# Notes for Intro to Algebraic Geometry

Ting Gong

Started Mar. 24, 2019. Last revision April 23, 2019

# Contents

# Chapter 1

# Notes: Geometry, Algebra and Algorithm

## 1.1 Polynomials and Affine Space

We are going to studt polynomials of a field in this course, since linear algebra works on any of them. Examples are $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ etc.

**Definition 1.1.1.** A *monomial* in $x_1, \ldots, x_n$ is a product of the form $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, where $\alpha_1, \ldots, \alpha_n$ are nonnegative integers. The *total degree* of the monomial is $\alpha_1 + \ldots + \alpha_n$

In the future, we denote$x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, $\alpha = (\alpha_1, \ldots, \alpha_n)$, and $|\alpha| = \alpha_1 + \ldots + \alpha_n$.

**Definition 1.1.2.** A *polynomial* $f$ in $x_1, \ldots, x_n$ with coefficients in a field $F$ is a finite linear combination of monomials. We denote $f = \sum_\alpha a_\alpha x^\alpha, a_\alpha \in F$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in $F$ is denoted as $F(x_1, \ldots, x_n)$ (A field extension of $F$.

We have examples $\mathbb{Q}(x), \mathbb{R}(x, y), \mathbb{C}(x, y, z)$.

**Definition 1.1.3.** Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $F(x_1, \ldots, x_n)$. Then we call $a_\alpha$ the *coefficient* of monomial $x^\alpha$. If the coefficient $a_\alpha \neq 0$, we call $a_\alpha x^\alpha$ a *term* of $f$. The *total degree* of $f \neq 0$ is denoted as $deg(f)$, is the maximum $|\alpha|$ such that $a_\alpha$ is nonzero. The total degree of the zero polynomial is undefined.

Then an example.

**Remark 1.1.4.** The sum and product of two polynomials are polynomials. We say $f$ *devides* a polynomial $g$ if $g = fh$ for some $h \in F(x_1, \ldots, x_n)$ nonzero. We can show $F[x_1, \ldots, x_n]$ to be a polynomial ring.

**Definition 1.1.5.** Given a field $F$, $n \in \mathbb{Z}^+$, we define the $n$-dimensional *affine space* over $F$ to be $F^n = \{(x_1, \ldots, x_n) | x_1, \ldots, x_n \in F\}$.

Examples are $\mathbb{R}^n$, for $F^1$ we call an affine line, and $F^2$ we call an affine plane. We can connect a polynomial with an affine space by having the evaluation map $f : F^n \to F$.

**Proposition 1.1.6.** *Let $F$ be an infinite field and $f \in F[x_1, \ldots, x_n]$. Then $f = 0$ in $F[x_1, \ldots, x_n]$ iff $f : F^n \to F$ is the zero function. (It might not be true in finite field.)*

*Proof.* ($\Rightarrow$) Obvious.

($\Leftarrow$) We prove by induction. Base case: $n = 1$, by Fundamental Theorem of Algebra, $f \in F[x]$ of degree $m$ has $m$ roots. Let $f(a) = 0, \forall a \in F$. Since $F$ is infinite, $f$ has infinitely many roots. Thus $f = 0$.

Assume this being true to $n-1$. Let $f \in F[x_1, \ldots, x_n]$ be a zero function. We can write $f = \sum_{i=1}^{N} g_1(x_1, \ldots, x_{n-1}) x_n^i$. Where $g_i \in F[x_1, \ldots, x_{n-1}]$. We want to show that $g_i$ is a zero polynomial in $F[x_1, \ldots, x_n]$. Let $(a_1, \ldots, a_{n-1}) \in F^{n-1}$. We have $f(a_1, \ldots, a_{n-1}, x_n) \in F[x_n]$. By induction hypothesis, $f(a_1, \ldots, a_{n-1}, x_n) = 0$ in $F[x_n]$. Thus, we see that $g_i(a_1, \ldots, a_{n-1}) = 0$. Therefore, by our inductive assumption, $g_i$ is the zero polynomial in $F[x_1, \ldots, x_{n-1}]$. Therefore, $f$ is the zero polynomial in $F[x_1, \ldots, x_n]$. □

**Corollary 1.1.7.** *Let $F$ be a infinite field. $f, g \in F[x_1, \ldots, x_n]$. Then $f = g$ iff $f : F^n \to F$, and $g : F^n \to F$ are the same function.*

*Proof.* ($\Rightarrow$) Obvious.

($\Leftarrow$) Assume $f, g$ are the same function. $f - g$ is a zero function. Therefore by our last proposition, $f - g = 0$, thus $f = g$. □

**Theorem 1.1.8.** *(Fundamental Theorem of Algebra) Every nonconstant polynomial $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.*

*Proof.* Assume there is no such root. Let $g = \frac{1}{f}$. Then we want to show that $g$ is bounded and entire, and by Liouville's Theorem we have $f$ is constant. $g$ is clearly entire since it is the inverse of the polynomial. Consider $g = \frac{1}{|z|^n(a_n + a_{n-1}/z + \ldots + a_0/z^n}$. As $n \to \infty$, $g \to 0$. Thus, $\exists R > 0$, such that $\forall |z| > R$, $|f(z)| < 1$. Since $|z| \leq R$ is compact, there is a maximum $M$. Thus $f(z)$ is bounded by either $M$ or 1. Thus we have our desired outcome. □

**Definition 1.1.9.** We say that $F$ is algebraically closed if every nonconstant polynomial in $F[x]$ has a root in $F$.

## 1.2 Affine Varieties

**Definition 1.2.1.** Let $F$ be a field, and let $f_1, \ldots, f_n$ be polynomials in $F[x_1, \ldots, x_n]$. Then $V(f_1, \ldots, f_n) = \{(a_1, \ldots, a_n) \in F^n | f_i(a_1, \ldots, a_n) = 0, \forall 1 \leq i \leq s\}$. We call $V$ the affine variety defined by $f_1, \ldots, f_n$.

Therefore, the affine variety is the set of all solutions of systems. We see examples such as $V(x^2 + y^2 - 1)$, $V(xy - x^3 + 1)$, $V(z - x^2 - y^2)$ and several others. Then the twisted

cubie. The dimensions of the affine varieties is not intuitive. Consider the linear variety of $F^n$ of $m$ equations, by linear algebra, we know the dimension is not necessarily $n-m$, but $n-r$, with $r$ being the rank. The key is "linear Independence". Consider Lagrange Multiplier Theorem. Moreover, an affine variety can be empty.

**Lemma 1.2.2.** *If $V, W$ are affine varieties, then $V \cup W$ and $V \cap W$ are affine varieties.*

*Proof.* Let $V = V(f_1, \ldots, f_n)$, $W = V(g_1, \ldots, g_m)$. For $V \cap W$, we see that $f_1, \ldots, f_n = 0$ and $g_1, \ldots, g_m = 0$. Thus $f_1, \ldots, f_n = g_1, \ldots, g_m = 0$. Thus $V \cap W = V(f_1, \ldots, f_n, g_1, \ldots, g_m)$. Therefore, $V \cap W$ is an affine variety.

Consider $V \cup W$, we want to show that $V \cup W \subseteq V(f_i g_j)$. If $f_i = 0$, then we know that $f_i g_j = 0$. Similarly, if $g_j = 0$, then $f_i g_j = 0$. Then we check $V(f_i g_j) \subseteq V \cup W$. If $f_i g_j = 0$, then either $f_i = 0$, where $f_i g_j \in V$, or $g_j = 0$, where $f_i g_j \in W$. Therefore, $V \cup W = V(f_i g_j)$ thus is also a variety. □

## 1.3 Parametrization of Affine Varieties

**Definition 1.3.1.** Let $F$ be a field, a *rational function* in $t_1, \ldots, t_n$ with coefficients in $F$ is a quotient $f/g$ of two polynomials $f, g \in F[t_1, \ldots, t_n]$, where $g \neq 0$. The set of all rational functions in $t_1, \ldots, t_n$ with coefficients in $F$ is denoted $F(t_1, \ldots, t_n)$.

Notice that two rational functions $f/g = f'/g'$ iff $g'f = gf'$. And $F(t_1, \ldots, t_n)$ forms a field.

**Definition 1.3.2.** Let $V = V(f_1, \ldots, f_n) \subseteq F^n$ be a variety. Then a *rational parametric representation* of $V$ consists of rational functions $r_1, \ldots, r_n \in F(t_1, \ldots, t_n)$ such that the points $x_n = r_n(t_1, \ldots, t_m), \forall n$ lie in $V$. If $r_1, \ldots, r_n$ are polynomials, then we call it a *polynomial parametric representation* of $V$. The original equations of $V$ are called *implicit representation* of $V$.

**Definition 1.3.3.** If an affine variety can be parametrized by a rational parametric represenation, then they are called *unirational*.

Notice that given a parametric representation of an affine variety, we can always find the defining equations. We will prove this later in the course.

Next, we look at examples, $x^2 + y^2 = 1$ and $V(y - x^2, z - x^3)$.

## 1.4 Ideals

**Definition 1.4.1.** A subset $I \subseteq F[x_1, \ldots, x_n]$ is an *ideal* if it satisfies:

(i) $0 \in I$

(ii) If $f, g \in I$, then $f + g \in I$.

(iii)If $f \in I$, $h \in F[x_1, \ldots, x_n]$, then $hf \in I$.

**Definition 1.4.2.** Let $f_1, \ldots, f_s$ be polynomials in $F[x_1, \ldots, x_n]$. Then we set

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i | h_1, \ldots, h_s \in F[x_1, \ldots, x_n] \right\}$$

We call it *ideal generated by* $f_1, \ldots, f_s$.

**Lemma 1.4.3.** *Let $f_1, \ldots, f_s$ be polynomials in $F[x_1, \ldots, x_n]$, then $\langle f_1, \ldots, f_s \rangle$ is an ideal of $F[x_1, \ldots, x_n]$.*

*Proof.* First, $0 \in \langle f_1, \ldots, f_s \rangle$ since $0 = \sum_{i=1}^{s} 0 f_i$. Then, Let $f, g \in \langle f_1, \ldots, f_s \rangle$, $f = \sum_{i=1}^{s} h_i f_i$, and $g = \sum_{i=1}^{s} k_i f_i$, $f + g = \sum_{i=1}^{s} (h_i + k_i) f_i$. Thus $f + g \in \langle f_1, \ldots, f_s \rangle$. Finally, let $x \in F[x_1, \ldots, x_n]$, then $xf = \sum_{i=1}^{s} (x h_i) f_i$. Thus $xf \in \langle f_1, \ldots, f_s \rangle$. Thus, $\langle f_1, \ldots, f_s \rangle$ is an ideal of $F[x_1, \ldots, x_n]$. □

**Definition 1.4.4.** An ideal $I$ is *finitely generated* if $\exists f_1, \ldots, f_s \in F[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \}$. And we say that $f_1, \ldots, f_s$ are basis of $I$.

Next, we show that a variety depends only on the ideal generated by defining functions.

**Proposition 1.4.5.** *If $f_1, \ldots, f_S$ and $g_1, \ldots, g_t$ are bases of the same ideal in $F[x_1, \ldots, x_n]$, then we have $V(f_1, \ldots, f_S) = V(g_1, \ldots, g_t)$.*

*Proof.* Take $a_g \in V(g_1, \ldots, g_t)$, $f \in \langle f_1, \ldots, f_s \rangle$, and since$g_1, \ldots, g_t$ and $f_1, \ldots, f_S$ span the same ideal, $f \in \langle g_1, \ldots, g_t \rangle$. $f = \sum_{i=1}^{s} a_i g_i$. Thus, $f(a_g) = \sum_{i=1}^{s} a_i g_i(a_g) = 0$. Therefore, $a_g \in V(f_1, \ldots, f_s)$. The other inclusion follows the same proof. □

**Definition 1.4.6.** Let $V \subseteq k^n$ be an affine variety, then

$$I(V) = \{ f \in k[x_1, \ldots, x_n] | f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in V \}$$

We call this the *ideal* of $V$.

**Lemma 1.4.7.** *If $V \subseteq k^n$ be an affine variety, then $I(V) \subseteq k[x_1, \ldots, x_n]$ is an ideal.*

*Proof.* It is clear $0 \in I(V)$. If $f, g \in I(V), a = (a_1, \ldots, a_n) \in V$, then $(f + g)(a) = f(a) + g(a) = 0$. Thus $(f + g) \in I(V)$. Let $h \in k[x_1, \ldots, x_n]$, then $hf(a) = h(a)f(a) = h(a)0 = 0$. Thus $hf \in I(V)$. Thus $I(V)$ is an ideal. □

Then we look at two examples of $I(V)$.

**Lemma 1.4.8.** *Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Then $\langle f_1, \ldots, f_s \rangle \subseteq I(V(f_1, \ldots, f_s))$. The other inclusion doesn't always work.*

*Proof.* First, let $a \in V(f_1, \ldots, f_s)$. Let $f \in \langle f_1, \ldots, f_s \rangle$, then $f = \sum_{i=1}^{s} h_i f_i, h \in k[x_1, \ldots, x_n]$. Then $f(a) = \sum_{i=1}^{s} h_i f_i(a) = 0$. Thus $f \in I(V(f_1, \ldots, f_s))$.

The other side doesn't work, consider counterexample $V(x^2, y^2)$. □

**Proposition 1.4.9.** *Let $V$, $W$ be affine varieties in $k^n$. Then*
*(i)$V \subseteq W$ iff $I(W) \subseteq I(V)$*
*(ii)$V = W$ iff $I(V) = I(W)$.*

*Proof.* (i) Let $V \subseteq W$. Then if $f$ vanishes on $W$, it vanishes in $V$. Then let $I(W) \subseteq I(V)$. Thus, if $g \in I(W)$, then $g \in I(V)$, meaning that $W$ has all common zeros. Thus $V \subseteq W$
(ii) If $V = W$, then $V \subseteq W$, $W \subseteq V$. By (i) $I(W) = I(V)$. The other direction follows. □

## 1.5 Polynomial of One Variable

**Definition 1.5.1.** Given a nonzero polynomial $f \in k[x]$, let $f = c_0x^m + \ldots + c_m$, where $c_i \in k$, $c_0 \neq 0$, then we say $c_0x^m$ the leading term of $f$, $m$ the degree of $f$.

**Proposition 1.5.2.** *(Division Algorithm) Let $F$ be a field, $g$ a nonzero polynomial in $F[x]$. Then every $f \in F[x]$ can be written as $f = qg + r$, where $q, g \in F[x]$, and either $r = 0$ or $deg(r) < deg(g)$. Furthermore, $q, r$ are unique.*

*Proof.* We first prove the existence. If $f = 0$, then the case is trivial. If $f \neq 0$, we use induction. Let $deg(f) = n$. If $n = 1$, then $f = ax + b$, we have either $g = c$, then we can compute $q, r$ and verify that $r < g$. Assume it is always the case for case $n$. Consider case $n + 1$. We can use long division to check this result.

Now we prove uniqueness. Assume $f = gq_1 + r_1$, $f = gq_2 + r_2$. Then we have $0 = g(q_1 - q_2) + (r_1 - r_2)$. Now $g(q_1 + q_2)$ is either 0 or has a degree greater than $g$. In the second case we have a contradiction. Therefore, $q_1 = q_2$, and $r_1 = r_2$. □

**Corollary 1.5.3.** *If $F$ is a field, $f \in F[x]$ is a nonzero polynomial, then $f$ has at most $deg(f)$ roots in $F$.*

*Proof.* We use induction. when $deg(f) = 0$, the solution is trivial. Assume it holds for $deg(f) = n$. Then consider $n+1$ case. If $a$ is a root of $f$, then $f = q(x - a) + r$ by devision algorithm. But notice, $f(a) = q(a)(a - a) + r = 0$, thus $r = 0$. Thus, we observe that $q$ is a degree $n$ polynomial since $(X - a)$ is degree one. By our hypothesis, there are at most $n + 1$ roots. we are done. □

**Definition 1.5.4.** An ideal generated by one element is called a *principal ideal*. An integral domain with all ideals being principal ideals are called a *principal ideal domain* (PID).

**Corollary 1.5.5.** *If $F$ is a field, then $F[x]$ is a PID.*

*Proof.* Consider $I \subseteq F[x]$. Choose $f$ to be of minimum degree in $I$. If $I = 0$ this is trivial. Otherwise, if $g, f \in I$. Then $g = qf + r$. We know that $q \in F[x]$, thus, $qf \in I$, $r = g - qf \in I$. Then $r = 0$. Therefore, $g = qf$, meaning that the ideal is generated by $f$. □

**Definition 1.5.6.** A *greatest common divisor* of polynomials $f, g \in k[x]$ is a polynomial $h$, such that $h|g$, $h|f$, and if $x|g$, and $x|f$, then $x|h$.

Similarly, we have a similar definition for the gcd for many polynomials

**Proposition 1.5.7.** *Let $f, g \in k[x]$,*
*(i)$gcd(f, g)$ exists and is unique*
*(ii)$gcd(f, g)$ is a generator of the ideal $(f, g)$*
*(iii) Euclidean Algorithm: $gcd(f, g) = af + bg$*
*We can declare the same things with many polynomials.*

*Proof.* Since $k[x]$ is a PID, $(f, g) = (h)$. Therefore, $h|f, h|g$. If $p|f, p|g$, then let $f = ap, g = bp$. Since $h \in (f, g)$, $h = cg + df = cbp + dap$. Therefore, $p|h$. Thus $h = gcd(f, g)$. Thus we proved uniqueness, (ii). If $h', h$ are both $gcd(f, g)$, then $h|h'$ and $h'|h$. Thus $h = h'$, thus unique. Since $(f, g) = (h)$, we have the Euclidean Algorithm. □

# Chapter 2

# Notes: Grobner Bases

## 2.1 Introduction

In this chapter, we want to consider ways to find all elements in an affine variety. In a linear example, this is the reduced echelon form.

## 2.2 Orderings on Monomials

**Definition 2.2.1.** A *monomial ordering* $>$ on $k[x_1, \ldots, x_n]$ is a relation $>$ on $\mathbb{Z}^n_{\geq 0}$ with the folloiwng properties:

(i)$>$ is a total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$

(ii)If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.

(iii)$>$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$. (Every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$)

Given a monomial ordering $>$, we say that $\alpha > \beta$ or $\alpha = \beta$.

**Lemma 2.2.2.** *An order relation $>$ on $\mathbb{Z}^n_{\geq 0}$ is a well-ordering iff every strictly decreasing sequence in $\mathbb{Z}^n_{\geq 0}$: $\alpha(1) > \alpha(2) \ldots$ eventually terminates.*

*Proof.* Consider the contrapositive: $>$ is not a well-ordering iff there is an infinite strictly decreasing sequence in $\mathbb{Z}^n_{\geq 0}$. Thus, we claim is obvious.

($\Rightarrow$)If $>$ is not a well-ordering, then if $A \subset \mathbb{Z}^n_{\geq 0}$ non-empty. Pick $\alpha(1)$, by definition, there is a number $\alpha(2)$ less than $\alpha(1)$. Continue in this fashion, we get a infinite decreasing sequence.

($\Leftarrow$) By definition, it is not a well-ordering. □

**Definition 2.2.3.** (Lexicographic Order) Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be in $\mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if the leftmost nonzero entry of the vector difference $\alpha - \beta \in \mathbb{Z}^n$ is positive. We write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

**Proposition 2.2.4.** *The lex ordering on $\mathbb{Z}^n_{\geq 0}$ is a monomial ordering.*

*Proof.* (i) Since the order on $\mathbb{Z}^n_{\geq 0}$ is a total ordering, we see that $>_{lex}$ is a total ordering.

(ii)If $\alpha >_{lex} \beta$, then we have $\alpha_i - \beta_i > 0$. Then $(\alpha+\gamma)-(\beta-\gamma)$ has the nonzero entry $\alpha_i - \beta_i > 0$

(iii) We prove by contradiction. Assume it is not a well-ordering, then there is a infinite strictly descending sequence $\alpha(1) >_{lex} \alpha(2)\ldots$ of elements $\alpha(1) > \alpha(2)\ldots$. Consider first $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$, then their first entries form a nonincreasing sequence of nonnegative integers. Since $\mathbb{Z}^n_{\geq 0}$ is well-ordered, this sequence has to terminate in the first entries, say at $\alpha(l)$. Then consider elements after $\alpha(l)$, they have to form nonincreasing sequences in the later entries. Continue in this fashion, assume it all terminates at $\alpha(m)$, then we have $\alpha(m) = \alpha(m+1)$, contradiciton. □

**Definition 2.2.5.** (Graded Lex Order) Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$.

**Definition 2.2.6.** (Graded Reverse Lex Order) Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, or $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.

**Definition 2.2.7.** Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$, and $>$ a monomial order. The *multidegree* of $f$ is $\max\{\alpha \in \mathbb{Z}^n_{\geq 0} | a_\alpha \neq 0\}$. The *leading coefficient of* $f$ is $a_{multideg(f)} \in k$, and the *leading monomial* of $f$ is $x^{multideg(f)}$, and the *leading term* of $f$ is $LT(f) = LC(f) \cdot LM(f)$

## 2.3 A Division Algorithm in $k[x_1, \ldots, x_n]$

We have a division algorithm for $k[x_1, \ldots, x_n]$ as well.

**Theorem 2.3.1.** *(Division Algorithm) Let $>$ be a monomial order on $\mathbb{Z}^n_{\geq 0}$, let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Then every $f \in k[x_1, \ldots, x_n]$ can be written as $f = q_1 f_1 + \ldots + q_s f_s + r$, where $q_i, r \in k[x_1, \ldots, x_n]$, and $r$ either $0$ or a linear conbination with coeffcients in $k$, and not divisible by any leading terms of our $f_i$. We call $r$ a remainder of $f$ divided by $F$, and $\forall i, multideg(f_i) > multideg(r)$.*

## 2.4 Monomial Ideals and Dickson's Lemma

**Definition 2.4.1.** An ideal $I \subseteq k[x_1, \ldots, x_n]$ is a *monomial ideal* if there is a subset $A \subseteq \mathbb{Z}^n_{\geq 0}$ such that $I$ consists of all polynomial which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, \ldots, x_n]$. In this case, we write $I = \langle x^\alpha | \alpha \in A \rangle$

**Lemma 2.4.2.** *Let $I = \langle x^\alpha | \alpha \in A \rangle$ be a monomial ideal. Then a monomial $x^\beta \in I$ iff $x^\alpha | x^\beta$.*

*Proof.* ($\Leftarrow$) This is the definition.

($\Rightarrow$) If $x^\beta \in I$, then $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, where $h_i \in k[x_1, \ldots, x_n]$, and $\alpha(i) \in A$. If we expand this equation, we can see that $x^\alpha | x^\beta$. □

**Lemma 2.4.3.** *Let $I$ be a monomial ideal, and let $f \in k[x_1, \ldots, x_n]$. The following are equivalent:*

*(i)$f \in I$*

*(ii)Every term of $f$ lies in $I$*

*(iii) $f$ is a $k$-linear combination of the monomials in $I$.*

**Corollary 2.4.4.** *Two monomial ideals are the same iff they contain the same monomials.*

**Theorem 2.4.5.** *(Dickson's Lemma) Let $I = \langle x^\alpha | \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$ be a monomial ideal. Then $I$ has a finite basis.*

*Proof.* We prove by induction. Base case: $n = 1$, then $I$ is generated by $x_1^\alpha$. Let $\beta$ be minimal in $A$, then $\beta < \alpha, \forall \alpha \in A$. Thus, $x^\alpha | x^\beta$. Thus $I = \langle x_1^\beta \rangle$.

Assume it works for $n-1$. Consider monomials in $k[x_1, \ldots, x_{n-1}, y]$. Let $J \subseteq k[x_1, \ldots, x_{n-1}]$ be an ideal, and $I = x^\alpha y^m$, where $x^\alpha \in J$. Since $J$ is a monomial, it is finitely generated. Thus, we can consider $k[x_1, \ldots, x_{n-1}, y] = k[x_1, \ldots, x_{n-1}][y]$, thus, by base case, $I = J[y]$. Thus, $I$ is also finitely generated. □

**Corollary 2.4.6.** *Let $>$ be a relation on $\mathbb{Z}_{\geq 0}^n$ satifying:*

*(i) $>$ is a total ordering on $\mathbb{Z}_{\geq 0}^n$*

*(ii) if $\alpha > \beta$, and $\gamma \in \mathbb{Z}_{\geq 0}^n$, then $\alpha + \gamma > \beta + \gamma$*

*Then $>$ is well ordering iff $\alpha \geq 0, \forall \alpha \in \mathbb{Z}_{\geq 0}^n$.*

The proof is easy.

**Proposition 2.4.7.** *A monomial ideal $I \in k[x_1, \ldots, x_n]$ has a basis $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ with the property that $x^{\alpha(i)}$ does not divide $x^{\alpha(j)}$ for $i \neq j$. This basis is unique and is called the* minimal basis *of $I$.*

*Proof.* By Dickson's Lemma, $I$ has a finite basis of monomials. If one devides another, we ignore it. We repeat until we get a basis described.

Assume another basis. Then we observe that $x^{\alpha(i)} | x^{\beta(j)} | x^{alpha(1)}$ which is a contradiction. Or we have to have $i = 1$, thus $x^{\beta(j)} = x^{alpha(1)}$, which means that this basis is unique □

## 2.5 The Hilbert Basis Theorem and Grobner Bases

We denote by $\langle LT(I) \rangle$ the ideal generated by the elements of $LT(I)$ (The set of leading terms of nonzero elements of $I \subseteq k[x_1, \ldots, x_n]$). Notice that $\langle LT(I) \rangle$ can be larger than $\langle LT(f_1), \ldots, LT(f_s) \rangle$.

**Proposition 2.5.1.** *Let $I \subseteq k[x_1, \ldots, x_n]$ be a non-zero ideal*

*(i) $\langle LT(I) \rangle$ is a monomial ideal.*

*(ii) There are $g_1, \ldots, g_t \in I$ such that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.*

*Proof.* (i) The leading monomial generates the leading term ideal.

(ii) Since $\langle LT(I)\rangle$ is a monomial ideal, by Dickson's lemma, it is generated by finitely many basis. Therefore, $\langle LT(I)\rangle = \langle LM(g_1), \ldots, LM(g_t)\rangle$. Since each leading monomial differs from the leading term by a constant, we have $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. □

**Theorem 2.5.2.** *(Hilbert Basis Theorem) Every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a finite generating set.*

*Proof.* If $I$ is trivial, then clearly it has a finite basis. Assume $I$ is not trivial. We first put an order topology on $I$, and we find a leading term. Then $I$ has an ideal of leading terms. Thus, we have $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. We want to show that $I = \langle g_1, \ldots, g_t\rangle$. $\langle g_1, \ldots, g_t\rangle \subseteq I$ is clear. Now, if $f \in I$, then by division algorithm, $f = q_1g_1 + \ldots + q_tg_t + r$, where no term of $r$ is divisible by any of the leading terms. Now notice that $r = f - q_1g_1 - \ldots - q_ng_n \in I$, we know $r$ must be 0. Thus $f \in \langle g_1, \ldots, g_t\rangle$. Thus we have the other inclusion. □

**Definition 2.5.3.** Consider $k[x_1, \ldots, x_n]$ with an order topology. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subseteq k[x_1, \ldots, x_n]$ different from 0 is said to be a *Grobner basis (standard basis)* if $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.

**Corollary 2.5.4.** *Fix an order topology. Every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a Grobner basis. Furthermore, any Grobner basis for an ideal $I$ is a basis of $I$.*

**Definition 2.5.5.** A ring $R$ is called *Noetherian* if its ideals are generated by finitely many elements

**Definition 2.5.6.** The *ascending chain condition* of ideals: $I_1 \subseteq I_2 \subseteq I_3 \ldots$ forms a finite ascending chain ($\exists$) an $N \geq 1$ such that $I_N = I_{N+1} = \ldots$.

**Theorem 2.5.7.** *$k[x_1, \ldots, x_n]$ satisfies the accending chain condition.*

*Proof.* Given an ascending chain $I_1 \subseteq I_2 \subseteq I_3 \ldots$, consider $I = \cup_{i=1}^{\infty} I_i$. We realize that $I$ is an ideal in $k[x_1, \ldots, x_n]$. By Hilbert Basis Theorem, $I$ must have a finite generating set: $I = \langle f_1, \ldots, f_s\rangle$. But each of them need to be in one of the $I_i$. Thus we take $N = max\{i\}$. Hence, the chain stables at $N$. □

**Remark 2.5.8.** $R$ be a ring, it is Noetherian iff it satisfies the ascending chain condition.

**Definition 2.5.9.** Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. We denote $V(I) = \{(a_1, \ldots, a_n) \in k^n | f(a_1, \ldots, a_n) = 0, \forall f \in I\}$

**Proposition 2.5.10.** *$V(I)$ be an affine variety. If $I = \langle f_1, \ldots, f_s\rangle$, then $V(I) = V(f_1, \ldots, f_s)$.*

*Proof.* By Hilbert Basis Theorem, $I = \langle f_1, \ldots, f_s\rangle$. Since $f_i \in I$, if $f(a_1, \ldots, a_n) = 0, \forall f \in I$, then $f_i(a_1, \ldots, a_n) = 0$. Thus $V(I) \subseteq V(f_1, \ldots, f_s)$. If on the other hand, we can write them as a linear combination. thus the other inclusion is satisfied. □

We conclude that varieties are determined by ideals.

## 2.6 Properties of Grobner Bases

**Proposition 2.6.1.** *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let $G = \{g_1, \ldots, g_t\}$ be a Grobner basis for $I$. Then given $f \in k[x_1, \ldots, x_n]$, there is a unique $r \in k[x_1, \ldots, x_n]$ with the following:*

*(i)No term of $r$ is divisible by any of $LT(g_1), \ldots, LT(g_t)$.*

*(ii) There is $g \in I$ such that $f = g + r$*

*Where $r$ is the remainder on division of $f$ by $G$.*

*Proof.* By division algorithem, $f = q_1 g_1 + \ldots + q_t g_t + r$, where $r$ satisfies (i). By letting $g = q_1 g_1 + \ldots + q_t g_t$ we satisfies (ii). Now we need to prove uniqueness.

Let $f = g + r = g' + r'$. Then $r - r' = g - g' \in I$. If $r \neq r'$, $LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Thus $r - r'$ is divisible by some $LT(g_i)$, contradiction. Thus uniqueness. □

**Definition 2.6.2.** The remainder $r$ above is called the *normal form* of $f$.

**Corollary 2.6.3.** *Let $G = \{g_1, \ldots, g_t\}$ be a Grobner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$, let $f \in k[x_1, \ldots, x_n]$. Then $f \in I$ iff $r$ on division of $f$ by $G$ is 0.*

**Definition 2.6.4.** We will write $\overline{f}^F$ for the remainder on division of $f$ by the ordered $s$-tuple $F = (f_1, \ldots, f_s)$. If $F$ is a Grobner basis for $\langle f_1, \ldots, f_s \rangle$, then we can regard $F$ as a set by prop 2.5.1

Now we are going to discuss how to tell if a basis is a Grobner basis.

**Definition 2.6.5.** Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials. If $multideg(f) = \alpha, multideg(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_1, \beta_i)$ for each $i$. We call $x^\gamma$ the *least common multiple* of $LM(f)$ and $LM(g)$, written as $x^\gamma = lcm(LM(f), LM(g))$. And the *S-polynomial* of $f$ and $g$ is the combination

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$$

**Lemma 2.6.6.** *Suppose we have $\sum_{i=1}^s p_i$, where $multideg(p_i) = \delta \in \mathbb{Z}^n_{\geq 0}$. If $multideg(\sum_{i=1}^s p_i) < \delta$, then it is a linear combination of the S-polynomials $S(p_j, p_l)$ for $1 \leq j, l \leq s$, with each $S(p_j, p_l)$ has multidegree $< \delta$*

*Proof.* Let $d_i = LC(p_i)$, so that $d_i x^\delta$ is the leading term of $p_i$. Since $\sum_{i=1}^s p_i$ has a smaller degree, we see that $\sum_{i=1}^s d_i = 0$. Since $p_i$ and $p_j$ have the same $LM$, the $S$-polynomial $S(p_i, p_j) = \frac{1}{d_i} p_i - \frac{1}{d_j} p_j$. Therefore $\sum_{i=1}^{s-1} d_1 S(p_i, p_s) = p_1 + \ldots + p_{s-1} - \frac{1}{d_s}(d_! + \ldots + d_{s-1} p_s = p_1 + \ldots + p_{s-1} + p_s$. Thus the sum is a sum of $S$-polynomials, and it has multidegree $< \delta$. □

**Theorem 2.6.7.** *(Buchberger's Criterion) Let $I$ be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of $I$ is a Grobner basis of $I$ iff $\forall i \neq j$, the remainder on division of $S(g_i, g_j)$ by $G$ is zero.*

*Proof.* ($\Rightarrow$) By the former Corollary.

($\Leftarrow$) Let $f \in I$ nonzero. $f = \sum_{i=1}^{t} h_i g_i, h_i \in k[x_1, \ldots, x_n]$. Thus we know $multideg(f) \leq \max(multideg(h_i g_i))$ for $h_i g_i \neq 0$. Let $\delta = \max(multideg(h_i g_i))$ be minimal. Thus, $multideg(f) \leq \delta$. If we take equal sign, then $LT(f) \in \langle g_1 \ldots, g_t \rangle$. Thus we are done. Assume not equal. Then we decrease $\delta$ by using the remainder equals to 0. $\square$

## 2.7 Buchberger;s Algorithm

**Theorem 2.7.1.** *Let $I = \langle f_1, \ldots, f_s \rangle \neq 0$ by a polynomial ideal. Then a Grobner basis for $I$ can be constructed in a finite number of steps in an algorithm. (Basically find the remainder of the S-polynomial and if it is 0, the algorithm terminates, or we add the remainder into the basis and do it again)*

We then talk about examples. But with this theorem, usually the basis computed are bigger than necessary

**Lemma 2.7.2.** *Let $G$ be a Grobner basis of $I \subseteq k[x_1, \ldots, x_n]$. Let $p \in G$ be a polynomial such that $LT(p) \in \langle LT(G - \{p\}) \rangle$. Then $G - \{p\}$ is also a Grobner basis for $I$.*

Now the same example but reduced to minimal Grobner basis.

**Definition 2.7.3.** A *reduced Grobner basis* for a polynomial ideal $I$ is a Grobner basis $G$ for $I$ such that

(i) $LC(p) = 1, \forall p \in G$

(ii) $\forall p \in G$, no monomial of $p$ lies in $\langle LT(G - \{p\}) \rangle$

**Theorem 2.7.4.** *Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, $I$ has a reduced Grobner basis, and the reduced Grobner basis is unique.*

Notice there is a connect between Buchberger's Algorithm and Gauss elimination.

## 2.8 First Applications of Grobner Bases

We see examples in solving the ideal membership problem, the problem of solving polynomial equations, and the implicitization problem

# Bibliography

[1] Cox, Little, O'Shea, *Ideals, Varieties and Algorithms* New York: Springer-Verlag, 2014