\mathfrak{a} : g)$. For all $f \in (\mathfrak{a} : g)$, or $fg \in \mathfrak{a}$, we have $fg \in \mathfrak{a} \cap (g)$. So there exist $a_1, \ldots, a_m \in K[X]$ such that

$$fg = \sum_{i=1}^{m} a_i f_i = \sum_{i=1}^{m} a_i q_i g.$$

Since $K[X]$ is a UFD, the above equation holds iff

$$f = \sum_{i=1}^{m} a_i q_i$$

holds, by the assumption that $g \neq 0$. So f is generated by q_i over $K[X]$. This means that $(\mathfrak{a} : g)$ is an ideal generated by

$$q_1, \ldots, q_m.$$

More intuitively, we can write $f_i/g \coloneqq q_i$, then the lemma has been proved. □

The following proposition reveals the relation between the Zariski closure $\overline{\mathbb{V}(\mathfrak{a})\backslash\mathbb{V}(g)}$ and the saturation ideal $(\mathfrak{a} : g^\infty)$.

Proposition 3.13. Let $\mathfrak{a} \subseteq K[X]$ be an ideal, and $0 \neq g \in K[X]$. Then

$$\overline{\mathbb{V}(\mathfrak{a})\backslash\mathbb{V}(g)} = \mathbb{V}((\mathfrak{a} : g^\infty)).$$

Proof. Since $\mathbb{V}(\mathfrak{a}) = \mathbb{V}(\sqrt{\mathfrak{a}})$ by the Nullstellensatz, we have

$$\overline{\mathbb{V}(\mathfrak{a})\backslash\mathbb{V}(g)} = \overline{\mathbb{V}(\sqrt{\mathfrak{a}})\backslash\mathbb{V}(g)}.$$

By Proposition 3.11 (ii),

$$\overline{\mathbb{V}(\sqrt{\mathfrak{a}})\backslash\mathbb{V}(g)} = \mathbb{V}(\sqrt{\mathfrak{a}} : g)$$

holds since $\sqrt{\mathfrak{a}}$ is radical. So

$$\overline{\mathbb{V}(\mathfrak{a})\backslash\mathbb{V}(g)} = \mathbb{V}(\sqrt{\mathfrak{a}} : g),$$

which means that it suffices to show $(\sqrt{\mathfrak{a}} : g) = \sqrt{(\mathfrak{a} : g^\infty)}$. Indeed, $\forall f \in (\sqrt{\mathfrak{a}} : g)$, we have $fg \in \sqrt{\mathfrak{a}}$, or equivalently there exists integer $s > 0$ such that $(fg)^s = f^s g^s \in \mathfrak{a}$. Thus $f^s \in (\mathfrak{a} : g^\infty) \iff f \in \sqrt{(\mathfrak{a} : g^\infty)}$. Conversely, $\forall f \in \sqrt{(\mathfrak{a} : g^\infty)}$, there exists a sufficiently large s such that $f^s g^s = (fg)^s \in \mathfrak{a} \iff fg \in \sqrt{\mathfrak{a}}$. This means that $f \in (\sqrt{\mathfrak{a}} : g)$. □

3.4 0-Dimensional Ideals

Theorem 3.14. Let $\mathfrak{a} \subset K[X]$ be an ideal. The followings are equivalent:

(i) $\mathbb{V}(\mathfrak{a})$ is a finite set in $\bar{K}^n$;

(ii) $\mathfrak{a} \cap K[x_i] \neq (0)$ for all $1 \leq i \leq n$;

(iii) if G is a Gröbner basis of $\mathfrak{a}$, then for all $1 \leq i \leq n$ there exist non-negative integers s_i such that $x_i^{s_i} \in \mathrm{lm}(G)$;

(iv) the K-vector space $K[X]/\mathfrak{a}$ is of finite dimension.

Proof. (i) $\implies$ (ii) If $\mathbb{V}(\mathfrak{a}) = \varnothing$, then by the Nullstellensatz $\mathfrak{a} = K[X]$. Since $1 \in \mathfrak{a} = K[X]$ and $1 \in K[x_i]$ for all $1 \leq i \leq n$, we have $1 \in \mathfrak{a} \cap K[x_i]$, implying that $\mathfrak{a} \cap K[x_i] \neq (0)$ for all $1 \leq i \leq n$. So we assume that $\mathbb{V}(\mathfrak{a}) = \{ c_1, \ldots, c_s \} \neq \varnothing$. More explicitly
(ii) $\implies$ (iii) Let G be a Gröbner basis for $\mathfrak{a}$. By assumption $\mathfrak{a} \cap K[x_i] \neq (0)$ for all $1 \leq i \leq n$, we can pick $0 \neq f_i \in \mathfrak{a} \cap K[x_i]$. Thus there exist $g_i \in G$ such that $\mathrm{lm}(g_i) \mid \mathrm{lm}(f_i)$ for all $1 \leq i \leq n$. Set $\mathrm{lm}(f_i) = x_i^{m_i}$ with $m_i \geq 0$, then we must have $\mathrm{lm}(g_i) = x_i^{s_i}$ for some $m_i \geq s_i \geq 0$.
(iii) $\implies$ (iv) For any $f \in K[X]$, we denote by $\overline{f}$ the image of f in $K[X]/\mathfrak{a}$. By Proposition 2.15 we know that the set

$$B \coloneqq \{ \bar{u} \mid u \in M_n \text{ reduced modulo } G \}$$

is a basis of $K[X]/\mathfrak{a}$ as a K-linear space. From (iii) we know that $x_i^{s_i} \in \mathrm{lm}(G)$, and are mutually reduced. Set $G' \coloneqq \{ x_1^{s_1}, \ldots, x_n^{s_n} \} \subseteq G$, and consider a new K-linear space

$$B' \coloneqq K[X]/(G').$$

A key observation is that $B \subseteq B'$, but if we look closer, we find that

$$B' = \left\{ x_1^{i_1} \cdots x_n^{i_n} \;\middle|\; 0 \leq i_1 \leq s_1 - 1, \ldots, 0 \leq i_n \leq s_n - 1 \right\}$$

So $|B'| = s_1 s_2 \cdots s_n$. On the other hand, $|B| \leq |B'|$, showing that $K[X]/\mathfrak{a}$ is at most of dimension $s_1 s_2 \cdots s_n$.

(iv) $\implies$ (ii) Let $d \coloneqq \dim_K(K[X]/\mathfrak{a})$. Thus the $d+1$ elements $1, \overline{x_i}, \ldots, \overline{x_i}^d$ are K-linear dependent for all $1 \leq i \leq n$, which means that there exist $c_{i,0}, c_{i,1}, \ldots, c_{i,d}$ such that

$$c_{i,0} + c_{i,1}\overline{x_i} + \cdots + c_{i,d}\overline{x_i}^d = 0,$$

or equivalently,

$$c_{i,0} + c_{i,1}x_i + \cdots + c_{i,d}x_i^d \in \mathfrak{a}.$$

Then we can take $f_i(x_i) = c_{i,0} + c_{i,1}x_i + \cdots c_{i,d}x_i^d$ for all $1 \leq i \leq n$, which all satisfy $f_i \in \mathfrak{a} \cap K[x_i]$. So $(0) \neq \mathfrak{a} \cap K[x_i]$ for all $1 \leq i \leq n$.
(ii) $\implies$ (i) Let $f_i \in \mathfrak{a} \cap K[x_i]$, we have $(f_1, \ldots, f_n) \subseteq \mathfrak{a}$, then by the strong Nullstellensatz $\mathbb{V}(f_1, \ldots, f_n) \supseteq \mathbb{V}(\mathfrak{a})$. Now we need to look closer at $\mathbb{V}(f_1, \ldots, f_n)$. We claim that

$$\mathbb{V}(f_1, \ldots, f_n) = \mathbb{V}(f_1) \times \cdots \times \mathbb{V}(f_n).$$

Indeed, if $x = (x_1, \ldots, x_n) \in K^n$ is also in $\mathbb{V}(f_1, \ldots, f_n)$, then $f_i(x_i) = 0$ for all $1 \leq i \leq n$, showing that $\mathbb{V}(f_1, \ldots, f_n) \subseteq \mathbb{V}(f_1) \times \cdots \times \mathbb{V}(f_n)$. Conversely, we take some $(x_1, \ldots, x_n) \in \mathbb{V}(f_1) \times \cdots \times \mathbb{V}(f_n)$. Since $f_i(x_i) = 0$ for all $1 \leq i \leq n$, we let $x \coloneqq (x_1, \ldots, x_n)$, satisfying $f_i(x) = 0$ for all i. So $x \in \mathbb{V}(f_1, \ldots, f_n)$, implying that $\mathbb{V}(f_1) \times \cdots \times \mathbb{V}(f_n) \subseteq \mathbb{V}(f_1, \ldots, f_n)$. By the Fundamental Theorem of Algebra, each $\mathbb{V}(f_i)$ consists of finitely many points, so is their Cartesian product. $\mathbb{V}(\mathfrak{a})$ is finite since it is a subset of the finite set $\mathbb{V}(f_1, \ldots, f_n)$. □

If an ideal $\mathfrak{a}$ fulfills any of the conditions in the above theorem, we say that $\mathfrak{a}$ is a 0-**dimensional ideal**. Later after introducing the concept of the dimension of an ideal, we will see that 0-dimensional ideals defined here are indeed ideals of 0-dimension.

Now recall that for an ideal $\mathfrak{a} \subseteq K[X]$, its jth elimination ideal $\mathfrak{a}^{(j)}$ is defined to be

$$\mathfrak{a}^{(j)} = \mathfrak{a} \cap K[x_{j+1}, \ldots, x_n], 1 \leq j < n.$$

Proposition 3.15. Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional ideal. Then

(i) the elimination ideals $\mathfrak{a}^{(j)}$ are all 0-dimensional; and

(ii) $\mathrm{pr}_j(\mathbb{V}(\mathfrak{a})) = \mathbb{V}(\mathfrak{a}^{(j)})$

for all $1 \leq j < n$.

Proof. (i) To show that $\mathfrak{a}^{(j)}$ is 0-dimensional for all $1 \leq j < n$, we must needs [6] show that $\mathfrak{a}^{(j)} \cap K[x_i] \neq (0)$ for all $1 \leq i \leq n$. If $j < i$, then

$$\mathfrak{a}^{(j)} \cap K[x_i] = (\mathfrak{a} \cap K[x_{j+1}, \ldots, x_n]) \cap K[x_i] = \mathfrak{a} \cap (K[x_{j+1}, \ldots, x_n] \cap K[x_i]) = \mathfrak{a} \cap K[x_i] \neq (0),$$

by assumption.

If $i \leq j$ [7]

[6] *It's a little bit surprising, but this expression was grammatically correct in past few centuries in English, though obsolete now. If you are interested in more about the verb "need", you must not miss this answer. By the way, it was answered by Peter Shor, one of the living gods in the field of quantum computation.*

[7] *I can't fill this gap now. To do.*

(ii) We use induction on j. When $j = 1$, there is a non-zero polynomial $f \in \mathfrak{a} \cap K[x_1]$, by the assumption that $\mathfrak{a}$ is 0-dimensional. Thus $\deg_{x_1} f > 0$. By Preposition 1.2, the identity $\mathrm{pr}_1 \mathbb{V}(\mathfrak{a}) = \mathbb{V}(\mathfrak{a}^{(1)})$ holds. Now we assume that the assertion holds for $j-1$, that is, we have

$$\mathrm{pr}_{j-1}(\mathbb{V}(\mathfrak{a})) = \mathbb{V}(\mathfrak{a}^{(j-1)}). \tag{3.1}$$

Now we define a projection map π_{j-1}:

$$\begin{aligned} \pi_j : \overline{K}^{n-j+1} &\to \overline{K}^{n-j}, \\ (c_j, \ldots, c_n) &\mapsto (c_{j+1}, \ldots, c_n). \end{aligned}$$

Immediately, $\pi_j \circ \mathrm{pr}_{j-1} = \mathrm{pr}_j$. Applying π_j to both sides of (3.1), we get

$$\mathrm{pr}_j(\mathbb{V}(\mathfrak{a})) = \pi_j(\mathbb{V}(\mathfrak{a}^{(j-1)})).$$

Here is an important observation

$$\begin{aligned} \mathfrak{a}^{(j)} &= \mathfrak{a} \cap K[x_{j+1}, \ldots, x_n] \\ &= \mathfrak{a} \cap (K[x_j, x_{j+1}, \ldots, x_n] \cap K[x_{j+1}, \ldots, x_n]) \\ &= (\mathfrak{a} \cap K[x_j, \ldots, x_n]) \cap K[x_{j+1}, \ldots, x_n] \\ &= \mathfrak{a}^{(j-1)} \cap K[x_{j+1}, \ldots, x_n]. \end{aligned}$$

Then we take $\mathfrak{b} \coloneqq \mathfrak{a}^{(j-1)} \subset K[x_j, \ldots, x_n]$, and view $\mathfrak{b}$ as an ideal in the new polynomial ring $K[x_j, \ldots, x_n]$. In these new notations $\mathfrak{b}^{(1)} \coloneqq \mathfrak{b} \cap K[x_{j+1}, \ldots, x_n] = \mathfrak{a}^{(j-1)} \cap K[x_{j+1}, \ldots, x_n] = \mathfrak{a}^{(j)}$. By (i) we know that $\mathfrak{b}$ is 0-dimensional. Then use Proposition 1.2 on $\mathfrak{b}$ and the ring $K[x_j, \ldots, x_n]$, we get $\mathrm{pr}_1(\mathbb{V}(\mathfrak{b})) = \mathbb{V}(\mathfrak{b}^{(1)})$. Finally,

$$\mathrm{pr}_j(\mathbb{V}(\mathfrak{a})) = \pi_j(\mathbb{V}(\mathfrak{a}^{(j-1)})) = \pi_j(\mathbb{V}(\mathfrak{b})) = \mathrm{pr}_1(\mathbb{V}(\mathfrak{b})) = \mathbb{V}(\mathfrak{b}^{(1)}) = \mathbb{V}(\mathfrak{a}^{(j)}),$$

completing the proof. □

Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional ideal and $f \in K[X]$ be a polynomial. We then define a map

$$\begin{aligned} L_f : K[X]/\mathfrak{a} &\to K[X]/\mathfrak{a}, \\ \bar{g} &\mapsto \overline{fg}, \end{aligned}$$

which is a K-linear map. Choose $1, g_2, \ldots, g_d \in K[X]$ such that $1, \overline{g_2}, \ldots \overline{g_d}$ form a basis of the K-linear space $K[X]/\mathfrak{a}$. Let M_f be the matrix of the linear map L_f under this basis.

Lemma 3.16. Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional ideal and Let $\mathbb{V}(\mathfrak{a}) = \{ c_1, \ldots, c_s \}$. Let $f \in K[X]$ be a polynomial and M_f, L_f be as above. Then for all $1 \le i \le s$, the vector $(1, g_2(c_i), \ldots, g_d(c_i))^T$ is an eigenvector of the matrix M_f, of the eigenvalue $f(c_i)$.

Proof. Let

$$M_f = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & & \vdots \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{pmatrix}$$

be the matrix presentation of L_f. Then for any $1 \leq j \leq d$, we have

$$L_f(\overline{g_j}) = \overline{fg_j} = \sum_{l=1}^{d} a_{jl}\overline{g_l},$$

or equivalently,

$$fg_j - \sum_{l=1}^{d} a_{jl}g_l \in \mathfrak{a}.$$

Take any $c_i \in \mathbb{V}(\mathfrak{a})$ for $1 \leq i \leq s$, evaluating the left hand side at c_i we get

$$f(c_i)g_j(c_i) - \sum_{l=1}^{d} a_{jl}g_l(c_i) = 0. \tag{3.2}$$

As each $g_j \notin \mathfrak{a}$, $g_j(c_i) \neq 0$, the vector

$$\begin{pmatrix} 1 \\ g_2(c_i) \\ \vdots \\ g_d(c_i) \end{pmatrix}$$

has non-zero entries. Equation (3.2) tells us that

$$M_f \begin{pmatrix} 1 \\ g_2(c_i) \\ \vdots \\ g_d(c_i) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & & \vdots \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{pmatrix} \begin{pmatrix} 1 \\ g_2(c_i) \\ \vdots \\ g_d(c_i) \end{pmatrix} = f(c_i) \begin{pmatrix} 1 \\ g_2(c_i) \\ \vdots \\ g_d(c_i) \end{pmatrix},$$

implying that $f(c_i)$ is an eigenvalue of M_f with eigen vector

$$\begin{pmatrix} 1 \\ g_2(c_i) \\ \vdots \\ g_d(c_i) \end{pmatrix},$$

as desired. □

Example. Let $\mathfrak{a} = (x_1^3 - x_2^2x_1, x_1^2x_2 - x_2^2) \subseteq K[x_1, x_2]$. Under the lexicographic order $x_1 \succ x_2$, we can find Gröbner basis

$$G = \left\{ x_1^3 - x_1x_2^2, x_1^2x_2 - x_2^2, x_1x_2^3 - x_1x_2^2, x_2^4 - x_2^3 \right\}$$

of the ideal $\mathfrak{a}$, via Buchberger's algorithm and with a little effort. By Proposition 2.15,

$$B \coloneqq \left\{ \overline{x_1}^2, \overline{x_1x_2}^2, \overline{x_1x_2}, \overline{x_1}, \overline{x_2}^3, \overline{x_2}^2, \overline{x_2}, 1 \right\}$$

is a K-linear basis for $K[x_1, x_2]/\mathfrak{a}$. Take $f = x_1$, we compute that

$$\overline{x_1}\begin{pmatrix} 1 \\ \overline{x_2} \\ \overline{x_2}^2 \\ \overline{x_2}^3 \\ \overline{x_1} \\ \overline{x_1x_2} \\ \overline{x_1x_2}^2 \\ \overline{x_1}^2 \end{pmatrix} = \begin{pmatrix} 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&1&0 \end{pmatrix} \begin{pmatrix} 1 \\ \overline{x_2} \\ \overline{x_2}^2 \\ \overline{x_2}^3 \\ \overline{x_1} \\ \overline{x_1x_2} \\ \overline{x_1x_2}^2 \\ \overline{x_1}^2 \end{pmatrix},$$

from which we read

$$M_{x_1} = \begin{pmatrix} 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&1&0 \end{pmatrix}.$$

The minimal polynomial of M_{x_1}.
On the other hand, from the Gröbner basis G of $\mathfrak{a}$, we can determine $\mathbb{V}(\mathfrak{a})$.

3.5 0-Dimensional Radical Ideals

In this subsection, we assume that $\operatorname{char} K = 0$.

Proposition 3.17. A proper 0-dimensional ideal is a prime ideal iff it is a maximal ideal.

Lemma 3.18. (i) Let $g_0 \in K[X]$ be an irreducible polynomial on K, and $g_1, \ldots, g_n \in K[X]$ be polynomials such that $\deg g_i < \deg g_0$, while $L \in K[X]$ be an element of transcendental degree 1. Set

$$\mathfrak{a} := (g_0(L), x_1 - g_1(L), \ldots, x_n - g_n(L)). \tag{3.3}$$

We conclude that if $\mathfrak{a} \neq K[X]$, then $\mathfrak{a}$ is maximal.

(ii) Any maximal ideal of $K[X]$ is generated in the manner described as in (i).

Proposition 3.19. If $\mathfrak{m} \subset K[X]$ is maximal, then

$$|\mathbb{V}(\mathfrak{m})| = \dim_k(K[X]/\mathfrak{m}).$$

Now we consider a more general case. Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional radical ideal. Suppose that

$$\mathfrak{a} = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_s.$$

is a minimal prime decomposition of $\mathfrak{a}$. Since $\mathfrak{a}$ is radical, such decomposition always exists, by Proposition 3.8. By the Nullstellensatz, we have $\mathbb{V}(\mathfrak{a}) = \mathbb{V}(\mathfrak{m}_1) \cup \mathbb{V}(\mathfrak{m}_2) \cup \cdots \cup \mathbb{V}(\mathfrak{m}_s)$. Since $\mathfrak{a}$ is 0-dimensional, $\mathbb{V}(\mathfrak{a})$ is a finite subset of $\overline{K}^n$. Thus each $\mathbb{V}(\mathfrak{m}_i)$ is a also a finite subset. So each $\mathfrak{m}_i$ is 0-dimensional, hence is maximal by Proposition 3.17.

Lemma 3.20. Let $\mathfrak{a}$ and $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be as above. There is an isomorphism

$$K[X]/\mathfrak{a} \simeq \bigoplus_{i=1}^{s} (K[X]/\mathfrak{m}_i)$$

of K-linear spaces.

The following proposition is a generalization of Proposition 3.19.

Proposition 3.21. Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional radical ideal, then

$$|\mathbb{V}(\mathfrak{a})| = \dim_K(K[X]/\mathfrak{a}).$$

For a general 0-dimensional ideal that is not necessarily radical, the following corollary holds.

Corollary 3.22. Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional ideal, then

$$|\mathbb{V}(\mathfrak{a})| \leq \dim_k(K[X]/\mathfrak{a}),$$

and the "=" holds iff $\mathfrak{a}$ is radical.

Proof. We consider the natural map

$$\begin{aligned} \pi : K[X]/\mathfrak{a} &\to K[X]/\sqrt{\mathfrak{a}}, \\ f + \mathfrak{a} &\mapsto f + \sqrt{\mathfrak{a}}. \end{aligned}$$

It's easy to see that π is a surjection, and it is a bijection iff $\mathfrak{a} = \sqrt{\mathfrak{a}}$. So

$$\dim_K(K[X]/\mathfrak{a}) \geq \dim_K(K[X]/\sqrt{\mathfrak{a}} = |\mathbb{V}(\mathfrak{a})| = |\mathbb{V}(\mathfrak{a})|.$$

□

Let $f \in K[X]$ be a non-zero polynomial. We say that f is **square-free** if it does not have as a divisor any square of a non-constant polynomial. Equivalently, f is square free iff $f = c\underline{f}$, where $c \in K$ is a constant and $\underline{f} := f/\gcd(f, f')$.

Proposition 3.23. Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional ideal, and let f_i be the generator of the ideal $\mathfrak{a} \cap K[x_i]$. Then we have

$$\sqrt{\mathfrak{a}} = \mathfrak{a} + (\underline{f_1}, \ldots, \underline{f_n}).$$

Proof.

Lemma 3.24. Let A be a commutative ring, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ be ideals that are mutually coprime with each other. Let $\mathfrak{a}$ be an arbitrary ideal of A, then

$$\mathfrak{a} + \cap_{i=1}^{m} \mathfrak{a}_i = \cap_{i=1}^{m} (\mathfrak{a} + \mathfrak{a}_i).$$

Lemma 3.25. Let $f_1, \ldots, f_n \in K[t]$ be square-free polynomials in one indeterminate, then the ideal $\mathfrak{a} = (f_1(x_1), \ldots, f_n(x_n))$ is a 0-dimensional radical ideal.

Proof. Obviously $\mathbb{V}(\mathfrak{a}) = \mathbb{V}(f_1, \ldots, f_n)$ is a finite subset of $\overline{K}^n$, by the Fundamental Theorem of Algebra. Thus $\mathfrak{a}$ is 0-dimensional. Furthermore, since $\overline{K}$ is algebraically closed, we have

$$|\mathbb{V}(\mathfrak{a})| = \deg(f_1) \cdots \deg(f_n)$$

We claim that the set

$$G \coloneqq \{\, f_1(x_1), \ldots, f_n(x_n) \,\}$$

is a Gröbner basis of the ideal $\mathfrak{a}$. If our claim holds, then by Proposition 2.15, we have

$$\dim_K(K[X]/\mathfrak{a}) = \deg(f_1)\deg(f_2)\cdots\deg(f_n) = |\mathbb{V}(\mathfrak{a})|.$$

By Corollary 3.22, we know that $\mathfrak{a}$ is 0-dimensional radical.
Now we prove the claim. For any $f_i(x_i), f_j(x_j) \in G$, we compute their S-polynomial.

$$\begin{aligned} S(f_i(x_i), f_j(x_j)) &= \mathrm{lc}(f_j)\frac{\mathrm{lcm}(\mathrm{lm}(f_i), \mathrm{lm}(f_j))}{\mathrm{lm}(f_i)} f_i - \mathrm{lc}(f_i)\frac{\mathrm{lcm}(\mathrm{lm}(f_i), \mathrm{lm}(f_j))}{\mathrm{lm}(f_j)} f_j \\ &= \mathrm{lc}(f_j)\mathrm{lm}(f_j) f_i - \mathrm{lc}(f_i)\mathrm{lm}(f_i) f_j, \end{aligned}$$

from which we conclude that

$$\mathrm{supp}(S(f_i(x_i), f_j(x_j))) \cap (\mathrm{lm}(G))_{M_n} \neq \varnothing.$$

The above equation shows that $S(f_i(x_i), f_j(x_j))$ is reduced modulo G, by Lemma 2.6. Then by Buchberger's Criterion 2.10, G is indeed a Gröbner basis of $\mathfrak{a}$, $S(f_i, f_j) \to_G 0$ for all $1 \leq i < j \leq n$. □

Now we prove the proposition. Let $\mathfrak{b} \coloneqq \mathfrak{a} + (\underline{f_1}, \ldots, \underline{f_n})$. By Lemma 3.25, the ideal $(\underline{f_1}, \ldots, \underline{f_n})$ is a 0-dimensional radical ideal. So there a decomposition

$$(\underline{f_1}, \ldots, \underline{f_n}) = \bigcap_{i=1}^{s} \mathfrak{m}_i,$$

with each $\mathfrak{m}_i$ a maximal ideal, by the argument below Proposition 3.19. Note that $\mathfrak{m}_i, \mathfrak{m}_j$ are coprime for any distinct $1 \leq i, j \leq s$, so we have

$$\mathfrak{b} = \mathfrak{a} + (\underline{f_1}, \ldots, \underline{f_n}) = \mathfrak{a} + \bigcap_{i=1}^{s} \mathfrak{m}_i = \bigcap_{i=1}^{s} (\mathfrak{a} + \mathfrak{m}_i),$$

by Lemma 3.24. Since $\mathfrak{a} + \mathfrak{m}_i = K[X]$ or $\mathfrak{a} + \mathfrak{m}_i = \mathfrak{m}_i$, $\mathfrak{b}$ is an intersection of finitely many maximal ideals. If we rewrite

$$\mathfrak{b} = \bigcap_{i=1}^{l} \mathfrak{m}_i,$$

then

$$\sqrt{\mathfrak{b}} = \sqrt{\bigcap_{i=1}^{l} \mathfrak{m}_i} = \bigcap_{i=1}^{l} \sqrt{\mathfrak{m}_i} = \bigcap_{i=1}^{l} \mathfrak{m}_i = \mathfrak{b},$$

as $\mathfrak{m}_i$ are all radical. This shows that $\mathfrak{b}$ is radical. On the other hand, by definition $f_i \in \sqrt{\mathfrak{a}} \cap K[x_i]$, so we have

$$\mathfrak{a} \subseteq \mathfrak{b} \subseteq \sqrt{\mathfrak{a}}.$$

Taking radicals, we have

$$\sqrt{\mathfrak{a}} \subseteq \mathfrak{b} \subseteq \sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}},$$

showing that $\mathfrak{b} = \sqrt{\mathfrak{a}}$. □

3.6 Decomposition of 0-Dimensional Radical Ideals

We assume that $\operatorname{char} K = 0$ in this subsection.

Lemma 3.26. Let $c_1, \ldots, c_m \in \overline{K}^n$, then there exists a linear homogeneous polynomial $L \in K[X]$ such that $L(c_i) \neq 0, 1 \leq i \leq m$.

Corollary 3.27. Let $c_1, \ldots, c_m \in \overline{K}^n$ be m distinct points, then there exists a polynomial $L \in K[X]$ satisfying $\operatorname{totdeg} L = 1$ and $L(c_i) \neq L(c_j), 1 \leq i < j \leq m$.

Proof. Consider the subset

$$S \coloneqq \{\, c_i - c_j \mid 1 \leq i < j \leq m \,\},$$

which is a finite subset of $\overline{K}^n \setminus \{\, 0 \,\}$. By Lemma 3.26, there is a linear homogeneous polynomial such that $L(c_i - c_j) \neq 0$ for all $1 \leq i < j \leq m$. In fancier language, we can find an $L \notin \mathbb{I}(S)$ such that $\operatorname{totdeg} L = 1$, as desired. □

Corollary 3.28. Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional radical ideal, then there exists a linear polynomial $L \in K[X]$ such that

$$1, \overline{L}, \ldots, \overline{L}^{d-1}$$

is a basis of $K[X]/\mathfrak{a}$, with $d = \dim_k(K[X]/\mathfrak{a})$.

Proof. Since $\mathfrak{a}$ is 0-dimensional radical, there holds $\mathbb{V}(\mathfrak{a}) = \{\, c_1, \ldots, c_d \,\}$ with $d = \dim_k(K[X]/\mathfrak{a})$. By the above corollary, there exists a linear homogeneous polynomial L such that $L(c_i) \neq L(c_j)$ for all $1 \leq i < j \leq d$.
We just need to show that $1, \overline{L}, \ldots, \overline{L}^{d-1}$ are K-linear dependent in $K[X]/\mathfrak{a}$. Otherwise, suppose there were $a_0, a_1, \ldots, a_{d-1} \in K$ such that

$$\sum_{i=0}^{d-1} a_i \overline{L}^i = 0,$$

or equivalently,

$$\sum_{i=0}^{d-1} a_i L^i \in \mathfrak{a} = \sqrt{\mathfrak{a}} = \mathbb{I}(\mathbb{V}(\mathfrak{a})). \tag{3.4}$$

This shows that the polynomial $\sum_{i=0}^{d-1} a_i L^i$ vanishes on $\mathbb{V}(\mathfrak{a})$. Let $g \coloneqq \sum_{i=0}^{d-1} a_i t^i \in K[t]$, which is a univariable polynomial of degree $d-1$. Equation 3.4 tells us that $g(t)$ has d distinct roots $L(c_1), L(c_2), \ldots, L(c_d)$, implying that $g = 0$. Thus $a_0 = \cdots = a_{d-1}$, as desired. □

Lemma 3.29 (Shape Lemma). Let $\mathfrak{a} \subset K[X]$ be a 0-dimensional radical ideal, $d = \dim_k(K[X]/\mathfrak{a})$. Then there exists a linear polynomial $L \in K[X]$ and exist polynomials $g_0, g_1, \ldots, g_n \in K[t]$ with $\deg g_0 = d, \deg g_i < d$ for all $1 \leq i \leq n$, such that

$$\mathfrak{a} = (g_0(L), x_1 - g_1(L), \ldots, x_n - g_n(L)).$$

Proof.

□

4 Dimension

As in the previous sections, we denote by $X = \{ x_1, \ldots, x_n \}$ the set of indeterminates $x_1, \ldots, x_n$. If $Y = \{ y_1, \ldots, y_m \} \subseteq X$ is a subset of X, we often denote by $K[Y]$ the polynomial ring with indeterminates $y_1, \ldots, y_m$.

Definition 4.1. Let Y, X be as above and $\mathfrak{a} \subset K[X]$ be a proper ideal. We say that Y is **irrelevant modulo** $\mathfrak{a}$, if $\mathfrak{a} \cap K[Y] = (0)$. The **dimension** of $\mathfrak{a}$ is defined to be the integer

$$\sup \{ \ |Y| \, | Y \subset X, \ Y \text{ irrelevant modulo } \mathfrak{a} \}.$$

We often use the notation $\dim(\mathfrak{a})$ for the dimension of the ideal $\mathfrak{a}$.

For a K-algebra R and a subset $S \subseteq R$, we say that S is **algebraically dependent** over K, if there exist $a_1, \ldots, a_m \in S$ and a non-zero polynomial $f \in K[x_1, \ldots, x_m]$ such that $f(a_1, \ldots, a_m) = 0$; say that S is **algebraically independent** over K, if it is not algebraically dependent over K.

Now let $\mathfrak{a} \subset K[X]$ be an ideal of $K[X]$ and $Y = \{ y_1, \ldots, y_m \}$ be a subset of X, then let $R \coloneqq K[X]/\mathfrak{a}$. It's easy to show that the image $\{ \overline{y}_1, \ldots, \overline{y}_m \}$ of Y in R is algebraically independent over K iff Y is irrelevant modulo $\mathfrak{a}$. Indeed, if $\{ \overline{y}_1, \ldots, \overline{y}_m \}$ is algebraically independent over K, then there are elements, say $\overline{y}_1, \ldots, \overline{y}_s$ and a polynomial f of s indeterminates, such that $f(\overline{y}_1, \ldots, \overline{y}_m) = 0$. But this means that $f(y_1, \ldots, y_m) \in \mathfrak{a}$. Since already we have $f \in K[y_1, \ldots, y_s] \subset K[Y]$, $0 \neq f \in \mathfrak{a} \cap K[Y]$, showing that Y is not irrelevant modulo $\mathfrak{a}$. Conversely, if Y is not irrelevant modulo $\mathfrak{a}$, then $(0) \neq K[Y] \cap \mathfrak{a}$. Then we can pick $0 \neq f \in \mathfrak{a} \cap K[Y]$, so $f(y_1, \ldots, y_s) \in \mathfrak{a}$ implies that $\overline{f(y_1, \ldots, y_s)} = f(\overline{y_1}, \ldots, \overline{y_s}) = 0$. This shows that $\{ \overline{y_1}, \ldots, \overline{y_s} \}$ is algebraically dependent over K.

Proposition 4.1. Let $\mathfrak{a} \subset K[X]$ be a proper ideal. Then

(i) if $\mathfrak{a}$ is a 0-dimensional ideal defined by Theorem 3.14, then $\dim \mathfrak{a} = 0$;

(ii) if $\mathfrak{a} = (f)$ with f non-constant, then $\dim \mathfrak{a} = n - 1$;

(iii) if $\mathfrak{p}$ is prime, then $\dim \mathfrak{p} = \operatorname{trdeg}(\operatorname{Frac}(K[X]/\mathfrak{p})/K)$;

(iv) $\dim \mathfrak{a} = \dim \sqrt{\mathfrak{a}}$.

Proof. (i) If $\mathfrak{a}$ is 0-dimensional, then by Theorem 3.14 (ii), $\mathfrak{a} \cap K[x_i] \neq (0)$ for all $1 \leq i \leq n$, so $\varnothing$ is the only subset of X irrelevant modulo $\mathfrak{a}$. Thus $\dim \mathfrak{a} = |\varnothing| = 0$.
(ii) Let $\deg_{x_1}(f) > 0$. Then it's easy to see that the subset $\{ x_2, \ldots, x_n \}$ is irrelevant modulo $\mathfrak{a}$.
(iii) For simplicity, let $F \coloneqq \operatorname{Frac}(K[X]/\mathfrak{p})$, by definition we have $F = K(\overline{x_1}, \ldots, \overline{x_n})$. For any subset $\{ y_1, \ldots, y_m \} \subseteq X$ irrelevant modulo $\mathfrak{p}$, from the discussion above

the proposition, the subset $\{ \overline{y_1}, \ldots, \overline{y_m} \}$ is algebraically independent over K. Thus $|Y| \leq \operatorname{trdeg}(F/K)$, so $\dim \mathfrak{p} \leq \operatorname{trdeg}(F/K)$. On the other hand, the subset $\{ \overline{x_1}, \ldots, \overline{x_n} \} \subseteq F$ is algebraically dependent over K by definition, so there exists a subset $\{ y_1, \ldots, y_m \} \subseteq X$ such that $\{ \overline{y_1}, \ldots, \overline{y_m} \}$ is a transcendental basis of the extension F/K. This happens iff the subset $\{ y_1, \ldots, y_m \}$ is irrelevant modulo $\mathfrak{p}$. So $\dim \mathfrak{p} \geq |Y| = \operatorname{trdeg}(F/K)$.
(iv) Since $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, $\dim \mathfrak{a} \geq \dim \sqrt{\mathfrak{a}}$ holds obviously. What left to us is to show that $\dim \mathfrak{a} \leq \dim \sqrt{\mathfrak{a}}$. It suffices to show that for any subset $Y \subseteq X$, $K[Y] \cap \mathfrak{a} = (0) \implies K[Y] \cap \sqrt{\mathfrak{a}} = (0)$. Otherwise, if $K[Y] \cap \sqrt{\mathfrak{a}} \neq (0)$, then there is a non-zero $f \in K[Y] \cap \sqrt{\mathfrak{a}}$. But $f^m \in \mathfrak{a}$ for some integer $m > 0$, then $f^m \in K[Y] \cap \mathfrak{a}$, a contradiction.

□

If $V \subseteq \overline{K}^n$ is an affine variety. We define the **dimension** $\dim V$ of the affine variety V by $\dim \mathbb{I}(V)$.

Proposition 4.2. Let $\mathfrak{a}, \mathfrak{b}$ be two ideals of $K[X]$. Then

(i) $\dim \mathfrak{b} \leq \dim \mathfrak{a}$, if $\mathfrak{a} \subseteq \mathfrak{b}$;

(ii) $\dim(\mathfrak{a} \cap \mathfrak{b}) = \max \{ \dim \mathfrak{a}, \dim \mathfrak{b} \}$.

Corollary 4.3. Let $\mathfrak{a} \subseteq K[X]$ be a radical ideal, $\mathfrak{a} = \cap_{i=1}^{s} \mathfrak{p}_i$ be a prime decomposition of $\mathfrak{a}$. Then

$$\dim \mathfrak{a} = \max \{ \dim \mathfrak{p}_1, \ldots, \dim \mathfrak{p}_s \}.$$

Proposition 4.4. Let $\mathfrak{p} \subseteq K[X]$ be a prime ideal, and $f \in K[X] \backslash \mathfrak{p}$ be a polynomial that is not in $\mathfrak{p}$. If $\mathfrak{p} + (f) \neq K[X]$, then

$$\dim(\mathfrak{p} + (f)) \leq \dim \mathfrak{p} - 1.$$

Corollary 4.5. Let $\mathfrak{p} \subseteq K[X]$ be a prime ideal and $\mathfrak{a} \subseteq K[X]$ be a proper ideal. If $\mathfrak{p} \subsetneq \mathfrak{a}$, then $\dim \mathfrak{a} \leq \dim \mathfrak{p} - 1$.

Let A be a commutative ring, then we consider all the strictly ascending chains

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_d \tag{4.1}$$

of prime ideals in A. We call the integer d to be the **length** of the strictly ascending chain (4.1). The **Krull dimension** a of a commutative ring A. Note that $\operatorname{kdim} A$ may be infinite, even when A is Noetherian. The **Krull dimension** of a proper ideal $\mathfrak{a} \subset A$ is defined to be the Krull dimension of the quotient ring $A/\mathfrak{a}$, and is denoted by $\operatorname{kdim} \mathfrak{a}$.

Proposition 4.6. Let $\mathfrak{a} \subseteq K[X]$ be an ideal, then $\dim \mathfrak{a} \geq \operatorname{kdim} \mathfrak{a}$.

4.1 Hilbert Polynomials

5 Affine Dimension Theorem

5.1 Noether Normalization Lemma

Let $A \hookrightarrow B$ be an extension of commutative rings. We say that $b \in B$ is **integral** over A, if there exists a non-zero monic polynomial $f(x) \in A[x]$ such that $f(b) = 0$. We say that the ring B is **integral** over A, if every element of B is integral over A.

Example. $\sqrt{2}$ is integral over $\mathbb{Z}$, but $1/\sqrt{2}$ is not.

Lemma 5.1. Let $A \hookrightarrow B$ be an extension of rings. If $a, b \in B$ are integral over A, then $a + b$ and ab are integral over A.

Proposition 5.2. Let $A \hookrightarrow B \hookrightarrow C$ be a ring extension. If C is integral over B and B is integral over A, then C is integral over A.

Theorem 5.3 (Noether Normalization Lemma)**.** Let A be a finitely generated K-algebra, then there exist $a_1, \ldots, a_d \in A$ such that:

(i) $a_1, \ldots, a_d$ are algebraically independent over K,

(ii) A is integral over $K[a_1, \ldots, a_d]$.

As in the above theorem, we call the ring $K[a_1, \ldots, a_d]$ to be a **Noether normalization** of A.

Proposition 5.4. Let $\mathfrak{a} \subseteq K[X]$ be a proper ideal, $K[a_1, \ldots, a_d]$ be a Noether normalization of $K[X]/\mathfrak{a}$. Then $\dim \mathfrak{a} = d$.

5.2 Norms

Let $F \subseteq E$ be a field extension with $[E : F] = d$, and let $a \in E$. Then we can construct an F-linear map

$$\begin{aligned} \phi_a : E &\to E, \\ b &\mapsto ab. \end{aligned}$$

Let $v_1, \ldots, v_d$ be a basis for E over F, then we denote by M_a the matrix of ϕ_a under this basis. It's easy to see that $\det M_a$ is independent of the choice of the basis $v_1, \ldots, v_d$; indeed, if two bases $\{v_1, \ldots, v_d\}$ and $\{u_1, \ldots, u_d\}$ are related by an invertible matrix $S \in \mathrm{GL}(d; F)$, then the matrix representations of ϕ_a under those bases are related by a similar transformation of S, which preserves determinants. So $\det M_a \in F$ is said to be the **norm** of a about the field extension $F \subseteq E$, and is denoted by $N_{E/F}(a)$.

Lemma 5.5. Let $F \subseteq E \subset K$ be finite extensions of fields, and let $a \in E$. Then

$$N_{K/F}(a) = N_{E/F}(a)^{[K:E]}.$$

Corollary 5.6. Let $F \subseteq E$ be a finite extension of fields, and $a \in E$. Suppose that the

minimal polynomial of $a \in E$ has the form

$$x^d + b_{d-1}x^{d-1} + \cdots + b_0, b_i \in F.$$

Then

$$N_{E/F}(a) = (-1)^{d[E:F(a)]} b_0^{[E:F(a)]}.$$

Now we assume that A is an integral domain. We say that A is **integrally closed**, if all elements in $\mathrm{Frac}(A)$ that are integral over A are in A itself. All unique factorization domains are integrally closed [8]. In particular, polynomial rings over a field are all integrally closed.

[8] *Why?*

Lemma 5.7. Let $A \subseteq B$ be an extension of integral domains, with B integrally closed and $a \in A$. Suppose that a in algebraic over $K := \mathrm{Frac}(B)$, with $g(x) \in K[x]$ the minimal polynomial of a over K. If a is integral over B, then $g(x) \in B[x]$.

5.3 Affine Dimension Theorem

Let $\mathfrak{p} \subseteq K[X]$ be a prime ideal, and let B be a Noether normalization of $A := K[X]/\mathfrak{p}$. Let $F := \mathrm{Frac}(A)$ and $E := \mathrm{Frac}(B)$, then $F \subseteq E$ is a finite algebraic extension[9] of fields hence $[E : F]$ is finite. For $f \in K[X]$, we use the notation $\overline{f}$ for its image in $A = K[X]/\mathfrak{p}$.

[9] *Why?*

Lemma 5.8. For any $f \in K[X]$, $N_{E/F}(\overline{f}) \in B$.

To avoid confusion, we use the notation $(-)_S$ for the ideal generated by $-$ in some commutative ring S.

Lemma 5.9. For any $f \in K[X]$,

$$B \cap \sqrt{(\overline{f})_A} = \sqrt{(N_{E/F}(\overline{f}))_B}$$

Proposition 5.10. Let $\mathfrak{p} \subseteq K[X]$ be a prime ideal, $f \in K[X] \backslash \mathfrak{p}$ be a polynomial. If $\sqrt{\mathfrak{p} + (f)}$ is a prime ideal of $K[X]$, then

$$\dim \sqrt{\mathfrak{p} + (f)} = \dim \mathfrak{p} - 1.$$

Lemma 5.11. Let $\mathfrak{p} \subseteq K[X]$ be a prime ideal, and $h \in K[X] \backslash \mathfrak{p}$. Set

$$\mathfrak{p}^h := \mathfrak{p} + (zh - 1) \subseteq K[X, z],$$

then $\mathfrak{p}^h$ is a prime ideal of $K[X, z]$ and $\dim \mathfrak{p}^h = \dim \mathfrak{p}$.

Proposition 5.12. Let $\mathfrak{p} \subseteq K[X]$ be a prime ideal, $f \in K[X] \backslash \mathfrak{p}$ be a polynomial. If $\mathfrak{p} + (f) \neq K[X]$, then the dimension of every minimal prime component of $\sqrt{\mathfrak{p} + (f)}$ is $\dim \mathfrak{p} - 1$.

We say that an affine variety V in $\overline{K}^n$ is a **hypersurface** if $V = \mathbb{V}(f)$ for some non-constant polynomial $f \in K[X]$. Using the mighty Nullstellensatz, we get the geometric version of Proposition 5.12:

Corollary 5.13. Let $U \subseteq \overline{K}^n$ be an irreducible affine variety, $V \subset \overline{K}^n$ be a hypersurface. If $U \cap V \neq \varnothing$ nor $U \nsubseteq V$, then the dimension of every minimal irreducible component of $U \cap V$ is $\dim U - 1$.

Corollary 5.14. Let $U, V \subseteq \overline{K}^n$ with V a hypersurface. Let $U = U_1 \cup \cdots \cup U_s$ be a minimal irreducible decomposition of U. If $U_i \nsubseteq V$ for all such $\dim U_i = \dim U$, then

$$\dim(U \cap V) \leq \dim U - 1.$$

Now we prove that the Krull dimension of an ideal $\mathfrak{a}$ of $K[X]$ coincides with the dimension of $\mathfrak{a}$ defined in Definition 4.1.

Proposition 5.15. Let $\mathfrak{a} \in K[X]$ be a proper ideal, then

$$\dim \mathfrak{a} = \operatorname{kdim} \mathfrak{a}.$$

Lemma 5.16. Let $\mathfrak{a} \subseteq K[X]$ and $\mathfrak{b} \subseteq K[Y]$ be two ideals, where X, Y are two finite sets with no intersection, and in addition $|X| = |Y| = n$. Then

$$\dim(\mathfrak{a} + \mathfrak{b}) = \mathfrak{a} + \mathfrak{b},$$

where $\mathfrak{a} + \mathfrak{b}$ is viewed as an ideal of the ring $K[X, Y]$, via the natural inclusions $\mathfrak{a} \subseteq K[X] \subseteq K[X, Y]$ and $\mathfrak{b} \subseteq K[Y] \subseteq K[X, Y]$.

Lemma 5.17. Let X, Y be finite subsets as in Lemma 5.16, and let $\mathfrak{a} \subseteq K[X, Y]$ be an ideal. If $x_i - y_i \in \mathfrak{a}$ for all $1 \leq i \leq n$, then

$$\dim \mathfrak{a} = \dim(\mathfrak{a} \cap K[X]),$$

where $\mathfrak{a} \cap K[X]$ in the right hand side is viewed as an ideal of $K[X, Y]$.

In the rest of this subsection, we denote pr_X by the following projection

$$\begin{aligned} \operatorname{pr}_X : \overline{K}^{2n} &\to \overline{K}^n, \\ (u, v) &\mapsto u, \end{aligned}$$

with $u, v \in \overline{K}^n$. The following is a direct corollary of Lemma 5.17.

Corollary 5.18. Let $U, V \subseteq \overline{K}^n$ be affine varieties, then

$$\dim(U \cap V) = \dim((U \times V) \cap \mathbb{V}(x_1 - y_1, \ldots, x_n - y_n)).$$

Lemma 5.19. Let K be an algebraically closed field, and $U, V \subseteq \overline{K}^n$ be irreducible affine varieties. Then $U \times V$ is again an irreducible affine variety in $\overline{K}^{2n}$.

Theorem 5.20. Let K be an algebraically closed field, and $U, V \subseteq \overline{K}^n$ be two irreducible affine varieties. If $U \cap V \neq \varnothing$, then every minimal irreducible component of

$U \cap V$ is of dimension no less than

$$\dim U + \dim V - n.$$

Lemma 5.21. Let K be a field, not necessarily algebraically closed. Then for any ideal $\mathfrak{a} \subset K[X]$, we have

$$\dim \mathfrak{a} = \dim \mathfrak{a}^{\mathrm{e}},$$

where $\mathfrak{a}^{\mathrm{e}}$ is the extension of $\mathfrak{a}$ along the natural inclusion $K[X] \hookrightarrow \overline{K}[X]$, with $\overline{K}$ the algebraic closure of K.

Lemma 5.22. Let $U \subset K^n$ be an irreducible K-affine variety. When viewed as a $\overline{K}$-variety, suppose $U = U_1 \cup \cdots \cup U_s$ be a maximal irreducible decomposition. Then

$$\dim U_i = \dim U$$

[10] for all $1 \leq i \leq s$.

[10] *In which ring the dimensions of both sides are taken?*

The following theorem is a refinement of Theorem 5.20.

Theorem 5.23 (Affine Dimension Theorem)**.** Let K be a field that is not necessarily algebraically closed, and $U, V \subseteq K^n$ be irreducible affine varieties. If $U \cap V \neq \varnothing$, then very minimal irreducible component of $U \cap V$ is of dimension no less than

$$\dim U + \dim V - n.$$

Claim 5.24. $\overline{K}$ is infinite.

Proof. If it were finite, let $\overline{K} = \{a_1, \ldots, a_m\}$, then construct $f \in \overline{K}[x]$ as

$$f = (x - a_1) + \cdots + (x - a_m) + 1$$

□

Example. $S = \{\, (0,0), (1,0), (0,1) \,\}$, what is $\mathbb{I}(S)$? Let $y \succ x$. De