A note on Gröbner bases

Ray D. Sameshima

2015/02/10 $\sim$ 2016/11/04 17:38

Contents

Chapter -1

Preface

-1.1 Reference

1. Ideals, Varieties, and Algorithms Our source book.
   An Introduction to Computational Algebraic Geometry and Commutative Algebra

   Authors: David Cox, John Little, Donal O'Shea
   ISBN: 978-0-387-35650-1 (Print) 978-0-387-35651-8 (Online)

2. nLab

   `https://ncatlab.org/`

3. Learn You a Haskell for Great Good!

   `http://learnyouahaskell.com/chapters`

4. ASCENDING CHAIN CONDITION DENNIS S. KEELER

   `http://www.users.miamioh.edu/keelerds/705/chain.pdf`

5. A basic linear algebra(Masayoshi Nagata, et al) (written in Japanese)

6. Maxima, a Computer Algebra System

   `http://maxima.sourceforge.net`

Chapter 0

Basics

We will assume living (working) knowledge on mathematics.

0.1 Set theoretical gadgets

Our set theory is ZFC.

0.1.1 Binary relations

A binary relation ρ on a set S is a function[1]

```
rho :: S -> S -> Bool
```
(1)

i.e., $\forall a, b \in S$, we can determine whether $a\rho b\,(= \rho(a,b))$ is `True` or `False`.

A set theoretical implementation is

$$\rho \subset A \times A, \tag{2}$$

and

$$a\rho b :\Leftrightarrow (a,b) \in \rho. \tag{3}$$

[1] This is Haskell type annotation. Haskell is pure, lazy, functional programming language. www.haskell.org

0.1.2 Partially ordered sets

Let $\leq$ be a binary relation on a set S. A structured set $(S, \leq)$ is a partially ordered set iff

$$\begin{aligned} \forall a \in S, a \leq a &\qquad \text{(reflexivity)} \qquad (4) \\ \forall a, b, c \in S, (a \leq b, b \leq c \Rightarrow a \leq c) &\qquad \text{(transitivity)} \qquad (5) \\ \forall a, b \in S, (a \leq b \leq a \Rightarrow a = b) &\qquad \text{(antisymmetry)} \qquad (6) \end{aligned}$$

0.1.3 Totally ordered sets

The partial order $(S, \leq)$ is called total (linear) order iff

$$\forall a, b \in S, \text{either } a \leq b \text{ or } b \leq a \tag{7}$$

holds. That is, all two elements are comparable in a totally ordered set.

0.1.4 Well-ordered sets

A partially ordered set $(S, \leq)$ is well-ordered iff an arbitrary subset $\forall T \subset S$ has a minimum element. That is,

$$\forall T \subset S, \exists t_0 \in T \text{ s.t. } \forall t \in T, t_0 \leq t. \tag{8}$$

Well-ordered sets are totally ordered

A well-ordered set $(S, \leq)$ is indeed totally ordered, since an arbitrary pair

$$\{a, b\} \subset S \tag{9}$$

has the minimum, that is, either $a \leq b$ or $b \leq a$.

0.1.5 Rings

A ring $(R, +, *)$ is a structured set with two binary operations

```
(+) :: R -> R -> R          (10)
(*) :: R -> R -> R          (11)
```

satisfying the following 3 (ring) axioms:

1. $(R, +)$ is an abelian, i.e., commutative group, i.e.,

$$\forall a, b, c \in R, (a+b)+c = a+(b+c) \quad \text{(associativity for } +) \quad (12)$$

$$\forall a, b, \in R, a+b = b+a \quad \text{(commutativity)} \quad (13)$$

$$\exists 0 \in R, \text{ s.t. } \forall a \in R, a+0 = a \quad \text{(additive identity)} \quad (14)$$

$$\forall a \in R, \exists(-a) \in R \text{ s.t. } a+(-a) = 0 \quad \text{(additive inverse)} \quad (15)$$

2. $(R, *)$ is a monoid, i.e.,

$$\forall a, b, c \in R, (a*b)*c = a*(b*c) \quad \text{(associativity for } *) \quad (16)$$

$$\exists 1 \in R, \text{ s.t. } \forall a \in R, a*1 = a = 1*a \quad \text{(multiplicative identity)} \quad (17)$$

3. Multiplication is distributive w.r.t addition, i.e., $\forall a, b, c \in R$,

$$a*(b+c) = (a*b)+(a*c) \quad \text{(left distributivity)} \quad (18)$$

$$(a+b)*c = (a*c)+(b*c) \quad \text{(right distributivity)} \quad (19)$$

0.1.6 Fields

A field is a ring $(\mathbb{K}, +, *)$ whose non-zero elements form an abelian group under multiplication, i.e.,

$$\forall r \in \mathbb{K}, r \neq 0 \Rightarrow \exists r^{-1} \in \mathbb{K} \text{ s.t. } r*r^{-1} = 1 = r^{-1}*r. \quad (20)$$

A field $\mathbb{K}$ is a finite field iff the underlying set $\mathbb{K}$ is finite. A field $\mathbb{K}$ is called infinite field iff the underlying set is infinite.

0.1.7 Equivalence relations

An equivalence relation $\sim$ on a set S is a binary relation which is reflexive, symmetric, and transitive:

$$\forall a \in S, a \sim a \quad \text{(reflexivity)} \quad (21)$$

$$\forall a, b \in S, (a \sim b \Rightarrow b \sim a) \quad \text{(symmetry)} \quad (22)$$

$$\forall a, b, c \in S, (a \sim b, b \sim c \Rightarrow a \sim c) \quad \text{(transitivity)} \quad (23)$$

Then the subset

$$[a] := \{x \in S | \, x \sim a\} \quad (24)$$

is called the equivalence class of a.

Partitions of disjoint subsets

An equivalence relation $\sim$ on S partitions S into disjoint subsets of equivalence classes.

$\forall a \in S$ is in the equivalence class of itself, since $\sim$ is reflexive,

$$a \sim a \Rightarrow a \in [a]. \tag{25}$$

They are disjoint; if there exists some elements that is shared by two equivalent classes,

$$x \in [a] \text{ and } x \in [b] \Rightarrow x \sim a \text{ and } x \sim b. \tag{26}$$

Since $\sim$ is transitive, we have

$$a \sim b \Rightarrow [a] = [b]. \tag{27}$$

■

Note

This partition is a function from S to the subsets of S:

$$[] : S \to (2^S - \emptyset); a \mapsto [a]. \tag{28}$$

0.2 The fundamental theorem in algebra

Here we review the fact that $\mathbb{C}$ of complex numbers is algebraically closed.

0.2.1 (ϵ-N) convergence

For simplicity, consider $\mathbb{C}$ of complex numbers and a function

$$z : \mathbb{N} \to \mathbb{C}; z \mapsto z_n \tag{29}$$

so called a sequence. This z converges to $c \in \mathbb{C}$ iff

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ s.t. } (\forall n \geq N, |c - z_n| < \epsilon), \tag{30}$$

where $\forall a, b \in \mathbb{R}$,

$$|a + ib| := \sqrt{a^2 + b^2} \tag{31}$$

is the euclidean distance.

0.2.2 (Sequence) continuity

Consider a $\mathbb{C}$-valued sequence

$$z : \mathbb{N} \to \mathbb{C}; z \mapsto z_n \tag{32}$$

which converges to $c \in \mathbb{C}$:

$$\lim_{n\to\infty} z_n = c. \tag{33}$$

A function $f : \mathbb{C} \to \mathbb{C}$ is continuous at $c \in \mathbb{C}$ iff

$$f(c) = f\left(\lim_{n\to\infty} z_n\right) = \lim_{n\to\infty} f(z_n). \tag{34}$$

A continuous function is a function which is continuous at every point.

0.2.3 Lemma (An extreme value theorem)

Let

$$C_1 := \left\{ z \,\middle|\, z \in \mathbb{C}, |z|^2 \leq 1 \right\} \tag{35}$$

be a unit circle and its inside area. An arbitrary function

$$f : C_1 \to \mathbb{R} \tag{36}$$

has the maximum and minimum.

Proof

It suffices to show the maximum case, and we prove by contradiction.

Suppose there is no maximum; that is either

1. (no upper limit) it diverges, i.e.,

$$\forall N \in \mathbb{N}, \exists z \in C_1 \text{ s.t. } f(z) > N, \tag{37}$$

or

2. (upper limit) there is NO $z \in C_1$ s.t. $f(z) = \alpha$ but

$$\forall n \in \mathbb{N}, f(z_n) < \alpha \tag{38}$$

and[2]

$$\lim_{n\to\infty} f(z_n) = \alpha. \tag{40}$$

holds.

Let us construct a sequence $p : \mathbb{N} \to C_1$ in C_1 by if there is no upper limit, put p_n s.t.

$$f(p_n) > n, \tag{41}$$

else if α is the upper limit, put p_n s.t.

$$\alpha - \frac{1}{n} < f(p_n) < \alpha. \tag{42}$$

Then we get a sequence[3]

$$p : \mathbb{N} \to C_1. \tag{43}$$

Next, consider the $\frac{1}{2} \times \frac{1}{2}$ squares determined by

$$y = \frac{n}{2}, x = \frac{n}{2}. \tag{44}$$

Since C_1 is covered by a finite number(=16) of these squares, and at least one of which has infinite number of p's, call it S_1. At least one of the quadrants of S_1 contains infinite number of p's, call it S_2. By induction, we get a sequence of squares

$$S_n|_{n\in\mathbb{N}} \tag{45}$$

s.t., $\forall n \in \mathbb{N}$, S_n is a $\frac{1}{2^n} \times \frac{1}{2^n}$ square and each S_n contains infinite p's.

Let us pick a sub sequence $q : \mathbb{N} \to C_1$ of p by

1. choose $q_1 \in S_1$ from arbitrary p's in S_1, say for some n,

$$q_1 := p_n. \tag{46}$$

[2] We sometimes write it as

$$f(z_n) \to \alpha - 0. \tag{39}$$

[3] Here we have used the Axiom of choice.

2. let $i \geq 1$ and from

$$q_1, \cdots, q_{i-1} = p_m, \tag{47}$$

of some $m \in \mathbb{N}$, pick q_i from

$$\{p_j \in S_i | j > m\} \tag{48}$$

This sequence $q : \mathbb{N} \to C_1$ satisfies for $j > i$,

$$q_j, q_i \in S_i \tag{49}$$

and its euclidean distance is smaller than

$$\sqrt{2}\frac{1}{2^i} \tag{50}$$

of diagonal. So, q converges to a point in C_1

$$\lim_{n\to\infty} q_n =: q_\infty \in C_1, \tag{51}$$

and since f is continuous,

$$f(q_\infty) = \lim_{n\to\infty} f(q_n). \tag{52}$$

If 1st (divergent) case holds, the right hand side is infinity,contradiction. Else 2nd (upper limit) case holds, the right hand side is α, contradiction.

Therefore, all function $f : C_1 \to \mathbb{R}$ has the maximum, and minimum.

■

0.2.4 The fundamental theorem in algebra

An arbitrary $\mathbb{C}$-coefficients n degree polynomial

$$a_n * x^n + a_{n-1} * x^{n-1} + \cdots + a_0 = 0, a_n \neq 0, a_i|_i \in \mathbb{C} \tag{53}$$

has a solution in $\mathbb{C}$. This means that $\mathbb{C}$ is algebraically closed.

Proof

Suppose there is no solution. Define

$$F : \mathbb{C} \to \mathbb{R} \tag{54}$$

by

$$F(x) := \left|a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0\right|. \tag{55}$$

We can choose a large $R' > 0$ and $|x| > R'$ s.t.[4]

$$\left|\frac{a_{n-1}}{x} + \cdots + \frac{a_0}{x^n}\right| < \frac{|a_n|}{2}. \tag{56}$$

Then $\forall |x| > R'$,

$$\begin{aligned} F(x) &= |x|^n * \left|a_n + \frac{a_{n-1}}{x} + \cdots + \frac{a_0}{x^n}\right| && (57)\\ &\geq |x|^n * \left(|a_n| - \left|\frac{a_{n-1}}{x} + \cdots + \frac{a_0}{x^n}\right|\right) && (58)\\ &> |x|^n \frac{|a_n|}{2} && (59)\end{aligned}$$

and[5] we also can find $R \geq R'$ s.t.

$$\forall |x| > R, F(x) > F(0), \tag{62}$$

since $F(0) = a_0$ is a constant.

So if we define

$$C_R := \{x \in \mathbb{C} | |x| \leq R\}, \tag{63}$$

then

$$x \notin C_R \Rightarrow F(x) > F(0). \tag{64}$$

Therefore, if $F(x)$ has a minimum in C_R, this is indeed the minimum in $\mathbb{C}$.

Above lemma in §0.2.3 guarantees that $F(x)$ has a minimum in C_R, and $F(x)$ has the minimum in $\mathbb{C}$:

$$\min F(x)\big|_x = \alpha \geq 0. \tag{65}$$

[4] Since this left hand side is decreasing if $|x|$ becomes larger and larger.

[5] We have used a triangle inequality

$$|a + b| \leq |a| + |b| \tag{60}$$

and its consequence

$$|a + b| - |b| \leq |b| \Leftrightarrow |c - b| \geq |c| - |b|. \tag{61}$$

Since this is not a solution for eq.(53), α is positive definite. Now suppose F has this minimum $\alpha > 0$ at p:

$$F(p) = \alpha > 0. \tag{66}$$

Consider

$$g(x) := a_n(x+p)^n + a_{n-1}(x+p)^{n-1} + \cdots + a_0. \tag{67}$$

Then $|g(x)|$ has its minimum $g(0) = \alpha$. Define $h(x)$ by

$$\begin{aligned} h(x) &:= g(x)/\alpha && (68)\\ &= g(x)/(a_n p^n + a_{n-1}p^{n-1} + \cdots + a_0) && (69)\\ &= 1 + b_1 x + \cdots b_n x^n. && (70) \end{aligned}$$

Consider $b_1, \cdots, b_n$, and let

$$b_s \tag{71}$$

be the first nonzero coefficient. Define

$$K := \max\{|b_{s+1}|, \cdots, |b_n|\} \tag{72}$$

We can find a small $r > 0$ which satisfies both

$$1 - |b_s| r^s > 0 \tag{73}$$

and

$$0 < |b_s| r^s - \frac{K r^{s+1}}{1-r} < 1 \tag{74}$$

If we write

$$b_s = |b_s| * e^{i\theta} \tag{75}$$

and define

$$q := r * e^{i(\pi-\theta)/s} \tag{76}$$

then $b_s q^s = |b_s|e^{i\theta} * r^s e^{i(\pi-\theta)} = |b_s|r^s e^{i\pi} = -|b_s|r^s$ and

$$\begin{aligned}
|h(q)| &= |1 + b_s q^s + \cdots + b_n q^n| && (77)\\
&\le 1 + |b_s q^s| + |b_{s+1} q^{s+1} + \cdots + b_n q^n| && (78)\\
&< 1 - |b_s| r^s + |b_{s+1}| r^{s+1} + \cdots + |b_n| r^n && (79)\\
&\le 1 - |b_s| r^s + K\left(r^{s+1} + \cdots + r^n\right) && (80)\\
&= 1 - |b_s| r^s + K r^{s+1} \frac{1 - r^{n-s-1}}{1-r} && (81)\\
&< 1 - |b_s| r^s + \frac{K r^{s+1}}{1-r} && (82)\\
&< 1. && (83)
\end{aligned}$$

Since

$$|h(q)| = \frac{F(q+p)}{F(q)} < 1, \tag{84}$$

we get

$$F(q+p) < F(p) = \alpha, \tag{85}$$

but it contradicts that α is the minimum of F.
■ minimality

0.3 Numbers; recipes without arithmetics

Here we review $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. If the readers are already familiar with (ZFC axiomatic) set theory and the set theoretic implementation of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, you can skip this section.

0.3.1 Natural numbers $\mathbb{N}$

Here is a recursive implementation of natural numbers (Peano):

$$\begin{aligned}
0 &:= \emptyset && (86)\\
n+1 &:= n \cup \{n\} && (87)
\end{aligned}$$

0.3.2 Integers $\mathbb{Z}$

The set of integers is complete under subtraction:

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/S,$$

where the equivalence relation S is given by

$$(m_1, m_2)S(n_1, n_2) :\Leftrightarrow m_1 + n_2 = m_2 + n_1. \tag{88}$$

I.e., a negative integer $(-m) \in \mathbb{Z}$ of some $m \in \mathbb{N}$ is represented by, for example,

$$(0, m). \tag{89}$$

0.3.3 Rational numbers $\mathbb{Q}$

The set of rational numbers is complete under non-zero division:

$$\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} - \{0\}))\,/F, \tag{90}$$

where the equivalence relation F is given by

$$(a, b)F(c, d) :\Leftrightarrow a * d = b * c. \tag{91}$$

Usually we denote

$$\frac{a}{b} := (a, b) \in \mathbb{Q}. \tag{92}$$

0.3.4 Real numbers $\mathbb{R}$

The set of real numbers should satisfy the Axiom of continuity, but before state it, let us define an important tool, the cut.

Dedekind cut of $\mathbb{Q}$

A Dedekind cut is a pair of non-empty subsets of $\mathbb{Q}$

$$(A_-, A_+) \in (2^{\mathbb{Q}} - \{\emptyset\})^2 \tag{93}$$

with

$$A_- \cup A_+ = \mathbb{Q} \tag{94}$$

and

$$x \in A_-, y \in A_+ \Rightarrow x < y. \tag{95}$$

Definition of $\mathbb{R}$

There are three possibilities

$$\nexists \max A_-, \exists \min A_+ \tag{96}$$
$$\exists \max A_-, \nexists \min A_+ \tag{97}$$
$$\nexists \max A_-, \nexists \min A_+ \tag{98}$$

Here is a preliminary definition of $\mathbb{R}$:[6]

$$\mathbb{R} := \{(A_-, A_+) | \, \text{Dedekind cut with}(97), (98)\} \tag{99}$$

We define a total order $\leq$ as follows. Let

$$\alpha := (A_-, A_+), \beta := (B_-, B_+) \in \mathbb{R} \tag{100}$$

then we define

$$\alpha \leq \beta :\Leftrightarrow A_- \subset B_-. \tag{101}$$

The Axiom of continuity

A cut of $\mathbb{R}$

$$(A, B) \tag{102}$$

with

$$A \cup B = \mathbb{R} \tag{103}$$

and

$$x \in A, y \in B \Rightarrow x < y \tag{104}$$

satisfies either

$$\exists \min A, \nexists \max B \tag{105}$$

or

$$\nexists \min A, \exists \max B. \tag{106}$$

[6] Alternatively, we can define $\mathbb{R}$ be the set of all Dedekind cuts identifying eq.(96) and eq.(97).

Check

We prove that our $\mathbb{R}$ satisfies the Axiom of continuity. Let

$$\{\alpha_\lambda\}_{\lambda\in\Lambda} \tag{107}$$

be bounded subspaces of $\mathbb{R}$, and

$$\alpha_\lambda := (A_-^\lambda, A_+^\lambda). \tag{108}$$

Now

$$\begin{aligned} \alpha &:= (A_-, A_+) && (109)\\ A_- &:= \bigcup_{\lambda\in\Lambda} A_-^\lambda && (110)\\ A_+ &:= \mathbb{Q} - A_- && (111) \end{aligned}$$

is an upper bound of $\{\alpha_\lambda\}_{\lambda\in\Lambda}$, since $\forall\lambda\in\Lambda$,

$$A_-^\lambda \subset A_- \Leftrightarrow \alpha_\lambda \le \alpha \tag{112}$$

by definition.

Indeed this α is the minimum of upper bound of $\{\alpha_\lambda\}_{\lambda\in\Lambda}$, i.e., the supremum: if

$$\beta := (B_-^\lambda, B_+^\lambda) \tag{113}$$

is another upper bound of $\{\alpha_\lambda\}_{\lambda\in\Lambda}$, then

$$\forall\lambda\in\Lambda, A_-^\lambda \subset B. \tag{114}$$

This means

$$A_- \subset B_- \Leftrightarrow \alpha \le \beta. \tag{115}$$

Therefore, if (A, B) is a cut of $\mathbb{R}$, then $A \subset \mathbb{R}$ has the supremum $\alpha \in \mathbb{R}$:

$$\alpha := \sup A \in \mathbb{R}. \tag{116}$$

Finally we show that either $\alpha = \max A$ or $\alpha = \max B$. If $\alpha \ne \max A$, then

$$\alpha \in B. \tag{117}$$

By definition, $\forall\beta \in B$ is an upper bound of α:

$$\alpha \le \beta, \tag{118}$$

that is

$$\alpha = \min B. \tag{119}$$

■

0.3.5 Complex numbers $\mathbb{C}$

Let us define

$$\mathbb{C} := (\mathbb{R} \times \mathbb{R}, +, *), \tag{120}$$

where

$$\begin{aligned} (a, b) + (c, d) &:= (a + c, b + d) && (121) \\ (a, b) * (c, d) &:= (a * c - b * d, a * d + b * c). && (122) \end{aligned}$$

Note that

$$(0, 1) * (0, 1) := (-1, 0). \tag{123}$$

Usually we denote

$$a + ib := (a, b) \in \mathbb{C}. \tag{124}$$

Chapter 1

Geometry, Algebra, and algorithms

Let $\mathbb{K}$ be an arbitrary fields. We will treat polynomial ring in n variables $(x_1, \cdots, x_n)$ with $\mathbb{K}$ coefficients:[1]

$$\mathbb{K}[x_1, \cdots, x_n]. \tag{1.1}$$

We will introduce affine varieties, which are sets defined by polynomial equations.

1.1 Polynomials and Affine space

1.1.1 Monomials

A monomial in $x_1, \cdots, x_n$ is a product of the form

$$x_1^{\alpha_1} * \cdots * x_n^{\alpha_n}, \tag{1.2}$$

where

$$\alpha_1, \cdots, \alpha_n \in \mathbb{N}. \tag{1.3}$$

The total degree of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$.

When every αs zero, then we write

$$x_1^0 * \cdots * x_n^0 = 1. \tag{1.4}$$

[1] We will define this set in eq.(1.9).

1.1.2 Multi index notation

We write a monomial using multi index notation

$$x^{\alpha} := x_1^{\alpha_1} * \cdots * x_n^{\alpha_n}, \tag{1.5}$$

and the total degree

$$|\alpha| := \alpha_1 + \cdots + \alpha_n. \tag{1.6}$$

1.1.3 Polynomials

A polynomial $f(x) = f(x_1, \cdots, x_n)$ is a finite linear combination of monomials:

$$f(x) = \sum_{\alpha} c_{\alpha} * x^{\alpha}, \tag{1.7}$$

where $\forall c_{\alpha} \in \mathbb{K}$ is called coefficient of monomial x^{α}.

For nonzero coefficient $c_{\alpha} \neq 0$,

$$c_{\alpha} * x^{\alpha} \tag{1.8}$$

is called a term (of $f(x)$).

The total degree of $f(x)$ is given by the maximum of $|\alpha|$ (of nonzero coefficients).

We write

$$\mathbb{K}[x_1, \cdots, x_n] := \left\{ f(x) = \sum_{\alpha} c_{\alpha} * x^{\alpha} \middle| \forall c_{\alpha} \in \mathbb{K} \right\} \tag{1.9}$$

1.1.4 Affine spaces

Let $\mathbb{K}$ be a field and $n \in \mathbb{N}$. The n dim affine space over $\mathbb{K}$ is the set

$$\mathbb{K}^n := \{ (a_1, \cdots, a_n) | \, a_1, \cdots, a_n \in \mathbb{K} \}. \tag{1.10}$$

1.1.5 Polynomials as functions

A polynomial

$$f(x) = \sum_{\alpha} c_{\alpha} * x^{\alpha} \tag{1.11}$$

can be seen as a function

$$f : \mathbb{K}^n \to \mathbb{K} \tag{1.12}$$

which is defined by

$$a := (a_1, \cdots, a_n) \overset{f}{\mapsto} f(a) := \sum_{\alpha} c_\alpha * a^\alpha. \tag{1.13}$$

That is, the function f replace every x_i by a_i in the expression for $f(x)$.

1.2 Affine Varieties

Affine varieties are higher curves and higher surfaces defined by polynomial equations.

1.2.1 Definition of affine varieties

Let $f_1(x), \cdots, f_s(x) \in \mathbb{K}[x_1, \cdots, x_n]$. Then

$$\mathbb{V}(f_1, \cdots, f_s) := \{ a := (a_1, \cdots, a_n) \in \mathbb{K}^n | \, f_i(a) = 0, 1 \leq \forall i \leq s \}. \tag{1.14}$$

is the affine variety defined by $f_1, \cdots, f_s$.

Thus, an affine variety $\mathbb{V}(f_1, \cdots, f_s)$ is the set of all solutions of the system of equations (for x):

$$f_1(x) = 0, \cdots, f_s(x) = 0. \tag{1.15}$$

1.2.2 Intersection and union of varieties

Let $V, W \subset \mathbb{K}^n$ be

$$V := \mathbb{V}(f_1, \cdots, f_s) \tag{1.16}$$
$$W := \mathbb{V}(g_1, \cdots, g_t) \tag{1.17}$$

of varieties. Then

$$V \cap W = \mathbb{V}(f_1, \cdots, f_s, g_1, \cdots, g_t) \tag{1.18}$$
$$V \cup W = \mathbb{V}\left(f_i * g_j | \, 1 \leq i \leq s, 1 \leq j \leq t \right) \tag{1.19}$$

Proof

1. $(V \cap W)$ The 1st equation holds since

$$a \in V \cap W \Leftrightarrow f(a) = 0 \text{ and } g(a) = 0 \Leftrightarrow a \in \mathbb{V}(f_1, \cdots, g_t). \tag{1.20}$$

2. $(V \cup W)$ Let us start $\subset$-direction. If $a \in V$, i.e.,

$$f_1(a) = \cdots = f_s(a) = 0. \tag{1.21}$$

Then $\forall i, j$,

$$f_i * g_j = 0. \tag{1.22}$$

That is

$$a \in \mathbb{V}\left(f_i * g_j | \, 1 \le i \le s, 1 \le j \le t \right), \tag{1.23}$$

and

$$V \subset \mathbb{V}\left(f_i * g_j | \, 1 \le i \le s, 1 \le j \le t \right). \tag{1.24}$$

This implies

$$V \cup W \subset \mathbb{V}\left(f_i * g_j | \, 1 \le i \le s, 1 \le j \le t \right). \tag{1.25}$$

For $\supset$-direction. Take

$$a \in \mathbb{V}\left(f_i * g_j | \, 1 \le i \le s, 1 \le j \le t \right). \tag{1.26}$$

If $a \in V$ then

$$a \in V \subset V \cup W \tag{1.27}$$

and done. If $a \notin V$, then there exists some i_0 s.t.

$$f_{i_0}(a) \neq 0. \tag{1.28}$$

However, $\forall i, j$,

$$f_i(a) * g_j(a) = 0 \tag{1.29}$$

implies

$$g_j(a) = 0, \forall j, \tag{1.30}$$

and $a \in W$. Therefore

$$a \in W \subset V \cup W. \tag{1.31}$$

■

1.3 Parameterizations of Affine Varieties

1.3.1 Rational functions

Let $f(x)$ be an arbitrary, and $g(x)$ be non-zero polynomials.

$$f(x), g(x)(\neq 0) \in \mathbb{K}[x_1, \cdots, x_n]. \tag{1.32}$$

A rational function in $(x_1, \cdots, x_n)$ with $\mathbb{K}$ coefficients is a quotient

$$f/g : \mathbb{K}^n \to \mathbb{K}; a \mapsto \frac{f(a)}{g(a)}. \tag{1.33}$$

The equality is given by

$$\begin{aligned} f/g = h/k \quad &:\Leftrightarrow \quad k * f = g * h && (1.34) \\ &\Leftrightarrow \quad k(x) * f(x) = g(x) * h(x), \forall x \in \mathbb{K}. && (1.35) \end{aligned}$$

1.4 Ideals

1.4.1 Ideals

A subset $I \subset \mathbb{K}[x_1, \cdots, x_n]$ is an ideal (or a polynomial ideal) iff

$$\begin{aligned} 0 &\in I && (1.36) \\ \forall f(x), g(x) \in I, f(x) + g(x) &\in I && (1.37) \\ \forall f(x) \in I, h(x) \in \mathbb{K}[x_1, \cdots, x_n], h(x) * f(x) &\in I. && (1.38) \end{aligned}$$

1.4.2 Generators of an ideal

A set of polynomials generate an ideal:

$$\langle f_1, \cdots, f_s \rangle := \left\{ \sum_i h_i(x) * f_i(x) \middle| h_i \in \mathbb{K}[x_1, \cdots, x_n] \right\} \tag{1.39}$$

We call it an ideal generated by $f(x)$'s.

1.5 Polynomials of One(1) Variable

Consider univariate polynomials

$$\mathbb{K}[x]. \tag{1.40}$$

1.5.1 Leading terms

Given nonzero polynomial $f(x) \in \mathbb{K}[x]$, let

$$f(x) = a_m * x^m + \cdots + a_1 * x + a_0, \tag{1.41}$$

where $a_i \in \mathbb{K}$ and $a_m \neq 0$. Then

$$m = \deg(f) \tag{1.42}$$

and

$$a_m * x^m \tag{1.43}$$

is the leading term of f:

$$LT\,(f(x)) = a_m * x^m. \tag{1.44}$$

1.5.2 A total order $\leq$ in one variable $\mathbb{K}[x]$

If $f(x), g(x) \in \mathbb{K}[x]$ are nonzero polynomials, then

$$\deg(f) \leq \deg(g) \Leftrightarrow LT\,(f(x)) \text{ divides } LT\,(g(x))\,. \tag{1.45}$$

This order is essentially the total order in $(\mathbb{N}, \leq)$, so we can define an totally ordered $(\mathbb{K}[x], \leq)$ by

$$f(x) \leq g(x) :\Leftrightarrow \deg(f) \leq \deg(g). \tag{1.46}$$

We write

$$f(x) > g(x) \tag{1.47}$$

for

$$\begin{aligned} \neg\,(f(x) \leq g(x)) \quad &:\Leftrightarrow \quad \neg\,(\deg(f) \leq \deg(g)) && (1.48)\\ &\Leftrightarrow \quad \deg(f) \not\leq \deg(g) && (1.49)\\ &\Leftrightarrow \quad \deg(f) > \deg(g). && (1.50) \end{aligned}$$

1.5.3 The Division Algorithm in 1 variable

Let $g(x) \in \mathbb{K}[x]$ be a nonzero polynomial. Then $\forall f(x) \in \mathbb{K}[x]$, $\exists q(x), r(x) \in \mathbb{K}[x]$ s.t.

$$f(x) = q(x) * g(x) + r(x) \tag{1.51}$$

and either

$$r = 0 \tag{1.52}$$

or

$$\deg(r) < \deg(g). \tag{1.53}$$

There is an algorithm that can find unique $q(x)$ and $r(x)$.

Pseudo code

Here is our pseudo (Pascal like) code:

```
Input:  f,g
Output: q,r

q := 0
r := f
WHILE r /= 0 AND LT(g) divides LT(r) DO
  q := q + LT(r) / LT(g)
  r := r - (LT(r) / LT(g)) * g
```

Proof

First, we shall prove that r and q are unique. If we assume that there are two expressions

$$q_1(x) * g(x) + r_1(x) = f(x) = q_2(x) * g(x) + r_2(x). \tag{1.54}$$

If $r_1 = 0$ and $r_2 \neq 0$, then

$$r_2(x) = (q_1(x) - q_2(x)) * g(x). \tag{1.55}$$

If $q_1(x) \neq q_2(x)$ then we can divide $r_2(x)$ by $g(x)$; contradiction (see eq.(1.53)), So $r_1 = 0$ requires $r_2 = 0$ and $q_1 = q_2$.

Else both $r_1(x)$ and $r_2(x)$ are nonzero, without loss of generality, we can put $\deg(r_1) \leq \deg(r_2)$ and eq.(1.53) holds: $\deg(r_2) < \deg(g)$.

$$\deg(r_1) \leq \deg(r_2) < \deg(g). \tag{1.56}$$

From eq.(1.54), we have

$$r_2 - r_1 \;=\; (q_1 - q_2) * g. \tag{1.57}$$

Therefore, if $r_2 \neq r_1$, then

$$\begin{aligned}
\deg(r_2) &= \deg(r_2 - r_1) && (1.58)\\
&= \deg\left((q_1 - q_2) * g\right) && (1.59)\\
&= \deg(q_1 - q_2) + \deg(g) && (1.60)\\
&> \deg(g) && (1.61)
\end{aligned}$$

but this contradict our assumption eq.(1.56). So, both r and q are unique.

Next we shall prove this algorithm terminate; we shall show that above WHILE is not an infinite loop. Since the process

```
r -> r - (LT(r) / LT(g))* g
```
(1.62)

is strict decreasing on their degree; suppose $m \geq k$ and[2]

$$\begin{aligned}
r &= a_0 * x^m + O(x^{m-1}) && (1.63)\\
g &= b_0 * x^k + O(x^{k-1}) && (1.64)
\end{aligned}$$

Then $r - (LT(r)/LT(g)) * g$ is

$$a_0 * x^m + O(x^{m-1}) - \frac{a_0 * x^m}{b_0 * x^k} \times \Big(b_0 * x^k + O(x^{k-1})\Big) \tag{1.65}$$

and clearly the coefficient of x^m is cancelled out, the result is at most $O(x^{m-1})$. So, for finite degree of inputs, it exits WHILE loop finite steps. ■

rem and quot

For $f(x), g(x)(\neq 0) \in \mathbb{K}[x]$ and the consequence of division algorithm,

$$f(x) = q(x) * g(x) + r(x), \tag{1.66}$$

let us define

$$\begin{aligned}
\text{rem}\left(f(x), g(x)\right) &:= r(x) && (1.67)\\
\text{quot}\left(f(x), g(x)\right) &:= q(x). && (1.68)
\end{aligned}$$

[2] This is so called ”big O notation”.

Recursive definition

Here is the recursive definition. The input of this algorithm is two polynomials

$$f(x), g(x)(\neq 0) \in \mathbb{K}[x] \tag{1.69}$$

and its outputs are

$$q(x), r(x) \in \mathbb{K}[x] \tag{1.70}$$

s.t. $f(x) = q(x) * g(x) + r(x)$.

1. Base case.

$$\begin{aligned} q_0(x) &:= 0 && (1.71) \\ r_0(x) &:= f(x) && (1.72) \end{aligned}$$

2. Induction step. If $r_n(x)$ is zero polynomial, or $LT\,(r_n(x)) \ngeq LT\,(g(x))$, then

$$\begin{aligned} q(x) &:= q_n(x) && (1.73) \\ r(x) &:= r_n(x) && (1.74) \end{aligned}$$

   otherwise, i.e. $r_n(x) \neq 0$ and $LT\,(r_n(x)) \geq LT\,(g(x))$,

$$\begin{aligned} q_{n+1}(x) &:= q_n(x) + \frac{LT\,(r_n(x))}{LT\,(g(x))} && (1.75) \\ r_{n+1}(x) &:= r_n(x) - \frac{LT\,(r_n(x))}{LT\,(g(x))} * g(x) && (1.76) \end{aligned}$$

Haskell code

todo: QuickCheck

Here is an actual code for one variable polynomial division. At first, we have used Double for coefficients, but Haskell can treat ”Rationals”.

```
DARation.lhs

For one variable K[x].

> module DARation where
> import Data.Ratio
> import Test.QuickCheck

> type Monomial = Int
> -- type ATerm = (Double, Monomial)
> type ATerm = (Ratio Int, Monomial)
```

A term is given by its coefficient and its non-negative power.

```
> type Poly = [ATerm]
```

We assume that there is no terms with same power like
  (3.0, 7) (-2.0, 7)
It’s much better to implement as an instance of Num!

```
> polySort :: Poly -> Poly
> polySort [] = []
> polySort (f1@(c,a):polys)
>   = if (c /= 0) then higher ++ (f1: lower)
>                 else higher ++ lower
>   where higher = polySort [(c’,a’) | (c’,a’) <- polys, c’ /= 0, a’ > a]
>         lower  = polySort [(c’,a’) | (c’,a’) <- polys, c’ /= 0, a’ < a]

> polyAdd :: Poly -> Poly -> Poly
> polyAdd f g = polyAdd’ (polySort f) (polySort g)
>   where
>     polyAdd’ :: Poly -> Poly -> Poly
>     polyAdd’ [] [] = []
>     polyAdd’ f [] = f
>     polyAdd’ [] g = g
>     polyAdd’ f@((c1,a1):fs) g@((c2,a2):gs)
>       | a1 > a2 = (c1,a1) : (polyAdd’ fs g)
>       | a1 < a2 = (c2,a2) : (polyAdd’ f gs)
>       | a1 == a2 = (c1+c2,a1) : (polyAdd’ fs gs)
>       | otherwise = error ":polyAdd"

> polyNegate :: Poly -> Poly
> polyNegate = map (\(c,a) -> (-c,a))
> polySub :: Poly -> Poly -> Poly
> polySub f g = polyAdd f (polyNegate g)

> polyMul :: Poly -> Poly -> Poly
> polyMul f g = polyMul’ (polySort f) (polySort g)
>   where
>     polyMul’ :: Poly -> Poly -> Poly
>     polyMul’ [] [] = []
>     polyMul’ [] _ = []
>     polyMul’ _ [] = []
>     polyMul’ ((c1,a1):fs) g@((c2,a2):gs)
>       = polyAdd first (polyMul’ fs g)
>       where first = map (\(c,a) -> (c*c1, a+a1)) g
```

```
  *DivisionAlgorithm> polyMul [(2,3),(-4,1),(3,0)] [(1,1),(1,0)]
  [(2.0,4),(2.0,3),(-4.0,2),(-1.0,1),(3.0,0)]
  (%i9) f: 2*x^3-4*x+3;
  (%o9) 2*x^3-4*x+3
  (%i10) g: x+1;
  (%o10) x+1
  (%i13) g*f, expand;
  (%o13) 2*x^4+2*x^3-4*x^2-x+3
```

```
> isDivisibleBy :: ATerm -> ATerm -> Bool
> isDivisibleBy (_, a) (_, b)
>   | a < 0 || b < 0 = error "ATerm is given by positive power"
>   | otherwise = (a >= b)

> leadingTermOf :: Poly -> ATerm
> leadingTermOf polynomial = head $ polySort polynomial
```

```
  *DivisionAlgorithm> let f = [(2,3),(-4,1),(3,0)] :: Poly
  *DivisionAlgorithm> leadingTermOf f
  (2.0,3)
```

```
> termDiv :: ATerm -> ATerm -> ATerm
> termDiv f@(c1,a1) g@(c2,a2)
>   | c2 == 0
>        = error "0 division"
>   | f ‘isDivisibleBy‘ g
>        = (c1/c2, a1-a2) -- since c1 :: Ratio Int, 1/3 = 1 % 3
>    | otherwise
>        = error "Not divisible"

> -- polyDiv :: Poly -> Poly -> (Quot, Rem)
> polyDiv :: Poly -> Poly -> (Poly, Poly)
> polyDiv f g = polyDiv’ (polySort f) (polySort g)
> polyDiv’ :: Poly -> Poly -> (Poly, Poly)
> polyDiv’ _ [] = error "zero division"
> polyDiv’ [] g = ([],g)
> f ‘polyDiv’‘ g = div’ g ([], f)
>   where
>     div’ :: Poly -> (Poly, Poly) -> (Poly, Poly)
>     div’ g (q, r)
>       | r /= [] && ltr ‘isDivisibleBy‘ ltg
>           = div’ g (q ‘polyAdd‘ newR, r ‘polySub‘ (newR ‘polyMul‘ g))
>       | otherwise = (polySort q, polySort r)
>       where
>         ltr = leadingTermOf r
>         ltg = leadingTermOf g
>         newR = [ltr ‘termDiv‘ ltg] :: Poly
```

```
(%i41) divide(x^3+2*x^2+x+1, 2*x+1,x);
(%o41) [(4*x^2+6*x+1)/8,7/8]

*DARation Data.Ratio> let f = [(1,3),(2,2),(1,1),(1,0)]
*DARation Data.Ratio> let g = [(2,1),(1,0)]
*DARation Data.Ratio> f ‘polyDiv‘ g
([(1 % 2,2),(3 % 4,1),(1 % 8,0)],[(7 % 8,0)])

*DARation Data.Ratio> f ‘polyDiv‘ g
([(1 % 2,2),(3 % 4,1),(1 % 8,0)],[(7 % 8,0)])
*DARation Data.Ratio> ((fst it) ‘polyMul‘ g) ‘polyAdd‘ (snd it)
[(1 % 1,3),(2 % 1,2),(1 % 1,1),(1 % 1,0)]
*DARation Data.Ratio> it == f
True
```

1.5.4 "is divisible" $\sqsupseteq$

Let us define

$$f(x) \sqsupseteq g(x) :\Leftrightarrow \exists q(x), f(x) = q(x) * g(x), \tag{1.77}$$

that is, iff $f(x)$ is divisible by $g(x)$ (so $r = 0$).

1.5.5 Every ideal of $\mathbb{K}[x]$ is generated by one polynomial

$\forall$ideal of $\mathbb{K}[x]$ over a field $\mathbb{K}$ can be written in the form $\langle f \rangle$.

Proof

Take an ideal $I \subset \mathbb{K}[x]$. If $I = \{0\}$, then we have done since $I = \langle 0 \rangle$.

Otherwise, we can take a polynomial $f(x) \in I$ which is minimum in degree in I. We shall prove that $I = \langle f \rangle$. Since I is an ideal, if $\forall f'(x) \in \langle f \rangle$ then $f'(x) \in I$, i.e.,

$$\langle f \rangle \subset I. \tag{1.78}$$

Conversely, $\forall g(x) \in I$, by division algorithm in §1.5.3, we have

$$g(x) = q(x) * f(x) + r(x) \tag{1.79}$$

where either $r = 0$ or $\deg(r) < \deg(f)$. Since I is an ideal, $f(x), g(x) \in I$ and $q(x) * f(x) \in I$, we get

$$r(x) = g(x) - q(x) * f(x) \in I. \tag{1.80}$$

If r were not 0, then from §1.5.3, $\deg(r) < \deg(f)$, which would contradict our minimum assumption. So $r = 0$ and this means

$$g(x) \in \langle f \rangle , \tag{1.81}$$

and this means

$$\langle f \rangle \supset I. \tag{1.82}$$

Therefore we get

$$\langle f \rangle = I. \tag{1.83}$$

■

Principal ideal domain (PID)

In general, an ideal generated by one element is called a principal ideal.

1.5.6 Corollary

Let $\mathbb{K}$ be a field and $f(x) \in \mathbb{K}[x]$ be a non zero polynomial. If $m = \deg(f)$, then $f(x) = 0$ has at most m roots in $\mathbb{K}$.

Proof

We will prove this statement by induction on m. When $m = 0$, then f is just a non zero constant, and there is no root, so we have 0 root.

Assume $m - 1$ case holds, then consider f of m degree. If f has no root, then done. Else $f(x) = 0$ has a root $a \in \mathbb{K}$, then by §1.5.3,

$$f(x) = q(x) * (x - a) + r(x), \deg(r) < \deg(x - a) = 1 \tag{1.84}$$

that is $r \in \mathbb{K}$. Since f is zero at a,

$$r = f(a) = 0 \tag{1.85}$$

and

$$f(x) = q(x) * (x - a). \tag{1.86}$$

Since $\deg(q)$ is $m - 1$, and has at most $m - 1$ root in $\mathbb{K}$. Therefore, $f(x) = 0$ has at most m root.
■

1.5.7 Zero function on an infinite field

Consider an infinite field $\mathbb{K}$ and $f(x) \in \mathbb{K}[x_1, \cdots, x_n]$. Then $f = 0$ in $f \in \mathbb{K}[x_1, \cdots, x_n]$ iff $f(x) : \mathbb{K}^n \to \mathbb{K}$ is the zero function.

Proof

($\Rightarrow$) part is obvious, since if $f(x)$ is the zero polynomial, i.e., all the coefficients are zero, then $f(x)$ gives zero function:

$$f : \mathbb{K}^n \to \mathbb{K}; \forall a \mapsto 0. \tag{1.87}$$

($\Leftarrow$) We will use induction on n to show the statement that if for every $a \in \mathbb{K}^n, f(a) = 0$ then $f(x)$ is the zero polynomial.

1. Base case ($n = 1$). Since $f(x) \in \mathbb{K}[x]$ has at most $\deg(f)$ roots in $\mathbb{K}$ by §1.5.6, if $\deg(f)$ is finite, we can choose some

   $$a \in \mathbb{K} \tag{1.88}$$

   s.t.

   $$f(a) \neq 0 \tag{1.89}$$

   since $\mathbb{K}$ is infinite (set). So, if $\forall a \in \mathbb{K}, f(a) = 0$ then $f(x) = 0$ has infinitely many roots, and hence $f(x)$ is the zero polynomial.

2. Induction step. Assume $n-1$ case is true, and let $f(x) \in \mathbb{K}[x_1, \cdots, x_n]$ be a polynomial s.t. $\forall a \in \mathbb{K}^n, f(a) = 0$. By collecting the terms which are powers of x_n, we can write

   $$f(x) = \sum_i g_i(x_1, \cdots, x_{n-1}) * x_n^i. \tag{1.90}$$

   Let us fix

   $$(a_1, \cdots, a_{n-1}) \in \mathbb{K}^{n-1} \tag{1.91}$$

   and treat

   $$f(a_1, \cdots, a_{n-1}, x_n) \in \mathbb{K}[x_n] \tag{1.92}$$

   as a polynomial only of x_n. Since $f(x)$ is zero for every x_n, $f(x)$ is the zero polynomial of x_n. This means the "coefficients" are zero

   $$g_i(a_1, \cdots, a_{n-1}) = 0. \tag{1.93}$$

   However, our choice of $(a_1, \cdots, a_{n-1})$ is arbitrary and this means every $g_i(x)$ is zero polynomial in $\mathbb{K}[x_1, \cdots, x_{n-1}]$. From the induction hypothesis, $g_i = 0$, and

   $$f = 0. \tag{1.94}$$

■

1.5.8 GCD

A greatest common divisor of $f(x), g(x) \in \mathbb{K}[x]$ is a polynomial $h(x) \in \mathbb{K}[x]$ s.t.

1.

$$f(x) \sqsupseteq h(x) \tag{1.95}$$

$$g(x) \sqsupseteq h(x) \tag{1.96}$$

2. If $h'(x) \in \mathbb{K}[x]$ satisfies

$$f(x) \sqsupseteq h'(x) \tag{1.97}$$

$$g(x) \sqsupseteq h'(x) \tag{1.98}$$

then

$$h(x) \sqsupseteq h'(x) \tag{1.99}$$

i.e., ”greatest”.

Proof

We show the existence of such a gcd. Let us consider an ideal

$$\langle f(x), g(x) \rangle \subset \mathbb{K}[x]. \tag{1.100}$$

Since $\forall$ ideal in $\mathbb{K}[x]$ is PID, there exists a polynomial $h(x) \in \mathbb{K}[x]$ s.t.

$$\langle f(x), g(x) \rangle = \langle h(x) \rangle . \tag{1.101}$$

So, there are $a(x), b(x) \in \mathbb{K}[x]$ s.t.

$$f(x) = a(x) * h(x) \tag{1.102}$$

$$g(x) = b(x) * h(x) \tag{1.103}$$

$$\tag{1.104}$$

since $f(x), g(x) \in \langle f(x), g(x) \rangle = \langle h(x) \rangle$. This is equivalent to

$$f(x) \sqsupseteq h(x) \tag{1.105}$$

$$g(x) \sqsupseteq h(x) \tag{1.106}$$

We claim that this $h(x)$ is a greatest common devisor of $f(x)$ and $g(x)$.

If we take $h'(x) \in \mathbb{K}[x]$ s.t.

$$\begin{aligned} f(x) &\sqsupseteq h'(x) \qquad (1.107) \\ g(x) &\sqsupseteq h'(x) \qquad (1.108) \end{aligned}$$

i.e., $\exists c(x), d(x) \in \mathbb{K}[x]$ s.t.,

$$\begin{aligned} f(x) &= c(x) * h'(x) \qquad (1.109) \\ g(x) &= d(x) * h'(x). \qquad (1.110) \end{aligned}$$

Then, since $\langle f(x), g(x) \rangle = \langle h(x) \rangle$, there exists $i(x), j(x) \in \mathbb{K}[x]$ s.t.

$$\begin{aligned} h(x) &= i(x) * f(x) + j(x) * g(x) \qquad (1.111) \\ &= (i(x) * c(x) + j(x) * d(x)) * h'(x). \qquad (1.112) \end{aligned}$$

That is,

$$h(x) \sqsupseteq h'(x). \qquad (1.113)$$

■

1.5.9 GCD is "unique"

GCD is unique up to overall factor.

Proof

If we have

$$h(x), h'(x) \in \mathbb{K}[x] \qquad (1.114)$$

as two GCD of $f(x), g(x) \in \mathbb{K}[x]$, then

$$\begin{aligned} h(x) &\sqsupseteq h'(x) \qquad (1.115) \\ h'(x) &\sqsupseteq h(x) \qquad (1.116) \end{aligned}$$

i.e., we have $l(x), m(x) \in \mathbb{K}[x]$ s.t.

$$\begin{aligned} h(x) &= l(x) * h'(x) \qquad (1.117) \\ h'(x) &= m(x) * h(x) \qquad (1.118) \end{aligned}$$

So

$$h(x) = (l(x) * m(x)) * h(x) \qquad (1.119)$$

i.e., $l(x), m(x)$ are constant polynomial:

$$l(x) * m(x) = 1, \forall x \in \mathbb{K}. \qquad (1.120)$$

■

1.5.10 GCD algorithm

Pseudo code and recursive definition

```
Input: f,g
Output: h
h := f
s := g
WHILE s /= 0 DO
  rem := remainder(h,s)
  h := s
  s := rem
```

Here is the recursive definition.

1. Base case.

$$h_0(x) := f(x) \tag{1.121}$$

$$s_0(x) := g(x) \tag{1.122}$$

2. Induction step. If $s_n(x)$ is zero polynomial, then

$$\mathrm{GCD}\left(f(x), g(x)\right) := h_n(x), \tag{1.123}$$

otherwise

$$h_{n+1}(x) := s_n(x) \tag{1.124}$$

$$s_{n+1}(x) := \mathrm{rem}\left(h_n(x), s_n(x)\right). \tag{1.125}$$

Proof

Let us prove that this algorithm will terminate in finite steps. From the division algorithm, observe

$$\deg\left(s_0(x)\right) > \deg\left(s_1(x)\right) > \cdots, \tag{1.126}$$

i.e., $\{\deg\left(s_n(x)\right)\}_n$ is strictly decreasing sequence. Since our termination condition is $\deg\left(s_n(x)\right) = 0$, this algorithm will stop at finite steps.

If we put

$$h_n(x) = q_n(x) * s_n(x) + \mathrm{rem}\left(h_n(x), s_n(x)\right) \tag{1.127}$$

as the consequence of polynomial division, then

$$\begin{aligned}\langle h_n(x), s_n(x)\rangle &= \langle q_n(x) * s_n(x) + \operatorname{rem}\left(h_n(x), s_n(x)\right), s_n(x)\rangle & (1.128)\\ &= \langle \operatorname{rem}\left(h_n(x), s_n(x)\right), s_n(x)\rangle & (1.129)\\ &= \langle s_{n+1}(x), h_{n+1}(x)\rangle & (1.130)\end{aligned}$$

Therefore, if $s_n(x)$ is zero polynomial, then we get

$$\begin{aligned}\langle f(x), g(x)\rangle &= \langle h_0(x), s_0(x)\rangle & (1.131)\\ &\vdots \\ &= \langle h_{n-1}(x), s_{n-1}(x)\rangle & (1.132)\\ &= \langle h_n(x), 0\rangle & (1.133)\\ &= \langle h_n(x)\rangle & (1.134)\end{aligned}$$

So

$$\operatorname{GCD}\left(f(x), g(x)\right) = h_n(x). \qquad (1.135)$$

■

1.5.11 Bëzout lemma

For arbitrary polynomials $f(x), g(x) \in \mathbb{K}[x]$, there are $a(x), b(x) \in \mathbb{K}[x]$ s.t.

$$f(x) * a(x) + g(x) * b(x) = \operatorname{GCD}\left(f(x), g(x)\right). \qquad (1.136)$$

To prove this claim, we extend our GCD algorithm.

1.5.12 Extended GCD

The following algorithm is a constructive proof for Bëzout lemma in §1.5.11.

1. Base case.

$$\begin{aligned}(r_0(x), s_0(x), t_0(x)) &:= (f(x), 1, 0) & (1.137)\\ (r_1(x), s_1(x), t_1(x)) &:= (g(x), 0, 1) & (1.138)\end{aligned}$$

2. Induction step. Define $n \geq 2$,

$$q_n(x) := \operatorname{quot}\left(r_{n-2}(x), r_{n-1}(x)\right) \qquad (1.139)$$

and

$$\begin{aligned} r_n(x) &:= \operatorname{rem}\left(r_{n-2}(x), r_{n-1}(x)\right) && (1.140)\\ &= r_{n-2}(x) - q_n(x) * r_{n-1}(x) && (1.141)\\ s_n(x) &:= s_{n-2}(x) - q_n(x) * s_{n-1}(x) && (1.142)\\ t_n(x) &:= t_{n-2}(x) - q_n(x) * t_{n-1}(x) && (1.143) \end{aligned}$$

If $r_{n+1}(x)$ is zero polynomial, then

$$\operatorname{GCD}\left(f(x), g(x)\right) := r_n(x). \qquad (1.144)$$

Proof

This algorithm will also terminate, since

$$\deg\left(r_n(x)\right) > \deg\left(r_{n+1}(x)\right). \qquad (1.145)$$

Observe that for $n = 0, 1$ they satisfy so called Bëzout identity

$$r_n(x) = s_n(x) * f(x) + t_n(x) * g(x). \qquad (1.146)$$

We claim this holds for all n. If we assume this is the case for $0, 1, \cdots, n(\geq 1)$, then

$$\begin{aligned} r_{n+1}(x) &:= r_{n-1}(x) - q_n(x) * r_n(x) && (1.147)\\ &= s_{n-1}(x) * f(x) + t_{n-1}(x) * g(x) - q_n(x) * (s_n(x) * f(x) + t_n(x) * g(x)) && (1.148)\\ &= (s_{n-1}(x) + q_n(x) * s_n(x)) * f(x) + (s_{n-1}(x) + q_n(x) * s_n(x)) * g(x) && (1.149)\\ &= s_{n+1}(x) * f(x) + t_{n+1}(x) * g(x) && (1.150) \end{aligned}$$

Now

$$\begin{aligned} \langle r_n(x), r_{n+1}(x)\rangle &= \langle r_n(x), r_{n-1}(x) - q_{n+1}(x) * r_n(x)\rangle && (1.151)\\ &= \langle r_n(x), r_{n-1}(x)\rangle && (1.152) \end{aligned}$$

we get

$$\begin{aligned} \langle f(x), g(x)\rangle &:= \langle r_0(x), r_1(x)\rangle && (1.153)\\ &= \langle r_1(x), r_2(x)\rangle && (1.154)\\ &\vdots \end{aligned}$$

Therefore, if we meet $r_{n+1}(x) = 0$, then

$$\begin{aligned} \langle f(x), g(x) \rangle &= \langle r_n(x), 0 \rangle && (1.155) \\ &= \langle r_n(x) \rangle && (1.156) \\ & && (1.157) \end{aligned}$$

so

$$\mathrm{GCD}\,(f(x), g(x)) := r_n(x). \tag{1.158}$$

For this n with $r_{n+1}(x) = 0$, we have

$$r_n(x) = s_n(x) * f(x) + t_n(x) * g(x). \tag{1.159}$$

■

Chapter 2

Gröbner Bases

I'd like to rewrite AAC related sections from scratch.

2.1 Introduction

2.2 Orderings on the Monomials in $\mathbb{K}\left[x_1, ..., x_n\right]$

2.2.1 Definition of monomial order $(\mathbb{N}^n, >)$

A monomial order on $\mathbb{K}[x_1, \cdots, x_n]$ is a relation $>$ on $\mathbb{N}^n$, or on a set $\{x^\alpha | \alpha \in \mathbb{N}^n\}$, satisfying

$$(\mathbb{N}^n, >) \text{ is totally ordered} \tag{2.1}$$

$$\alpha > \beta, \gamma \in \mathbb{N}^n \Rightarrow \alpha + \gamma > \beta + \gamma \tag{2.2}$$

$$(>, \mathbb{N}^n) \text{ is well-ordered.} \tag{2.3}$$

The following lemma will help us understand what the well-ordering condition of the third part of above definition:

2.2.2 A condition for $(\mathbb{N}^n, >)$ is well-ordered

An order $>$ on $\mathbb{N}^n$ is well-ordered iff $\forall$ strictly decreasing sequence $\{\alpha(i)\}_i$ in $\mathbb{N}^n$ will terminate:

$$\alpha(1) > \alpha(2) > \cdots > \alpha(m). \tag{2.4}$$

Proof

We shall prove this in contrapositive form.[1]

If $(\mathbb{N}^n, >)$ is not well-ordered, then there is a non-empty subset $S \subset \mathbb{N}^n$ that has no smallest element. We can pick $\alpha(1) \in S$, but $\alpha(1)$ is not the smallest element. Thus $\exists\alpha(2) \in S$ s.t. $\alpha(1) > \alpha(2)$. Continuing the same way, we can get an infinite strictly decreasing sequence in S:

$$\alpha(1) > \alpha(2) > \cdots \tag{2.5}$$

Conversely, given such an infinite sequence, then

$$\{\alpha(1), \alpha(2), \cdots\} \tag{2.6}$$

is a nonempty subset in $\mathbb{N}^n$ with no smallest element. That is, we have shown

$$(\mathbb{N}^n, >) \text{ is not well-ordered} \Leftrightarrow \exists \text{infinite strict decreasing sequence in } \mathbb{N}^n. \tag{2.7}$$

■

Note

This lemma guarantees that several algorithms must terminate in a finite number of steps. At each step of the algorithm, some monomials strictly decrease with respect to a fixed monomial order.

2.2.3 Terminologies

Let

$$f = \sum_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1, \cdots, x_n] \tag{2.8}$$

be a nonzero polynomial, and $>$ is a (fixed) monomial order.

The multi degree of f is given by

$$MD(f) := \max(\alpha \in \mathbb{N}^n, a_\alpha \neq 0) = \alpha_{\max} \in \mathbb{N}^n \tag{2.9}$$

with respect to the monomial order $>$.

The leading coefficient of f is

$$LC(F) := a_{\alpha_{\max}} \in \mathbb{K}. \tag{2.10}$$

[1] For $P \Rightarrow Q$, its contraposition is $\neg Q \Rightarrow \neg P$.

The leading monomial of f is

$$LM(f) := x^{\alpha_{\max}}, \tag{2.11}$$

of course this is a term with 1 as its coefficient. The leading term of f is

$$LT(f) := LC(F) * LM(f) = a_{\alpha_{\max}} * x^{\alpha_{\max}}. \tag{2.12}$$

2.2.4 Lemma (Multiplications and summations)

Let $f, g \in \mathbb{K}[x_1, \cdots, x_n]$ be nonzero polynomial. Then

$$MD(f * g) = MD(f) + MD(g), \tag{2.13}$$

and if $f + g \neq 0$, then

$$MD(f + g) \leq \max(MD(f), MD(g)). \tag{2.14}$$

If, in addition, $MD(f) \neq MD(g)$, then equality holds.[2]

Proof

Let us write

$$\begin{aligned} f &= a_{\alpha_{\max}} * x^{\alpha_{\max}} + O(x^{\alpha_{\max}-1}) && (2.15)\\ g &= b_{\beta_{\max}} * x^{\beta_{\max}} + O(x^{\beta_{\max}-1}) && (2.16) \end{aligned}$$

then clearly

$$f * g = a_{\alpha_{\max}} * b_{\beta_{\max}} * x^{\alpha_{\max}+\beta_{\max}} + O(x^{\alpha_{\max}-1+\beta_{\max}-1}) \tag{2.17}$$

and

$$f + g = a_{\alpha_{\max}} * x^{\alpha_{\max}} + O(x^{\alpha_{\max}-1}) + b_{\beta_{\max}} * x^{\beta_{\max}} + O(x^{\beta_{\max}-1}) \tag{2.18}$$

There might be a cancellation on the leading terms.
■

[2] In this case, there is no cancellation on the leading terms.

2.3 Division algorithm in $\mathbb{K}[x_1, ..., x_n]$

2.3.1 ”is divisible by” as a binary relation

Define a binary relation $\sqsupseteq$ (”is divisible by”) on $\mathbb{K}[x_1, \cdots, x_n]$ by $\forall r, f \in \mathbb{K}[x_1, \cdots, x_n]$,

$$r \sqsupseteq f :\Leftrightarrow \exists q \in \mathbb{K}[x_1, \cdots, x_n], r = q * f. \tag{2.19}$$

i.e. r is divisible by f iff there is some polynomial q and $r = q * f$.[3]

Let us write the negation:

$$r \sqsubset f :\Leftrightarrow \nexists q \in \mathbb{K}[x_1, \cdots, x_n], r = q * f \tag{2.20}$$

i.e. r is not divisible by f.

2.3.2 Division algorithm in $\mathbb{K}[x_1, ..., x_n]$

Let $>$ be a (fixed) monomial order[4] and $(\mathbb{N}^n, >)$ be well-ordered, and

$$F := (f_1, \cdots, f_s) \tag{2.21}$$

be an ordered s-tuple (or a list) of polynomials in $\mathbb{K}[x_1, \cdots, x_n]$. Then $\forall f \in \mathbb{K}[x_1, \cdots, x_n]$,

$$\exists a_i, r \in \mathbb{K}[x_1, \cdots, x_n] \text{ s.t. } f = a_1 * f_1 + \cdots + a_s * f_s + r, \tag{2.22}$$

and either $r = 0$ or r is a linear combination, with coefficients in $\mathbb{K}$, of monomials, none of which is divisible by any of $LT(f_1), \cdots, LT(f_s)$:[5]

$$r \sqsubset LT(f_1), \cdots, \text{ and } r \sqsubset LT(f_s). \tag{2.23}$$

Furthermore, if $a_i f_i \neq 0.$, then we have [6]

$$MD(f) \geq MD(a_i * f_i) \tag{2.24}$$

with respect to the fixed monomial order.

[3] $r|f$ is the usual notation for ”is divisible”, but I would like to use an asymmetric notation for such an asymmetric binary relation.

[4] We will introduce some monomial orders in §2.4.6.

[5] See §2.3.1

[6] This is notation abuse, $\geq$ means $>$ or $=$ (as an ordered monomial $\mathbb{N}^n$).

Pseudo code

```
Input: f_1 .. f_s,f
Output: a_1 .. a_s,r
a_1 := 0; ..; a_s := 0; r := 0
p := f

WHILE p /= 0 DO
  i := 1
  divisionOccured := False
  WHILE i <= s AND divisionOccured = False DO
    IF LT(f_i) divides p THEN
      a_i := a_i + LT(p) / LT(f_i)
      p   := p - (LT(p) / LT(f_i)) * f_i
      divisionOccured := True
    Else
      i := i + 1
  IF divisionOccured = False THEN
    r := r + LT(p)
    p := p - LT(p)
```

Proof

To prove that the above algorithm works, we'll first show that

$$f = a_1 * f_1 + \cdots + a_s * f_s + p + r \tag{2.25}$$

holds at every stage, by induction on steps. This is clearly true for the initial values of $a_1, \cdots, a_s (= 0), p (= f), r (= 0)$. Suppose eq.(2.25) holds at one step of the algorithm. If the next step is a Division Step, i.e.,

$$\texttt{LT(f\_i) divides p} \tag{2.26}$$

then the following combination

$$a_i f_i + p = \left(a_i + \frac{LT(p)}{LT(f_i)} \right) * f_i + \left(p - \frac{LT(p)}{LT(f_i)} * f_i \right) \tag{2.27}$$

stays unchanged. Since all other variables are unaffected, eq.(2.25) remains true in this case.

On the other hand, if the next step is a Remainder Step, then both r and p will be changed,

$$\texttt{r := r + LT(p)} \tag{2.28}$$

$$\texttt{p := p - LT(p)} \tag{2.29}$$

but the sum is unchanged:

$$r + p = (r + LT(p)) + (r + LT(p)) \,. \tag{2.30}$$

Also eq.(2.25) remains true in this case.

Note that this algorithm comes to halt when $p = 0$, see the first `WHILE` statement. In this situation (when $p = 0$), eq.(2.25) becomes

$$f = a_1 * f_1 + \cdots + a_s * f_s + r. \tag{2.31}$$

Finally, we need to show that this algorithm will terminate. The key observation is the rewriting process:

```
p := p - (LT(p) / LT(f_i)) * f_i                    (2.32)
```

By Lemma in §2.2.4,

$$LT\left(\frac{LT(p)}{LT(f_i)} * f_i\right) = \frac{LT(p)}{LT(f_i)} * LT(f_i) = LT(p). \tag{2.33}$$

If p becomes 0 in this process, then this algorithm halts. Even if $p \neq 0$, the leading term will vanish, and the multi degree must decrease strictly.

If this algorithm never terminated, that is, we never meet $p = 0$, then we could get an infinite decreasing sequence of multi degrees. But since our monomial order satisfies eq.(2.3), i.e. $\forall$ strict decreasing sequence will terminate (as §2.2.2) and eventually $p = 0$.

Finally, consider $MD(f)$ and $MD(a_i f_i)$. Every term in a_i is of the form

$$\frac{LT(p)}{LT(f_i)} \tag{2.34}$$

for some p. Above algorithm starts with $p = f$ and the multi degree of p's are decreasing:

$$MD(f = p) > MD(p') > \cdots \,. \tag{2.35}$$

This shows that for every step, either $>$ or $=$ holds

$$MD(f) \geq MD(p) \tag{2.36}$$

and

$$MD(a_i f_i) = MD\left(\frac{LT(p)}{LT(f_i)} * f_i\right) = MD(p) \leq MD(f) \tag{2.37}$$

■

2.3.3 The ideal membership problems

As a consequence of the above division algorithm §2.3.2 in multi-variables is the followings; if after division of f by the ordered tuple $F := (f_1, \cdots, f_s)$ we obtain $r = 0$, then we have

$$f = a_1 * f_1 + \cdots a_t * f_t. \tag{2.38}$$

Thus $r = 0$ is a sufficient condition for ideal membership:

$$r = 0 \Rightarrow f \in \langle f_1, \cdots, f_s \rangle . \tag{2.39}$$

However, we'll see soon, $r = 0$ is not a necessary condition for being in the ideal.[7]

Example

Let us consider $\mathbb{K}[x, y]$ with lex order and

$$\begin{aligned} f_1 &:= x * y + 1 && (2.40) \\ f_2 &:= y^2 - 1 && (2.41) \end{aligned}$$

Dividing

$$f = x * y^2 - x \tag{2.42}$$

by an ordered 2-tuple (f_1, f_2), the result is

$$\begin{aligned} f &= x * y^2 - x && (2.43) \\ &= y * (f_1 - 1) - x && (2.44) \\ &= y * f_1 - x - y. && (2.45) \end{aligned}$$

On the other hand, by (f_2, f_1), the result is

$$\begin{aligned} f &= x * y^2 - x && (2.46) \\ &= x * (f_2 + 1) - x && (2.47) \\ &= x * f_2 + 0 && (2.48) \\ \Rightarrow f &\in \langle f_1, f_2 \rangle . && (2.49) \end{aligned}$$

Thus, the first trial show that even if $f \in \langle f_1, f_2 \rangle$, the reminder can be non zero.
■

[7] We'll find the iff condition for an ideal membership in §2.6.3, using Gröbner basis.

2.4 Monomial Ideals and Dickson's Lemma

2.4.1 Definition of monomial ideals

$I \subset \mathbb{K}[x_1, \cdots, x_n]$ is a monomial ideal iff the elements can be written as a finite sum form:

$$\exists A \subset \mathbb{N}^n \text{ s.t. } I = \left\{ \sum_{i=1}^{s} h_i * x^{\alpha(i)} \middle| \alpha(i) \in A, h_i \in \mathbb{K}[x_1, \cdots, x_n] \right\} \tag{2.50}$$

Then we write as a generator form:

$$I := \langle x^\alpha | \, \alpha \in A \rangle \tag{2.51}$$

2.4.2 Monomial ideal memberships

Let $I = \langle x^\alpha | \, \alpha \in A \rangle \subset \mathbb{K}[x_1, \cdots, x_n]$ be a monomial ideal. Then a monomial x^β is in I iff

$$\exists \alpha \in A \text{ s.t. } x^\beta \sqsupseteq x^\alpha \tag{2.52}$$

i.e., x^β is divisible by some $x^\alpha \in I$.

Proof

($\Leftarrow$) If $x^\beta \sqsupseteq x^\alpha$, then there is some $h \in \mathbb{K}[x_1, \cdots, x_n]$ s.t.,

$$x^\beta = h * x^\alpha. \tag{2.53}$$

So clearly $x^\beta \in I$ by the definition of ideal.

($\Rightarrow$) Conversely, if $x^\beta \in I$, then we have an expression for x^β:

$$x^\beta = \sum_{i=1}^{s} h_i * x^{\alpha(i)} \tag{2.54}$$

Now our generating set

$$\left\{ x^{\alpha(1)}, \cdots, x^{\alpha(s)} \right\} \tag{2.55}$$

is finite by definition of monomial ideals. From the well-ordered property of our monomial order, this generating set has the minimum element. Without loss of generality, we can put $\alpha(1)$ is the minimum[8] and $h_1 \neq 0$, then

$$x^\beta \sqsupseteq x^{\alpha(1)}. \tag{2.56}$$

■

[8] Indeed, we can put this generating set as $\left\{ x^{\alpha(1)} < \cdots < x^{\alpha(s)} \right\}$.

2.4.3 Dickson's Lemma

Let $I = \langle x^{\alpha} |\, \alpha \in A\rangle \subset \mathbb{K}[x_1, \cdots, x_n]$ be a monomial ideal. Then

$$\exists \text{ finite } s \in \mathbb{N}, I = \left\langle x^{\alpha(1)}, \cdots, x^{\alpha(s)} \right\rangle, \tag{2.57}$$

where $x^{\alpha(1)}, \cdots, x^{\alpha(s)} \in A$. That is, every monomial ideal has a finite number of monomial generators.

Proof

By induction on n.[9]

$n = 1$ case, $I = \left\langle x_1^{\alpha(1)} \middle| \alpha(1) \in A \subset \mathbb{N} \right\rangle$. Then just take the smallest $\beta \in A$ and

$$I = \left\langle x_1^{\beta} \right\rangle. \tag{2.58}$$

Now assume that $n > 1$ and this theorem holds for up to $n-1$. Consider the following form of monomial

$$x^{\alpha} * y^{m} \in \mathbb{K}[x_1, \cdots, x_{n-1}, y], \tag{2.59}$$

where

$$\alpha \in \mathbb{N}^{n-1}, m \in \mathbb{N}. \tag{2.60}$$

and a monomial ideal

$$I \subset \mathbb{K}[x_1, \cdots, x_{n-1}, y]. \tag{2.61}$$

Define an ideal in $\mathbb{K}[x_1, \cdots, x_{n-1}]$ (not in $\mathbb{K}[x_1, \cdots, x_{n-1}, y]$):

$$J := \{ x^{\alpha} \in \mathbb{K}[x_1, \cdots, x_{n-1}] |\, \exists m \in \mathbb{N} \text{ s.t. } x^{\alpha} y^{m} \in I\} \tag{2.62}$$

By our inductive hypothesis, there is a finite s s.t.

$$J = \left\langle x^{\alpha(1)}, \cdots, x^{\alpha(s)} \right\rangle. \tag{2.63}$$

From this construction, $\forall\, \alpha(i)|_{i=1}^{s}, \exists m_i \in \mathbb{N}$ s.t. $x^{\alpha(i)} y^{m_i} \in I$. Now we can take

$$m := \max \left(m_i|_{i=1}^{s} \right). \tag{2.64}$$

[9] Here we uses the well-ordering property of $\mathbb{N}$.

$0 \leq \forall j \leq m-1$, define an ideal in $\mathbb{K}[x_1, \cdots, x_{n-1}]$:

$$J_j := \left\{ x^\beta \in \mathbb{K}[x_1, \cdots, x_{n-1}] \middle| x^\beta * y^j \in I \right\}. \tag{2.65}$$

Using our inductive hypothesis, again, we get a finite s_j:

$$J_j = \left\langle x^{\alpha_j(1)}, \cdots, x^{\alpha_j(s_j)} \right\rangle. \tag{2.66}$$

Define a union of above generators

$$\tilde{J} := \{x^{\alpha(1)}, \cdots, x^{\alpha(s)}, x^{\alpha_0(1)}, \cdots, x^{\alpha_{m-1}(s_{m-1})}\} \tag{2.67}$$

and write $\left\langle \tilde{J} \right\rangle$ is an ideal generated by the elements of $\tilde{J}$. From above construction, $\left\langle \tilde{J} \right\rangle$ is a monomial ideal and

$$\left\langle \tilde{J} \right\rangle \subset I. \tag{2.68}$$

Then we can show that $\forall$monomial in I is divisible by one of the element of $\tilde{J}$. Since, $\forall x^\alpha * y^p \in I$, if $p \geq m$,

$$x^\alpha * y^p \sqsupseteq \exists x^{\alpha(i)} * y^m \in \left\langle \tilde{J} \right\rangle, \tag{2.69}$$

else (i.e., $0 \leq p \leq m-1$),

$$x^\alpha y^p \sqsupseteq \exists x^{\alpha_p(j)} y^p \in J_p. \tag{2.70}$$

(In both case, y part is done, and x part is from the inductive hypothesis.)

Let us prove $\left\langle \tilde{J} \right\rangle = I$. Since $\forall f \in I$ of monomial ideal is written as the finite sum of monomials with appropriate factors:

$$f = \sum_{\alpha,p} h_{\alpha,p} * x^\alpha * y^p, h_{\alpha,p} \in \mathbb{K}[x_1, \cdots, x_{n-1}, y] \tag{2.71}$$

$\forall$ monomial $x^\alpha y^p$ of above is divisible by $\left\langle \tilde{J} \right\rangle$, and this shows that

$$I \subset \left\langle \tilde{J} \right\rangle. \tag{2.72}$$

Therefore,

$$I = \left\langle \tilde{J} \right\rangle. \tag{2.73}$$

■

2.4.4 $(\mathbb{N}^n, >)$ is well-ordering iff "positive definite"

Consider $(\mathbb{N}^n, >)$ of a binary relation. If two conditions hold,

$$> \text{ is total order} \tag{2.74}$$

$$\forall \alpha, \beta, \gamma \in \mathbb{N}^n, \alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma \tag{2.75}$$

then [10] the followings are equivalent:

$$(\mathbb{N}^n, >) \text{ is well-ordering } \Leftrightarrow \forall \alpha \in \mathbb{N}^n, \alpha \geq 0. \tag{2.76}$$

Proof

($\Rightarrow$) Assume $(\mathbb{N}^n, >)$ be well-ordering, then we can pick a minimum element:

$$\alpha_0 \in \mathbb{N}^n \text{ s.t. } \forall \alpha \in \mathbb{N}^n, \alpha_0 \leq \alpha \tag{2.77}$$

It suffices to show that $0 \geq \alpha_0$; if $0 > \alpha_0$ were true, using the second assumption,

$$\alpha_0 = 0 + \alpha_0 > \alpha_0 + \alpha_0 = 2\alpha_0 \tag{2.78}$$

i.e., $2\alpha_0$ became smaller than the minimum α_0, contradiction. So,

$$0 \leq \alpha_0. \tag{2.79}$$

($\Leftarrow$) Assume $\forall \alpha \in \mathbb{N}^n, \alpha \geq 0$. Let

$$(\emptyset \neq) A \subset \mathbb{N}^n \tag{2.80}$$

be a non-empty subset and we shall prove $\exists$ a smallest element of A.

Consider an ideal of A:

$$I := \langle x^\alpha | \, \alpha \in A \rangle \tag{2.81}$$

By Dickson's lemma, there is a finite generator:

$$I = \left\langle x^{\alpha(1)}, \cdots, x^{\alpha(s)} \right\rangle \tag{2.82}$$

We can replace the order of such generators by using the monomial total[11] order $<$,

$$I = \left\langle x^{\alpha(1)} < \cdots < x^{\alpha(s)} \right\rangle \tag{2.83}$$

[10] We abuse 0; $0 \in \mathbb{N}^n$.

[11] By definition, our monomial order is total.

Now we can proove $x^{\alpha(1)}$ of the smallest generator is the smallest element of I, and this is the same as $\alpha(1) \in A$ is the smallest. Since $\forall \alpha \in A$,

$$x^{\alpha} \in I = \left\langle x^{\alpha(1)} < \cdots < x^{\alpha(s)} \right\rangle, \tag{2.84}$$

and from the lemma §2.4.2, $1 \leq \exists i \leq s$,

$$x^{\alpha} \sqsupseteq x^{\alpha(i)} \tag{2.85}$$

and this means

$$\exists \gamma \in \mathbb{N}^n \text{ s.t. } \alpha = \alpha(i) + \gamma. \tag{2.86}$$

By our hypothesis, $\gamma \geq 0$, so if $\gamma > 0$,

$$\alpha = \alpha(i) + \gamma > \alpha(i) + 0 = \alpha(i) \geq \alpha(1). \tag{2.87}$$

else $\gamma = 0$,

$$\alpha = \alpha(i) + \gamma = \alpha(i) + 0 = \alpha(i) \geq \alpha(1). \tag{2.88}$$

This means $\alpha(1)$ is the smallest element of given A.
■

2.4.5 Another definition of monomial orders

As a result of the proof in §2.4.4, we can simplify the monomial order $(\mathbb{N}^n, >)$ in §2.2.1, we can replace the 3rd condition by eq.(2.76) of "positive definite":

A monomial order on $\mathbb{K}[x_1, \cdots, x_n]$ is a relation $>$ on $\mathbb{N}^n$, or on a set $\{x^{\alpha} | \alpha \in \mathbb{N}^n\}$, satisfying

$$(\mathbb{N}^n, >) \text{ is totally ordered} \tag{2.89}$$

$$\alpha > \beta, \gamma \in \mathbb{N}^n \Rightarrow \alpha + \gamma > \beta + \gamma \tag{2.90}$$

$$\forall \alpha \in \mathbb{N}^n, \alpha \geq 0. \tag{2.91}$$

2.4.6 Monomial orders in $\mathbb{K}[x_1, ..., x_n]$

We introduce some important instances of monomial orders.

Lexicographic order $>_{lex}$

For $\alpha := (\alpha_1, \cdots, \alpha_n), \beta := (\beta_1, \cdots, \beta_n) \in \mathbb{N}^n$, we say $\alpha >_{lex} \beta$ iff, in the ”vector” difference

$$(\alpha_1 - \beta_1, \cdots, \alpha_n - \beta_n) \tag{2.92}$$

the leftmost nonzero entry is positive.

$$\begin{align} x * y^2 &>_{lex} y^3 * z^4 \tag{2.93} \\ x^3 * y^2 * z^4 &>_{lex} x^3 * y^2 * z \tag{2.94} \\ x &>_{lex} y \tag{2.95} \end{align}$$

In the following (real) code, we assume the length of the list is the same:[12]

```
> type Monomial = [Int]

> lexO :: Monomial -> Monomial -> Ordering
> lexO [] [] = EQ
> lexO (a:as) (b:bs)
>   | a > b = GT
>   | a < b = LT
>   | otherwise = lexO as bs

  *MonomialOrder> lexO [1,2,0] [0,3,4]
  GT
  *MonomialOrder> lexO [3,2,4] [3,2,1]
  GT
  *MonomialOrder> lexO [1,0,0] [0,1,0]
  GT
```

$>_{lex}$ is a monomial ordering Since the number of variables is finite (n in $\mathbb{K}[x_1, \cdots, x_n]$), the above algorithm will terminate, i.e., all two monomials α, β are in one of

$$\alpha >_{lex} \beta, \alpha = \beta, \beta >_{lex} \alpha. \tag{2.97}$$

[12] We use builtin list as an expression for a monomial in Haskell:

$$x^\alpha = x_1^{\alpha_1} * \cdots * x_n^{\alpha_n} \rightarrow [\alpha_1, \cdots, \alpha_n] \tag{2.96}$$

So $>_{lex}$ is total.

Since for every entry of $\forall\gamma$,

$$(\alpha_i + \gamma_i) - (\beta_i + \gamma_i) = \alpha_i - \beta_i, \tag{2.98}$$

we have $\forall\gamma$,

$$\alpha >_{lex} \beta \Leftrightarrow \alpha + \gamma >_{lex} \beta + \gamma. \tag{2.99}$$

Finally, for every entry,

$$\alpha_i = \alpha_i - 0 \geq 0 \Leftrightarrow \alpha \geq_{lex} 0 \tag{2.100}$$

since all the entry in α is positive definite in $\mathbb{N}$. Therefore, $>_{lex}$ is a monomial ordering.

■

Graded Lexicographic order $>_{grlex}$

For $\alpha, \beta \in \mathbb{N}^n$, define $\alpha >_{grlex} \beta$ iff

$$|\alpha| > |\beta| \tag{2.101}$$

or

$$|\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta \tag{2.102}$$

where

$$|\alpha| := \sum_i \alpha_i. \tag{2.103}$$

$$x * y^2 \quad >_{grLex} \quad y^3 * z^4 \tag{2.104}$$

$$x^3 * y^2 * z^4 \quad >_{grLex} \quad x^3 * y^2 * z \tag{2.105}$$

$$x \quad >_{grLex} \quad y \tag{2.106}$$

```
> grLex :: Monomial -> Monomial -> Ordering
> grLex [] [] = EQ
> grLex a b
>   | sum a > sum b = GT
>   | sum a < sum b = LT
>   | otherwise = lexO a b
```

```
  *MonomialOrder> grLex [1,2,3] [3,2,0]
  GT
  *MonomialOrder> grLex [1,2,4] [1,1,5]
  GT
```

$>_{grLex}$ **is a monomial ordering** $>_{grLex}$ is clearly total order, since the comparison process will terminate in finite steps.

$\forall\gamma$, we have already seen $\alpha >_{lex} \beta \Leftrightarrow \alpha + \gamma >_{lex} \beta + \gamma$ in $>_{lex}$ case, and

$$|\alpha + \gamma| > |\beta + \gamma| \Leftrightarrow |\alpha| > |\beta| \tag{2.107}$$

since $|\alpha + \gamma| = |\alpha| + |\gamma|$. So $\gamma \in \mathbb{N}^n$,

$$\alpha >_{grLex} \beta \Leftrightarrow \alpha + \gamma >_{grLex} \beta + \gamma. \tag{2.108}$$

Finally, $\forall\alpha$ is positive definite,

$$|\alpha| \geq 0 \Rightarrow \alpha \geq_{grLex} 0. \tag{2.109}$$

■

Graded Reversed Lex

For $\alpha, \beta \in \mathbb{N}^n$, define $\alpha >_{grevlex} \beta$ iff

$$|\alpha| > |\beta| \tag{2.110}$$

or

$|\alpha| = |\beta|$ and the rightmost nonzero entry of difference in $\mathbb{N}^n$ is negative. (2.111)

$$\begin{aligned} x^4 * y^7 * z &\quad >_{gRevLex} \quad x^4 * y^2 * z^3 && (2.112) \\ x * y^5 * z^2 &\quad >_{gRevLex} \quad x^4 * y * z^3 && (2.113) \end{aligned}$$

```
> gRevLex :: Monomial -> Monomial -> Ordering
> gRevLex [] [] = EQ
> gRevLex a b
>   | sum a > sum b = GT
>   | sum a < sum b = LT
>   | otherwise = helper (reverse a) (reverse b)
>   where
>     helper (a:as) (b:bs)
>       | a < b     = GT
>       | otherwise = helper as bs
```

```
  *MonomialOrder> gRevLex [4,7,1] [4,2,3]
  GT
  *MonomialOrder> gRevLex [1,5,2] [4,1,3]
  GT
```

$>_{gRevLex}$ is a monomial ordering This comparison algorithm terminate finitely, so $>_{gRevLex}$ is a total order, and the comparison does not change under $\alpha, \beta \leftrightarrow \alpha + \gamma, \beta + \gamma$. In addition, $>_{gRevLex}$ is positive definite since

$$|\alpha| \geq 0 \Rightarrow \alpha \geq_{grLex} 0. \tag{2.114}$$

■

2.5 The Hilbert Basis Theorem and Gröbner Bases

2.5.1 Definition of the ideal of leading terms

Let $I \subset \mathbb{K}[x_1, \cdots, x_n]$ be an ideal other than $\{0\}$. Define a set of leading terms of I,

$$LT(I) := \{\, LT(f) |\, f \in I\} \tag{2.115}$$

and the ideal generated by that set:

$$\langle LT(I) \rangle := \langle \{\, LT(f) |\, f \in I\} \rangle \, . \tag{2.116}$$

2.5.2 Trivial inclusion

For $I = \langle f_1, \cdots, f_s \rangle$, then $\langle LT(f_1), \cdots, LT(f_s) \rangle \subset \langle LT(I) \rangle$.

Proof

By definition, the leading term of f_1 is

$$LT(f_1) \in \langle LT(I) \rangle \, . \tag{2.117}$$

This means $\forall$ generators of the ideal $\langle LT(f_1), \cdots, LT(f_s) \rangle$ is in $\langle LT(I) \rangle$, and

$$\langle LT(f_1), \cdots, LT(f_s) \rangle \subset \langle LT(I) \rangle \tag{2.118}$$

■

Example

$\langle LT(I)\rangle$ can be strictly larger than $\langle LT(f_1), \cdots, LT(f_s)\rangle$.

Consider

$$\begin{aligned} f_1 &:= x^3 - 2*x*y && (2.119)\\ f_2 &:= x^2*y - 2*y^2 + x && (2.120)\\ I &:= \langle f_1, f_2\rangle && (2.121)\end{aligned}$$

and use the grlex ordering on monomial in $\mathbb{K}[x, y]$. Then we have

$$\begin{aligned} -y*f_1 + x*f_2 &= -y*(x^3 - 2*x*y) + x*(x^2*y - 2*y^2 + x) && (2.122)\\ &= x^2 && (2.123)\end{aligned}$$

so that

$$x^2 \in I. \qquad (2.124)$$

Thus

$$LT(x^2) = x^2 \in \langle LT(I)\rangle\,, \qquad (2.125)$$

but x^2 is not divisible by leading terms

$$\begin{aligned} LT(f_1) &:= x^3 && (2.126)\\ LT(f_2) &:= x^2*y, && (2.127)\end{aligned}$$

therefore,

$$x^2 \notin \langle LT(f_1), LT(f_2)\rangle\,. \qquad (2.128)$$

This example shows that

$$\langle LT(f_1), LT(f_2)\rangle \subsetneq \langle LT(I)\rangle\,. \qquad (2.129)$$

■

2.5.3 $\langle LT(I)\rangle$ is a monomial ideal, and finitely generated

$\forall I \subset \mathbb{K}[x_1, \cdots, x_n]$ be an ideal, then

$$\langle LT(I)\rangle \qquad (2.130)$$

is a monomial ideal, and there is a finite set of generators $\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle$.

Proof

By definition,

$$\langle LT(I)\rangle := \langle\{\, LT(f) |\, f \in I\}\rangle \tag{2.131}$$

and $\forall f \in I$,

$$f \neq 0 \Rightarrow \exists c \in \mathbb{K}, \text{ s.t. } c * LT(f) \text{ is a monomial.} \tag{2.132}$$

If we write such a monomial g, then

$$\langle LT(I)\rangle := \langle\{\, g \in I |\, g (\neq 0) \text{ is a monomial}\}\rangle \tag{2.133}$$

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

Since we have proved that $\langle LT(I)\rangle$ is a monomial ideal, Dickson's lemma in §2.4.3 tells us that there is a finite number of monomials:

$$\langle LT(I)\rangle = \langle g_1, \cdots, g_t\rangle\,, \tag{2.134}$$

but since g's are monomials

$$\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle\,. \tag{2.135}$$

■

2.5.4 Hilbert Basis Theorem

Every ideal $I \subset \mathbb{K}[x_1, \cdots, x_n]$ has a finite generators.

Proof

If $I = \{0\}$, this singleton set $\{0\}$ is certainly finite.[13]

If I contains some nonzero polynomial, we can construct a finite generating set for I as follows. By §2.5.3, there is a set of finite $g_1, \cdots, g_t \in I$ s.t. $\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle$. We claim that $I = \langle g_1, \cdots, g_t\rangle$.

Since each g's are in I,

$$\langle g_1, \cdots, g_t\rangle \subset I. \tag{2.136}$$

Conversely, $\forall f \in I$, by the division algorithm in §2.3.2 we can divide f by the ideal $\langle g_1, \cdots, g_t\rangle$:

$$f = a_1 * g_1 + \cdots + a_t * g_t + r, \tag{2.137}$$

[13] Here we have two different $\{0\}$, the first one is a trivial ideal (as a structured set), and the other one is a singleton set of zero.

where no term of r is divisible by $LT(g_1), \cdots, LT(g_t)$. Now

$$r = f - (a_1 * g_1 + \cdots + a_t * g_t) \in I \tag{2.138}$$

If $r \neq 0$, then

$$LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle \,, \tag{2.139}$$

but by §2.4.2, there is some $LT(g_i)$ s.t.

$$LT(r) \sqsupseteq LT(g_i) \tag{2.140}$$

since $\langle LT(g_1), \cdots, LT(g_t) \rangle$ is an monomial ideal by §2.5.3 and $LT(r)$ is a term (i.e., a monomial times a coefficient). This clearly contradicts our definition of remainder, and consequently,

$$r = 0 \Leftrightarrow f = a_1 * g_1 + \cdots + a_t * g_t. \tag{2.141}$$

Thus

$$f \in \langle g_1, \cdots, g_t \rangle \tag{2.142}$$

and this means

$$I \subset \langle g_1, \cdots, g_t \rangle \,. \tag{2.143}$$

Finally we have

$$I = \langle g_1, \cdots, g_t \rangle \,. \tag{2.144}$$

■

2.5.5 Definition of Gröbner basis

Let us fix a monomial order $>$. A finite subset of given ideal I

$$G := \{g_1, \cdots, g_t\} \subset I \tag{2.145}$$

is a Gröbner basis iff

$$\langle LT(g_1), \cdots, LT(g_t) \rangle = \langle LT(I) \rangle \tag{2.146}$$

holds.[14]

Informally, a set $G := \{g_1, \cdots, g_t\} \subset I$ of generators is a Gröber basis iff the leading of all element of I is divisible by one of the $LT(g_i)$.

[14] From §2.5.2, we already have $\langle LT(g_1), \cdots, LT(g_t) \rangle \subset \langle LT(I) \rangle$, so $\langle LT(g_1), \cdots, LT(g_t) \rangle \supset \langle LT(I) \rangle$ is the essential condition for G is a Gröbner basis. I personally call G is "gröbner" if

$$\langle LT(g_1), \cdots, LT(g_t) \rangle \supset \langle LT(I) \rangle \tag{2.147}$$

holds, (indeed $\langle LT(g_1), \cdots, LT(g_t) \rangle = \langle LT(I) \rangle$ holds).

2.5.6 Every nontrivial ideal has a Gröbner basis

The proof of Hilbert Basis Theorem in §2.5.4 also establishes the following result.

Fix a monomial order $>$. All ideal $I \subset \mathbb{K}[x_1, \cdots, x_n]$ other than $\{0\}$ has a Gröbner basis. Furthermore, any Gröbner basis for an ideal I is a basis of I.

Proof

Given a nonzero ideal I, take

$$G = \{g_1, \cdots, g_t\} \tag{2.148}$$

of its Hilbert Basis which generates $I = \langle g_1, \cdots, g_t \rangle$ (2.144) (for the second claim).

This Hilbert basis has the following property:

$$\langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle \, . \tag{2.149}$$

(see also §2.5.3). This is indeed the condition for being a Gröbner basis.
■

2.5.7 The Ascending Chain Condition

Let

$$I_0 \subset I_1 \subset I_2 \subset I_3 \subset \cdots \, . \tag{2.150}$$

be an ascending chain of ideals in $\mathbb{K}[x_1, \cdots, x_n]$. Then, there exists an $m \leq 1$ s.t.

$$I_m = I_{m+1} = I_{m+2} \cdots \, . \tag{2.151}$$

That is, the ascending chain will have stabilized after finite steps m.

Proof

Given an ascending chain of ideal, let us define a set

$$I := \bigcup_{j \geq 0}^{\infty} I_j , \tag{2.152}$$

and we shall show that I is an ideal.[15] First, since $0 \in \forall I_j$ and $0 \in I$. Next, if $f, g \in I$, then we can put

$$f \in I_j, g \in I_k, j \leq k, \tag{2.153}$$

without loss of generality. We have assumed that the chain is ascending, so $I_j \subset I_k$ and

$$f, g \in I_k \Rightarrow f + g \in I_k \tag{2.154}$$

since I_k is an ideal, and we get

$$f + g \in I. \tag{2.155}$$

Similarly, $\forall f \in I$, there is I_j s.t.

$$f \in I_j \Rightarrow \forall h \in \mathbb{K}[x_1, \cdots, x_n], h * f \in I_j, \tag{2.156}$$

hence $\forall h \in \mathbb{K}[x_1, \cdots, x_n]$,

$$h * f \in I. \tag{2.157}$$

Therefore I is an ideal.

By the Hilbert Basis Theorem in §2.5.4, for this ideal, there is a finite generator:

$$I = \langle f_1, \cdots, f_s \rangle, \tag{2.158}$$

and each generator is in some ideal in the ascending chain:

$$f_i \in I_{j_i}, 1 \leq \forall i \leq s, j_i \geq 1 \tag{2.159}$$

We can take

$$m := \max j_i|_i \tag{2.160}$$

for $1 \leq i \leq s$, and then

$$I = \langle f_1, \cdots, f_s \rangle \subset I_m \subset I_{m+1} \subset \cdots \subset I. \tag{2.161}$$

As a result, the ascending chain stabilizes with I_m and

$$I = \langle f_1, \cdots, f_s \rangle \subset I_m = I_{m+1} = \cdots = I. \tag{2.162}$$

■

[15] See the definition in §1.4.1.

Note

This "every ascending chain of ideals in $\mathbb{K}[x_1, \cdots, x_n]$ stabilizes in finite steps" is often called the ascending chain condition (ACC).

We have used the Hilbert basis in the proof of ACC, but ACC is, actually, equivalent to the Hilbert Basis Theorem. In §2.9.2, we will treat ACC more precisely.

Here we prove Hilbert Basis Theorem without using Hilbert basis; if $I \subset \mathbb{K}[x_1, \cdots, x_n]$ is NOT finitely generated, then we can select an infinite generating sequence s.t., $I_i := \langle f_1, \cdots, f_i \rangle$. This is an ascending chain of ideals $I_1 \subset I_2 \subset \cdots$ which does NOT stabilize, but it contradicts our ACC. ■

2.5.8 Definition of the affine variety of an ideal

Let $I \subset \mathbb{K}[x_1, \cdots, x_n]$ be an ideal. The affine variety $\mathbb{V}(I)$ of the ideal I is defined by

$$\mathbb{V}(I) := \{ a \in \mathbb{K}^n \,|\, \forall f \in I, f(a) = 0 \} . \tag{2.163}$$

2.5.9 Varieties of ideals is well-defined

Let $\mathbb{V}(I)$ be an affine variety of an ideal I. Then, there is a finite generating set and

$$\mathbb{V}(I) = \mathbb{V}(f_1, \cdots, f_s) \tag{2.164}$$

holds.[16] So, the varieties of ideals are well defined.

Proof

By the Hilbert Basis Theorem §2.5.4, we have a finite generator for the ideal I:

$$I = \langle f_1, \cdots, f_s \rangle . \tag{2.165}$$

$\forall a \in \mathbb{V}(I)$, by definition

$$\forall f \in I, f(a) = 0, \tag{2.166}$$

and since $I = \langle f_1, \cdots, f_s \rangle$, we get

$$f_1(a) = \cdots = f_s(a) = 0. \tag{2.167}$$

[16] The left hand side is defined in §1.2.1.

Thus $a \in \mathbb{V}(f_1, \cdots, f_s)$ and

$$\mathbb{V}(I) \subset \mathbb{V}(f_1, \cdots, f_s) \tag{2.168}$$

Conversely, $\forall a \in \mathbb{V}(f_1, \cdots, f_s)$, then by definition,

$$f_1(a) = \cdots = f_s(a) = 0. \tag{2.169}$$

Since $I = \langle f_1, \cdots, f_s \rangle$, we can write

$$\forall f \in I, f = \sum_i h_i * f_i \tag{2.170}$$

and

$$\forall f \in I, f(a) = \sum_i h_i(a) * f_i(a) = \sum_i h_i(a) * 0 = 0. \tag{2.171}$$

This means that $a \in \mathbb{V}(I)$ and

$$\mathbb{V}(I) \supset \mathbb{V}(f_1, \cdots, f_s) \tag{2.172}$$

Therefore we have

$$\mathbb{V}(I) = \mathbb{V}(f_1, \cdots, f_s) \tag{2.173}$$

■

2.6 Properties of Gröbner Bases

From this section, we will omit $*$ symbol to indicate the multiplication.

2.6.1 Unique reminder properties

Let

$$G := \{g_1, \cdots, g_t\} \subset I \tag{2.174}$$

be a Gröbner basis[17] for an ideal $I \subset \mathbb{K}[x_1, \cdots, x_n]$. Then $\forall f \in \mathbb{K}[x_1, \cdots, x_n]$, there is a unique reminder $r \in \mathbb{K}[x_1, \cdots, x_n]$ with the following properies:

1. No term of r is divisible by any of $LT(g_1), \cdots, LT(g_t)$:

$$r \sqsubset LT(g_1), \cdots, r \sqsubset LT(g_t). \tag{2.175}$$

[17] This inclusion is for underlying sets, so G is just a set.

2. There is $g \in I$ s.t.
$$f = g + r. \tag{2.176}$$
In particular, r is "the" unique reminder on division of f by G.[18]

Proof

The division algorithm in §2.3.2 gives us
$$f = a_1 g_1 + \cdots + a_t g_t + r, \tag{2.177}$$
where r satisfies 1st condition. By putting
$$g := a_1 g_1 + \cdots + a_t g_t, \tag{2.178}$$
we can also satisfy 2nd condition.

To prove the uniqueness, let us suppose
$$g + r = f = g' + r' \tag{2.179}$$
satisfy both properties. Then we have
$$g - g' = r' - r \in I. \tag{2.180}$$
If $r \neq r'$, then the leading term is in $\langle LT(I) \rangle$:
$$LT(r' - r) \in \langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle . \tag{2.181}$$
Here we have assumed G be a Gröbner basis (see the definition §2.5.5), and this leads equality. That is, the monomial $LT(r' - r)$ is in the monomial ideal $\langle LT(g_1), \cdots, LT(g_t) \rangle$. By §2.4.2, it follows that
$$1 \leq \exists i \leq t \text{ s.t. } LT(r' - r) \sqsupseteq LT(g_i) \tag{2.182}$$
holds.[19] This, however, contradicts our division algorithm; no term in r, r' is divisible by $LT(g_1), \cdots, LT(g_t)$. Therefore we have a unique reminder
$$r' = r \tag{2.183}$$
and $g - g' = r' - r = 0$ implies
$$g' = g. \tag{2.184}$$
■

[18] Here G is just a set, not an ordered set, since this unique reminder does not depend on the order of g_i's.

[19] Pronounce it as "$LT(r' - r)$ is divisible by some $LT(g_i)$".

Note

This unique reminder properties is sometimes taken as the definition of a Gröber basis.[20]

2.6.2 Reminder and normal forms

The remainder r is called the normal form of f with respect to the Gröbner basis $G := \{g_1, \cdots, g_t\}$.

We will write

$$\bar{f}^F \tag{2.185}$$

as the remainder on division of f by the ordered tuple [21]

$$F := (f_1, \cdots, f_s). \tag{2.186}$$

If F is a Gröbner basis (for $f_1, \cdots, f_s$), then we can regard F as merely a set, since we have shown the uniqueness of the reminder in §2.6.1.

Sometimes, we also write

$$f \overset{F}{\to} r \tag{2.187}$$

as a division process, r is the reminder of f by the tuple F. Using this notation, the property in §2.6.1 becomes the following statement; if G is gröbner, then $\forall f \in \mathbb{K}[x_1, \cdots, x_n]$,

$$\exists! r \in \mathbb{K}[x_1, \cdots, x_n] \text{ s.t. } f \overset{G}{\to} r. \tag{2.188}$$

2.6.3 An ideal membership condition

Let $G := \{g_1, \cdots, g_t\}$ be a Gröbner basis for an ideal $I \subset \mathbb{K}[x_1, \cdots, x_n]$. Then $f \in I$ iff the reminder on division of f by G is zero.

Proof

Now we have

$$I = \langle g_1, \cdots, g_t \rangle \tag{2.189}$$

[20] We will summarize several equivalent statements for being Gröbner basis in §2.6.9.

[21] The remainder is also unique for the ordered tuple F.

of Gröbner basis for I. In §2.3.3 we have already proved $\Leftarrow$ part:

$$f \in I \Leftarrow f = a_1 g_1 + \cdots + a_t g_t. \tag{2.190}$$

Conversely, given $f \in I$, then

$$f = f + 0 \tag{2.191}$$

satisfies the two conditions in §2.6.1. The uniqueness implies that the reminder is zero, therefore

$$f \in I \Rightarrow f = a_1 g_1 + \cdots + a_t g_t. \tag{2.192}$$

■

Note

This property is also sometimes taken as the definition of a Gröbner basis, since we can show [22] that it is true iff G is "gröbner", i.e.,

$$\langle LT(g_1), \cdots, LT(g_t) \rangle = \langle LT(I) \rangle \tag{2.193}$$

holds.[23]

2.6.4 Definition of S-polynomials

Consider nonzero polynomials $f, g \in \mathbb{K}[x_1, \cdots, x_n]$, and multi degrees

$$\alpha := MD(f), \beta := MD(g), \tag{2.194}$$

then clearly,

$$x^\alpha = LM(f), x^\beta = LM(g). \tag{2.195}$$

Define a multi index

$$\gamma = (\gamma_1, \cdots, \gamma_n), \gamma_i := \max(\alpha_i, \beta_i), \tag{2.196}$$

and call

$$x^\gamma \tag{2.197}$$

[22] We will complete this statement in §2.6.8. Here in §2.6.3 we have proved $\Rightarrow$ part.

[23] See the definition of Gröbner basis in §2.5.5.

the least common multiple of leading monomials $LM(f), LM(g)$:

$$x^{\gamma} := LCM\left(LM(f), LM(g)\right). \tag{2.198}$$

Then we can define the S-polynomial of f and g:

$$S(f,g) := \frac{x^{\gamma}}{LT(f)}f - \frac{x^{\gamma}}{LT(g)}g \tag{2.199}$$

As we will see, S-polynomial is designed to cancel the leading terms, moreover, all cancellation of leading terms among polynomials of the same multi degree result from the combination of S-polynomials.

2.6.5 S-polynomial of I is in I

We will show the following property of S-polynomials for later use.

$$\forall f, g \in I, S(f,g) \in I. \tag{2.200}$$

Proof

Since $LG(f), LG(g) \sqsubseteq x^{\gamma}$ by definition of γ, and

$$\frac{x^{\gamma}}{LT(f)}, \frac{x^{\gamma}}{LT(g)} \in \mathbb{K}[x_1, \cdots, x_n], \tag{2.201}$$

we get

$$S(f,g) = \frac{x^{\gamma}}{LT(f)}f - \frac{x^{\gamma}}{LT(g)}g \in I. \tag{2.202}$$

Therefore, S-polynomial of I is in I.[24]
■

2.6.6 Lemma

Suppose we have a sum

$$\sum_{i=1}^{s} c_i f_i, c_i \in \mathbb{K}, \tag{2.203}$$

where $\forall i$,

$$MD(f_i) = \delta \in \mathbb{N}^n.$$

[24] This if the sum of elements in I with $\mathbb{K}[x_1, \cdots, x_n]$ "coefficients" form.

If the multi degree of this sum is strictly smaller than δ[25]

$$MD\left(\sum_{i=1}^{s} c_i f_i\right) < \delta, \tag{2.204}$$

then this sum $\sum_{i=1}^{s} c_i f_i$ is a linear combination, with $\mathbb{K}$ coefficients, of the S-polynomials

$$S(f_j, f_k), 1 \leq j, k \leq s. \tag{2.205}$$

Furthermore, each $S(f_j, f_k)$,

$$MD\left(S(f_j, f_k)\right) < \delta. \tag{2.206}$$

Proof

Let $d_i = LC(f_i)$, so that

$$c_i d_i = LC(c_i f_i). \tag{2.207}$$

Since all $c_i * f_i$ have multi degree δ and their sum has strictly smaller multi degree (eq.(2.204)). It follows that

$$\sum_i c_i d_i = 0, \tag{2.208}$$

i.e., the leading coefficient is cancelled out.

Define polynomials which has 1 as the leading coefficient:[26]

$$p_i := f_i/d_i = x^\delta + o(x^\delta). \tag{2.209}$$

[25] The cancellation of leading terms do occur.

[26] Here we used the "small o notation" $o(x^\delta)$ to indicate the terms that have smaller multi degree than x^δ.

Consider the telescoping sum[27]

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i d_i p_i \qquad (2.210)\\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots \\ &\quad +(c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) \\ &\quad +(c_1 d_1 + \cdots + c_s d_s) p_s \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots \\ &\quad +(c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s), \qquad (2.211)\end{aligned}$$

where we have used $\sum_i c_i * d_i = 0$. From our assumption, we have, $\forall i$,

$$LT(f_i) = d_i x^{\delta}, \qquad (2.212)$$

which implies that the least common multiple of $LT(f_j)$ and $LT(f_k)$ is x^{δ}. Thus

$$\begin{aligned}S(f_j, f_k) &= \frac{x^{\delta}}{LT(f_j)} f_j - \frac{x^{\delta}}{LT(f_k)} f_k \qquad (2.213)\\ &= \frac{x^{\delta}}{d_j x^{\delta}} f_j - \frac{x^{\delta}}{d_k x^{\delta}} f_k \qquad (2.214)\\ &= p_j - p_k. \qquad (2.215)\end{aligned}$$

Here, the leading terms of p_j, p_k are cancelled out and

$$MD\left(S(f_j, f_k)\right) = MD(p_j - p_k) < \delta. \qquad (2.216)$$

Now the above telescoping sum becomes

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots \\ &\quad +(c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s) \qquad (2.217)\\ &=: \sum_{j,k} c_{j,k} S(f_j, f_k). \qquad (2.218)\end{aligned}$$

This [28] is clearly a linear combination of the S-polynomials of $\mathbb{K}$ coefficients. ■

[27] From Wikipedia :

> ...whose partial sums eventually only have a fixed number of terms after cancellation.

[28] The last equality can be seen as the definition of $\mathbb{K}$ coefficients $c_{j,k}$'s.

2.6.7 Buchberger's Criterion

Let I be a polynomial ideal. Then an ordered tuple of basis $G = (g_1, \cdots, g_t)$ for I is a Gröbner basis for I iff for all pairs $j \neq k$, the remainder on division $S(g_j, g_k)$ by G is zero:[29]

$$G \text{ is gröbner} \Leftrightarrow \forall j \neq k, S(g_j, g_k) \overset{G}{\to} 0. \tag{2.219}$$

($\Rightarrow$) part

From §2.6.5,

$$S(g_j, g_k) = \frac{x^\gamma}{LT(g_j)} g_k - \frac{x^\gamma}{LT(g_k)} g_k \in I. \tag{2.220}$$

If G is a Gröbner basis for I, the remainder on division by G is 0 by §2.6.3.

($\Leftarrow$) part

It suffices to show that if $\forall j \neq k, S(g_j, g_k) \overset{G}{\to} 0$, then $\forall f \in I$, $LT(f) \in \langle LT(g_1), \cdots, LT(g_t)\rangle$, i.e., $\langle LT(I)\rangle \subset \langle LT(g_1), \cdots, LT(g_t)\rangle$.[30] We have assumed that G is a generator of I, so $\forall f \in I, \exists h_i$, s.t.,

$$f = \sum_i h_i g_i. \tag{2.221}$$

Construction of δ_0 Let us write

$$\begin{aligned} m(i) &:= MD(h_i g_i) && (2.222)\\ \delta &:= \max(m(i))|_i && (2.223)\end{aligned}$$

then clearly

$$MD(f) \leq \delta. \tag{2.224}$$

If $MD(f) < \delta$ then some cancellations of the leading terms must occur.

There is at least one combination of h_i's s.t. $f = \sum_i h_i g_i$, we can define the following non empty set:

$$\left\{ \delta = \delta(\{h_i\}) \middle| \forall \{h_i\} \text{ s.t. } f = \sum_i h_i g_i \right\} \subset \mathbb{N}^n. \tag{2.225}$$

[29] It seems like a Cauchy sequence.

[30] See the definition of Gröbner basis in §2.5.5, or eq.(2.147).

Since our monomial order is well-ordering,[31] we can pick up the minimal element, let's call it δ_0.

Lemma ($MD(f) = \delta_0$) Since we still have $MD(f) \leq \delta_0$, we can decompose $f = \sum_i h_i g_i$ as

$$\begin{aligned} f &= \sum_i h_i g_i \\ &= \sum_{m(i)=\delta_0} h_i g_i + \sum_{m(i)<\delta_0} h_i g_i \\ &= \sum_{m(i)=\delta_0} LT(h_i) g_i + \sum_{m(i)=\delta_0} \left(h_i - LT(h_i)\right) g_i + \sum_{m(i)<\delta_0} h_i g_i \end{aligned} \tag{2.226}$$

Both 2nd and 3rd terms clearly have strictly smaller multi degrees, e.g.,

$$MD\left(h_i - LT(h_i)\right) < \delta_0. \tag{2.227}$$

Therefore, if $MD(f) < \delta_0$, then we have

$$MD\left(\sum_{m(i)=\delta_0} LT(h_i) g_i\right) < \delta_0 \tag{2.228}$$

but we will see that $MD(f) < \delta_0$ contradicts our minimal assumption of δ_0.

Assuming $MD(f) < \delta_0$, all the terms in the 1st sum $\sum_{m(i)=\delta_0} LT(h_i) g_i$ have the same multi degree, since the summation is under $m(i) = \delta_0$:[32]

$$MD\left(LT(h_i) g_i\right) = \delta_0 \tag{2.229}$$

This is the form of §2.6.6 with $c_i = 1, f_i = LT(h_i) g_i$, and the lemma implies

$$\sum_{m(i)=\delta_0} LT(h_i) g_i = \sum_{j,k} c_{j,k} S\left(LT(h_j) g_j, LT(h_k) g_k\right). \tag{2.230}$$

[31] See eq.(2.9), multi degrees are essentially monomials.

[32] The leading term carries the maximum monomial, so $m(i) = MD(h_i g_i) = MD\left(LT(h_i) g_i\right)$.

By definition, since the least common multiple of $LT(h_i)g_i$'s is δ_0,

$$\begin{aligned} S\left(LT(h_j)g_j, LT(h_k)g_k\right) &= \frac{x^{\delta_0}}{LT\left(LT(h_j)g_j\right)}LT(h_j)g_j - (j \to k) && (2.231)\\ &= \frac{x^{\delta_0}}{LT(h_j)LT\left(g_j\right)}LT(h_j)g_j - (j \to k) && (2.232)\\ &= \frac{x^{\delta_0}}{LT\left(g_j\right)}g_j - (j \to k) && (2.233)\\ &= x^{\delta_0 - \gamma_{j,k}}S(g_j, g_k), && (2.234) \end{aligned}$$

where

$$\gamma_{j,k} := LCM\left(LM(g_j), LM(g_k)\right). \tag{2.235}$$

The 1st sum becomes

$$\sum_{m(i)=\delta_0} LT(h_i)g_i = \sum_{j,k} c_{j,k} x^{\delta_0 - \gamma_{j,k}} S(g_j, g_k). \tag{2.236}$$

Now we use our hypothesis $S(g_j, g_k) \overset{G}{\to} 0$, i.e., the division algorithm implies that there exists $a_{i,j,k} \in \mathbb{K}[x_1, \cdots, x_n]$ s.t.

$$S(g_j, g_k) = \sum_i a_{i,j,k} g_i \tag{2.237}$$

By eq.(2.24), we have

$$MD\left(S(g_j, g_k)\right) \geq MD(a_{i,j,k} g_i). \tag{2.238}$$

Therefore, the right hand side of eq.(2.236) becomes

$$c_{j,k} x^{\delta_0 - \gamma_{j,k}} \sum_i a_{i,j,k} g_i = \sum_i c_{j,k}(x^{\delta_0 - \gamma_{j,k}} a_{i,j,k}) g_i = \sum_i c_{j,k} b_{i,j,k} g_i, \tag{2.239}$$

where

$$b_{i,j,k} := x^{\delta_0 - \gamma_{j,k}} a_{i,j,k}. \tag{2.240}$$

Similarly, by eq.(2.24), we have[33]

$$\delta_0 > MD\left(x^{\delta_0 - \gamma_{j,k}} S(g_j, g_k)\right) \geq MD(b_{i,j,k} g_i) \tag{2.241}$$

[33] See eq.(2.228).

for all possible combinations.

Finally, eq.(2.236) becomes

$$\begin{aligned}
\sum_{m(i)=\delta_0} LT(h_i)g_i &= \sum_{j,k} c_{j,k} x^{\delta_0-\gamma_{j,k}} S(g_j,g_k) \\
&= \sum_{j,k}\sum_i c_{j,k} b_{i,j,k} g_i \\
&= \sum_i \left(\sum_{j,k} b_{i,j,k} c_{j,k}\right) g_i \qquad (2.242) \\
&= \sum_i \tilde{h}_i g_i \qquad (2.243)
\end{aligned}$$

and eq.(2.241) implies

$$MD(\tilde{h}_i g_i) < \delta_0, \forall i. \qquad (2.244)$$

Now, by eq.(2.243),

$$\begin{aligned}
f &= \sum_{m(i)=\delta_0} LT(h_i)g_i + \sum_{m(i)=\delta_0} (h_i - LT(h_i))\, g_i + \sum_{m(i)<\delta_0} h_i g_i \\
&= \sum_i \tilde{h}_i g_i + \sum_{m(i)=\delta_0} (h_i - LT(h_i))\, g_i + \sum_{m(i)<\delta_0} h_i g_i. \qquad (2.245)
\end{aligned}$$

We have shown that if we suppose $MD(f) < \delta_0$, then we get eq.(2.244), and this shows all three sums have strictly smaller multi degrees than δ_0. This, however, contradicts the minimal assumption of δ_0, therefore we have[34]

$$MD(f) = \delta_0. \qquad (2.246)$$

$LT(f)$ is divisible by $LT(g_j)|_j$ Since we have shown $MD(f) = \delta_0$ (eq.(2.246)), then

$$MD(f) = \delta_0 = \max\left(MD(h_i g_i)\right)|_i \geq MD(g_j), \forall j. \qquad (2.247)$$

This tells us that the leading term of f is divisible by any generators

$$LT(f) = LC(f) * x^{\delta_0} \sqsupseteq LT(g_j), \forall j. \qquad (2.248)$$

[34] Actually, we show $MD(f) \not< \delta_0$, but we already have eq.(2.224), thus we get this equality.

and this is equivalent to

$$LT(f) \in \langle LT(g_1), \cdots, LT(g_t) \rangle . \qquad (2.249)$$

Therefore, G is gröbner.

■

2.6.8 Ideal membership condition, with S-polynomials

With this Buchberger's Criterion, we can show the the divisibility is the property of Gröbner basis as we stated in §2.6.3; if G is a basis for I with $\forall f \in I$,

$$f \overset{G}{\to} 0, \qquad (2.250)$$

then G is gröbner.

Proof

Let $G = \{g_1, \cdots, g_t\}$, then it suffices to show $S(g_j, g_k) \overset{G}{\to} 0$. By §2.6.5

$$S(g_j, g_k) = \frac{x^\gamma}{LT(g_j)} g_k - \frac{x^\gamma}{LT(g_k)} g_k \in I \qquad (2.251)$$

where $\gamma = LCM\left(LM(g_j), LM(g_k)\right)$, and by our assumption,

$$S(g_j, g_k) \overset{G}{\to} 0. \qquad (2.252)$$

This is iff condition for gröbner G.

■

2.6.9 Several "isGröbner"'s

We have several conditions for gröbner property of $G = \{g_1, \cdots, g_t\}$ in a polynomial ideal I. By definition, eq.(2.147); if G satisfies

$$\langle LT(g_1), \cdots, LT(g_t) \rangle \supset \langle LT(I) \rangle ,$$

then we call this G gröbner.[35] From Buchberger's Criterion §2.6.7:

$$G \text{ is gröbner} \Leftrightarrow S(g_j, g_k) \overset{G}{\to} 0.$$

[35] As we saw, this inclusion provides

$$\langle LT(g_1), \cdots, LT(g_t) \rangle = \langle LT(I) \rangle .$$

From §2.6.3 and §2.6.8,

$$G \text{ is gröbner} \Leftrightarrow \forall f \in I, f \overset{G}{\to} 0. \tag{2.253}$$

In addition, from §2.6.1, $\forall f \in \mathbb{K}[x_1, \cdots, x_n]$, we have proved the sufficient condition[36]

$$G \text{ is gröbner} \Rightarrow \exists! r \in \mathbb{K}[x_1, \cdots, x_n] \text{ s.t. } f \overset{G}{\to} r.$$

2.6.10 Unique remainder among different Gröbner bases

Let us fix a monomial order $<$. Consider $\forall f \in I$ and two Gröbner bases G, G' for I, then the remainders of f by G and that of G' are the same.

Proof

From §2.6.1, there exists $g, g' \in I$ s.t.

$$g + r = f = g' + r', \tag{2.254}$$

where

$$f \overset{G}{\to} r, f \overset{G'}{\to} r', \tag{2.255}$$

and r, r' satisfy eq.(2.23), i.e., $r \sqsubset LT(g_j)\big|_j$. Let us suppose $r' - r \neq 0$. Since the differences are in I

$$g - g' = r' - r \in I, \tag{2.256}$$

their normal forms become 0 by §2.6.8. This contradicts the condition for the remainder (eq.(2.23)), they are not divisible by any leading terms of generators. Therefore we have

$$r = r'. \tag{2.257}$$

■

[36] From our source book,

> In fact, Groebner bases can be characterized by the uniqueness of the remainder – see Theorem 5.35 of BECKER and WEISPFENNING(1993) for this and other conditions equivalent to being a Groebner basis.

2.7 Buchberger's Algorithm

§2.6.7 gives us the function of the following type

$$\texttt{Basis -> Bool} \tag{2.258}$$

So, we will find a constructive algorithm of Gröbner basis:

$$\texttt{Basis -> GroebnerBasis} \tag{2.259}$$

2.7.1 Buchberger's Algorithm

Let $I = \langle f_1, \cdots, f_s \rangle \neq \{0\}$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite steps by the following algorithm:

Pseudo code

```
Input:  F = (f_1, .., f_s)
Output: G = (g_1, .., g_t)

G := F
REPEAT
  G' := G

  FOR each pair (p,q), p \= q in G' DO
    S(p,q) -> s
    IF s \= 0 THEN G := G \cup {s}
UNTIL G == G'
```

That is, for arbitrary generator of an ideal $I = \langle f_1, \cdots, f_s \rangle$, the out put is a Gröbner basis for I.

Proof

Let us define, for a generating set $G = \{g_1, \cdots, g_t\}$,

$$\langle G \rangle := \langle g_1, \cdots, g_t \rangle \tag{2.260}$$

$$\langle LT(G) \rangle := \langle LT(g_1), \cdots, LT(g_t) \rangle \tag{2.261}$$

for later uses. Using this notation, the generator G is a Gröbner basis for I iff $\langle LT(I) \rangle = \langle LT(G) \rangle$.

At every stage of the algorithm, we shall show $G' \subset I$, where

$$I = \langle f_1, \cdots, f_s \rangle . \tag{2.262}$$

This is true at the first step:

$$G \subset I. \tag{2.263}$$

In some intermediate step, assume $G' \subset I$. Since $\forall p, q \in G'$,

$$S(p,q) \in G' \tag{2.264}$$

we get

$$S(p,q) \overset{G'}{\to} s \in G' \tag{2.265}$$

since $S(p,q) \overset{G'}{\to} s$ is equal to

$$\exists g' \in G' \text{ s.t. } S(p,q) = g' + s, \tag{2.266}$$

therefore

$$s = S(p,q) - g' \in G'. \tag{2.267}$$

If $s = 0$, then the next G' is unchanged $G' \mapsto G'$, else ($s \neq 0$), let us add s into G':

$$G' \mapsto G' \cup \{s\} \subset I. \tag{2.268}$$

When this algorithm terminates, we'll get $G = G'$. This holds when

$$\forall p, q \in G', S(p,q) \overset{G'}{\to} 0, \tag{2.269}$$

i.e., G' is gröbner (see §2.6.7).

Finally, we claim that the algorithm terminates finitely. After one step of main loop, if $G' \neq G$ then

$$G' \mapsto G'' := G' \cup \{s\}. \tag{2.270}$$

Since the reminder s is strictly smaller than any generators of G' $s \sqsubset LT(g_i'), g_i' \in G'$ (see eq.(2.23)),

$$LT(s) \notin LT(G') \tag{2.271}$$

but by definition

$$LT(s) \in LT(G''). \tag{2.272}$$

So

$$\left\langle LT(G') \right\rangle \subsetneq \left\langle LT(G'') \right\rangle. \tag{2.273}$$

The ACC in §2.5.7 implies that after a finite number of iterations, this chain will stabilize in finite steps, so that

$$\langle LT(G) \rangle \subset \cdots \subset \left\langle LT(G^{(m)}) \right\rangle = \left\langle LT(G^{(m+1)}) \right\rangle \tag{2.274}$$

happen eventually. This occur when we meet $G^{(m+1)} = G^{(m)}$, therefore this algorithm will terminate finitely.
■

2.7.2 An elimination method

Let G be a Gröbner basis for the polynomial ideal I. $\forall p \in G$ s.t.

$$LT(p) \in \langle LT(G - \{p\}) \rangle, \tag{2.275}$$

then the set $G - \{p\}$ is also a Gröbner basis.

Proof

By definition, this Gröbner basis G satisfies

$$\langle LT(I) \rangle = \langle LT(G) \rangle. \tag{2.276}$$

We can write

$$\begin{aligned} G &:= \{g_1, \cdots, g_t, p\} & (2.277) \\ G - \{p\} &:= \{g_1, \cdots, g_t\} & (2.278) \end{aligned}$$

If $q \in \langle LT(G - \{p\}) \rangle$, then we have $q \in \langle LT(G) \rangle$ automatically, and

$$\langle LT(G - \{p\}) \rangle \subset \langle LT(G) \rangle. \tag{2.279}$$

Conversely, if $LT(p) \in \langle LT(G - \{p\}) \rangle$, $\forall q \in \langle LT(G) \rangle$ we have an expression

$$q = \sum_i h_i * LT(g_i) + h * LT(p), \tag{2.280}$$

where $h, h_i \in \mathbb{K}[x_1, \cdots, x_n]$. But since $LT(p) \in \langle LT(G - \{p\}) \rangle$, we can decompose $LT(p)$ in $G - \{p\}$ and

$$q = \sum_i h'_i * LT(g_i), \tag{2.281}$$

and this implies $q \in \langle LT(G - \{p\}) \rangle$:

$$\langle LT(G - \{p\}) \rangle \supset \langle LT(G) \rangle \tag{2.282}$$

Therefore, we have

$$\langle LT(G - \{p\}) \rangle = \langle LT(G) \rangle \tag{2.283}$$

and

$$\langle LT(I) \rangle = \langle LT(G - \{p\}) \rangle . \tag{2.284}$$

■

2.7.3 Definition of minimal Gröbner bases

A minimal Gröbner basis for a polynomial ideal I is a Gröbner basis G for I s.t. the leading coefficients are normalized; $\forall p \in G$,

$$LC(p) = 1 \tag{2.285}$$

and

$$LT(p) \notin \langle LT(G - \{p\}) \rangle . \tag{2.286}$$

By adjusting the leading coefficients 1 and removing $LT(p) \in \langle LT(G - \{p\}) \rangle$ from an arbitrary Gröbner basis, we will arrive at this minimal Gröbner basis.

2.7.4 Definition of reduced Gröbner bases

A reduced Gröbner basis for a polynomial ideal I is a Gröbner basis G for I s.t. $\forall p \in G$,

$$LC(p) = 1 \tag{2.287}$$

and

$$\text{no monomial of } p \text{ lies in } \langle LT(G - \{p\}) \rangle . \tag{2.288}$$

In general, $g \in G$ is reduced for a Gröbner basis G iff no monomial of g is in $\langle LT(G - \{g\}) \rangle$.

2.7.5 A unique reduced Gröbner basis

In general, reduced Gröbner bases have the following nice property.

Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial order, I has a unique reduced Gröbner basis.

Proof

Let G be a minimal Gröbner basis for I. Our goal is to modify G until all of elements are reduced.

If $g \in G$ is reduced for G, then g is also reduced for any other minimal Gröbner basis G' of I that contains g and has the same set of leading terms,

$$LT(G) = LT(G'), \tag{2.289}$$

since the process of reducing only sees the leading terms $\langle LT(G - \{g\})\rangle$.

Next, given $g \in G$, let g' be the remainder by $G - \{g\}$

$$g \overset{G-\{g\}}{\to} g' \tag{2.290}$$

and let

$$G' := (G - \{g\}) \cup \{g'\} \tag{2.291}$$

be a new set.[37] We claim that this new G' is also a minimal Gröbner basis for I.

First,

$$LT(g') = LT(g) \tag{2.292}$$

since when we divide g by $G - \{g\}$, $LT(g)$ goes to the remainder because $LT(g)$ is not divisible by any element of $\langle LT(G - \{g\})\rangle$.[38] This shows that the generators and the monomial ideals are the same:

$$\begin{aligned} LT(G) &= LT(G') & (2.293)\\ \langle LT(G)\rangle &= \left\langle LT(G')\right\rangle . & (2.294)\end{aligned}$$

Since G is a Gröbner basis for I, G satisfies $\langle LT(I)\rangle = \langle LT(G)\rangle$ and so

$$\langle LT(I)\rangle = \left\langle LT(G')\right\rangle , \tag{2.295}$$

[37] This new set can be seen as the same G with g' replaced by g.

[38] We have assumed G is a minimal Gröbner basis for I, so $LT(g) \notin \langle LT(G - \{g\})\rangle$ eq.(2.286).

i.e., G' is also a Gröbner basis, and is minimum. Note that $g' \in G'$ is reduced for G' by construction.

Now, reduce all the element in G by using above process until they are all reduced. Since once an element is reduced, it stays reduced even if G changes due to other reducing processes. Thus, we end up with a reduced Gröbner basis.

Finally, we'll prove the uniqueness. Suppose $G, \tilde{G}$ be reduced Gröbner bases for I. Under reducing process $G \mapsto G' := (G - \{g\}) \cup \{g'\}$, the leading terms of generators are unchanged:

$$LT(G) = LT(\tilde{G}), \tag{2.296}$$

i.e. $\forall g \in G$,

$$\exists \tilde{g} \in \tilde{G} \text{ s.t. } LT(g) = LT(\tilde{g}). \tag{2.297}$$

Consider the difference $g - \tilde{g}$. Since this is in I,

$$g - \tilde{g} \overset{G}{\to} 0. \tag{2.298}$$

But we also know $LT(g) = LT(\tilde{g})$, the leading terms cancel in the difference. Since $G, \tilde{G}$ are reduced, we have

$$g - \tilde{g} \overset{G}{\to} g - \tilde{g} \tag{2.299}$$

but this is 0. Thus we get $g = g'$ and

$$G = \tilde{G}, \tag{2.300}$$

since we have shown that $\forall g \in G, \exists! g \in \tilde{G}$.
■

Note

A consequence of the uniqueness of the reduced Gröbner basis in §2.7.5 is we have an ideal equality algorithm.

Consider two sets of generators

$$\{f_1, \cdots, f_s\}, \{g_1, \cdots, g_t\} \tag{2.301}$$

and the ideals which are generated by f's and g's. Compute the reduced Gröbner bases for f's and g's. Then the ideals are equal iff the Gröbner bases are the same.[39]

[39] These Gröbner bases are merely sets, so we can compare them simply element by element.

2.8 Improvements on Buchberger's Algorithm

The most heaviest part of computation in Buchberger's Algorithm is the polynomial divisions. Hence, a good way to improve the efficiency of the algorithm would be to reduce the number of S-polynomials need to be considered.

2.8.1 Definition of $\rightarrow_G$

Fix a monomial order and let $G = \{g_1, \cdots, g_s\} \subset \mathbb{K}[x_1, \cdots, x_n]$. Given $f \in \mathbb{K}[x_1, \cdots, x_n]$, we say that f reduces to zero modulo G,[40]

$$f \rightarrow_G 0, \tag{2.302}$$

if f can be written in the form,

$$f = \sum_{i=1}^{t} a_i g_i \tag{2.303}$$

s.t., whenever $a_i g_i \neq 0$, we have

$$MD(f) \geq MD(a_i g_i). \tag{2.304}$$

2.8.2 $f \overset{G}{\rightarrow} 0$(division) $\Rightarrow f \rightarrow_G 0$(reduction to 0 modulo G)

Let $G = (g_1, \cdots, g_s)$ be an ordered tuple of elements in $\mathbb{K}[x_1, \cdots, x_n]$. Then $f \overset{G}{\rightarrow} 0$ implies $f \rightarrow_G 0$, though the converse is false in general.

Proof

Here we will do essentially the same discussion in §2.3.3. If $f \overset{G}{\rightarrow} 0$, by definition

$$f = \sum_{i=1}^{t} a_i g_i + 0, \tag{2.305}$$

and for $a_i g_i \neq 0$, they satisfy eq.(2.24),

$$MD(f) \geq MD(a_i g_i). \tag{2.306}$$

This shows that $f \rightarrow_G 0$.

The counterexample for ⇐ direction is in §2.3.3.[41]

■

[40] This is different from $\overset{G}{\rightarrow}$ of division algorithm in §2.6.2.

[41] If G is gröbner, both $\overset{G}{\rightarrow}$ and $\rightarrow_G$ are equivalent, see §2.6.3.

2.8.3 Gröbner basis criterion, a more general version

A basis $G = \{g_1, \cdots, g_s\}$ for an ideal $I \subset \mathbb{K}[x_1, \cdots, x_n]$ is a Gröbner basis iff $\forall i \neq j, S(g_i, g_j) \to_G 0$.

Proof

In the proof of §2.6.7, what we have used are the expressions

$$S(g_j, g_k) = \sum_i a_{i,j,k} g_i \tag{2.307}$$

with the conditions eq.(2.238)

$$MD\left(S(g_j, g_k)\right) \geq MD(a_{i,j,k} g_i) \tag{2.308}$$

for nonzero $a_{i,j,k}$. This is the same as $S(g_i, g_j) \to_G 0$ in §2.8.2, and

$$G \text{ is gröbenr} \Leftrightarrow S(g_i, g_j) \to_G 0. \tag{2.309}$$

■

2.8.4 Proposition

Given a finite set $G \subset \mathbb{K}[x_1, \cdots, x_n]$, suppose that we have $f, g \in G$ s.t.

$$LCM(LM(f), LM(g)) = LM(f) * LM(g). \tag{2.310}$$

This means that the leading monomials of f and g are relatively prime. Then $S(f, g) \to_G 0$.

If this condition eq.(2.310) holds, then this S-polynomial is guaranteed to reduce to zero, so we don't need to polynomial division on this particular $S(f, g)$.

Proof

For simplicity, we can assume $LC(f) = 1 = LC(g)$, i.e. $LT(f) = LM(f), LT(g) = LM(g)$ and

$$\begin{aligned} f &= LM(f) + p & (2.311)\\ g &= LM(g) + q & (2.312) \end{aligned}$$

Clearly,

$$\begin{aligned} MD\left(LM(f)\right) &> MD(p) & (2.313)\\ MD\left(LM(g)\right) &> MD(q). & (2.314) \end{aligned}$$

By definition of S-polynomial,

$$S(f,g) = \frac{x^\gamma}{LT(f)}f - \frac{x^\gamma}{LT(g)}g, \tag{2.315}$$

where $x^\gamma = LCM(LM(f), LM(g))$ satisfies eq.(2.310) and then

$$\begin{aligned} S(f,g) &= \frac{LM(f)*LM(g)}{LT(f)}f - \frac{LM(f)*LM(g)}{LT(g)}g && (2.316)\\ &= LM(g)f - LM(f)g && (2.317)\\ &= (g-q)f - (f-p)g && (2.318)\\ &= pg - qf. && (2.319) \end{aligned}$$

Since $f, g \in G$, we have

$$S(f,g) \to_G 0. \tag{2.320}$$

If the leading terms in pg and gf are the same, then

$$LM(p)LM(g) = LM(q)LM(f). \tag{2.321}$$

Since we have assumed eq.(2.310), this means

$$\exists h (\neq 0) \in \mathbb{K}[x_1, \cdots, x_n] \text{ s.t. } LM(p) = h * LM(f), LM(q) = h * LM(g). \tag{2.322}$$

It contradicts eq.(2.313) and eq.(2.314). Thus the leading terms in the last expression for $S(f,g)$ cannot cancel:

$$MD\left(S(f,g)\right) = \max\left(MD(pg), MD(qf)\right). \tag{2.323}$$

■

Note

This proof gives us a more efficient version of §2.8.3; to test for a Gröbner basis, we need only have

$$\forall i < j, S(g_i, g_j) \to_G 0, \tag{2.324}$$

where $LM(g_i), LM(g_j)$ are not relatively prime, see eq.(2.310).

Here is another way to improve, a kind of generalization of S-polynomials.

2.8.5 Definition of syzygies

Let $F = (f_1, \cdots, f_s)$ be a tuple of polynomials. A syzygy[42] on the leading terms $LG(f_1), \cdots, LT(f_s)$ of F is an s-tuple of polynomials

$$(h_1, \cdots, h_s) \in (\mathbb{K}[x_1, \cdots, x_n])^s \tag{2.325}$$

s.t.,

$$\sum_{i=1}^{s} h_i * LT(f_i) = 0. \tag{2.326}$$

We let $S(F)$ be the subset of $(\mathbb{K}[x_1, \cdots, x_n])^s$ consisting of all syzygies on the leading terms of F.

Let

$$e_i = (0, \cdots, 0, \underbrace{1}_{\text{i-th}}, 0, \cdots, 0) \in (\mathbb{K}[x_1, \cdots, x_n])^s \tag{2.327}$$

be a unit tuple, then a syzygy $S \in S(F)$ can be written as

$$S = \sum_{i=1}^{s} h_i e_i. \tag{2.328}$$

Given a pair, $i < j$,

$$(f_i, f_j) \subset F, \tag{2.329}$$

then

$$S_{ij} = \frac{x^\gamma}{LT(f_i)} e_i - \frac{x^\gamma}{LT(f_j)} e_j \tag{2.330}$$

gives a syzygy on the leading terms of F, where x^γ is the least common multiple of $LT(f_i), LT(f_j)$. In fact, the name S-polynomial is actually an abbreviation for "syzygy polynomial."

[42] From our source book;

> This word is used in astronomy to indicate an alignment of three planets or other heavenly bodies. The root is a Greek word meaning "yoke." In an astronomical syzygy, planets are "yoked together"; in a mathematical syzygy, it is polynomials that are "yoked."

2.8.6 Definition of homogeneous of multidegree

An element $S \in S(F)$ is homogeneous of multidegree α, where $\alpha \in \mathbb{N}^n$, provided that

$$S = (c_1 x^{\alpha(1)}, \cdots, c_s x^{\alpha(s)}), \tag{2.331}$$

where $c_i \in \mathbb{K}$ and $\alpha(i) + MD(f_i) = \alpha$, whenever $c_i \neq 0$.

2.8.7 ? Lemma

Every element of $S(F)$ can be written uniquely as a sum of homogeneous elements of $S(F)$. That is, $S(F)$ has a finite basis.

Proof

Let $S = (h_1, \cdots, h_s) \in S(F)$, i.e. $F = (f_1, \cdots, f_s)$ with

$$\sum_{i=1}^{s} h_i * LT(f_i) = 0. \tag{2.332}$$

2.8.8 ? Proposition

Given $F = (f_1, \cdots, f_s)$, every syzygy $S \in S(F)$ can be written as

$$S = \sum_{i<j} u_{ij} S_{ij}, \tag{2.333}$$

where $u_{ij} \in \mathbb{K}[x_1, \cdots, x_n]$ and the syzygy S_{ij} is defined in eq.(?)

2.8.9 ? Theorem

A basis $G = (g_1, \cdots, g_t)$ for an ideal I is a Gröbner basis iff for every element $S = (h_1, \cdots, h_t)$ in a homogeneous basis for the syzygies $S(G)$, we have

$$S \cdot G = \sum_{i=1}^{t} h_i g_i \rightarrow_G 0. \tag{2.334}$$

2.8.10 ? Proposition

Give $G = (g_1, \cdots, g_t)$, suppose that $S \subset \{S_{ij} | 1 \leq i < j \leq t\}$ is a basis of $S(G)$. In addition, suppose we have distinct elements $g_i, g_j, g_k \in G$ s.t.

$$LT(g_k) \text{ divides } LCM(LT(g_i), LT(g_j)) \tag{2.335}$$

IF $S_{ij}, S_{jk} \in \mathcal{S}$, then $\mathcal{S} - \{S_{ij}\}$ is also a basis of $S(G)$. (Note: If $i > j$, we set $S_{ij} = S_{ji}$.)

2.8.11 ? Theorem

Let $I = \langle f_1, \cdots, f_s \rangle$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm: $\cdots$

2.9 A side story on ACC

We have used Hilbert Basis Theorem in the proof of ACC §2.5.7, but ACC is independent from Hilbert Basis Theorem. First of all, we should give more precise definitions.

2.9.1 Chains, and ascending chains

Let $(S, \leq)$ be a non-empty partially ordered set. The subset $C \subset S$ is called a chain iff C is totally ordered, i.e.,

$$\forall c, c' \in C, \text{ either } c \leq c' \text{ or } c' \leq c. \tag{2.336}$$

The chain C is an ascending chain iff the elements of C are $\mathbb{N}$ indexed s.t.,

$$\forall k \in \mathbb{N}, c_k \leq c_{k+1}, \neg(\exists d \in C \text{ s.t. } c_k < d < c_{k+1}), \tag{2.337}$$

where $<$ is equivalent to ($\leq$ and $\neq$, i.e., $\lneq$).[43]

2.9.2 Two equivalent conditions for ACC

Let $(S, \leq)$ be a non-empty partially ordered set. Then the following conditions are equivalent.

[43] Descending chains are defined similarly.

1. (maximal) $\forall T \subset S$ of a partially ordered subset,
$$\exists m \in T \text{ s.t. } \neg(\exists n \in T \text{ s.t. } m \leq n). \tag{2.338}$$
2. (strict upper bound)[44] $\forall C \subset S$ of a chain,
$$\exists u \in C \text{ s.t. } \forall c \in C, c \leq u. \tag{2.339}$$
3. (ACC) $\forall C \subset S$ of an ascending chain, with $c_k|_{k\in\mathbb{N}} \in C$, then
$$\exists n \in \mathbb{N} \text{ s.t. } c_{n+1} = c_n. \tag{2.340}$$
That is, every ascending chain will terminate finitely:
$$C = \{c_0 \leq c_1 \leq \cdots \leq c_n\} \tag{2.341}$$

Proof

We prove 1. ⇒ 2. ⇒ 3. ⇒ 1.

(maximal) ⇒ (strict upper bound) Take
$$u := \max(C). \tag{2.342}$$
(strict upper bound) ⇒ (ACC) For
$$u := \text{upper bound}(C) \tag{2.343}$$
there should be $n \in \mathbb{N}$ s.t.
$$u = c_n. \tag{2.344}$$

(ACC) ⇒ (maximal) Consider $\forall T(\neq \emptyset) \subset S$. Suppose T has NO maximal element, then take an element $t_0 \in T$. We can take
$$t_1 \in (T - \{t_0\}) \text{ s.t. } t_0 < t_1, \tag{2.345}$$
since t_0 is not maximal. Inductively, we can take a subset
$$\{t_0 < t_1 < \cdots\} \subset T, \tag{2.346}$$
by Axiom of Choice.[45] However, this is an infinite (strictly) ascending chain, and contradicts ACC. Thus T has a maximal element.

■

[44] The upper bound is in S, in general.

[45] More rigorously, for non empty sets
$$T_0 := T, T_1 := T_0 - \{t_0\}, \cdots, T_n := T_{n-1} - \{t_{n-1}\} \tag{2.347}$$
there exists a choice function
$$t : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} T_i = T; n \mapsto t_n \in T_n. \tag{2.348}$$

Chapter 3

Elimination Theory

the Geometric Extension Theorem for (weak) Nullstellensatz

3.1 The Elimination and Extension Theorems

3.1.0 Example

Here is the list of equations that we will solve:

$$x^2 + y + z = 1 \tag{3.1}$$

$$x + y^2 + z = 1 \tag{3.2}$$

$$x + y + z^2 = 1 \tag{3.3}$$

Putting them into Maxima, we get the Gröbner basis for the ideal that is generated by above equations.

```
(%i1) load(grobner)$
(%i2) display2d:false$
(%i3) poly_reduced_grobner ([x^2+y+z-1, x+y^2+z-1, x+y+z^2-1],[x,y,z]);
(%o3) [z^2+y+x-1,(-z^2)+z+y^2-y,z^4+2*y*z^2-z^2,z^6-4*z^4+4*z^3-z^2]
```

where the default settings are

```
(%i5) poly_monomial_order;
(%o5) lex
(%i6) poly_grobner_algorithm;
(%o6) buchberger
```

If we set

```
(%i14) g: poly_reduced_grobner ([x^2+y+z-1, x+y^2+z-1, x+y+z^2-1],[x,y,z]);
(%o14) [z^2+y+x-1,(-z^2)+z+y^2-y,z^4+2*y*z^2-z^2,z^6-4*z^4+4*z^3-z^2]
(%i15) g[4], factor;
(%o15) (z-1)^2*z^2*(z^2+2*z-1)
```

we can solve the 4th Gröbner basis `g[4]` for z:

```
(%i16) solve(%,z);
(%o16) [z = (-sqrt(2))-1,z = sqrt(2)-1,z = 0,z = 1]
```

Substituting these solution in the rest equations, we'll get the full solutions.

```
(%i46) g, z=0;
(%o46) [y+x-1,y^2-y,0,0]
(%i47) solve(%, [x,y]);
(%o47) [[x = 1,y = 0],[x = 0,y = 1]]

(%i49) g, z=1;
(%o49) [y+x,y^2-y,2*y,0]
(%i50) solve(%, [x,y]);
(%o50) [[x = 0,y = 0]]

(%i52) g, z = (-sqrt(2))-1;
(%o52) [y+x+((-1)-sqrt(2))^2-1,y^2-y-sqrt(2)-((-1)-sqrt(2))^2-1,
        2*((-1)-sqrt(2))^2*y+((-1)-sqrt(2))^4-((-1)-sqrt(2))^2,
        ((-1)-sqrt(2))^6-4*((-1)-sqrt(2))^4+4*((-1)-sqrt(2))^3
                         -((-1)-sqrt(2))^2]
(%i53) solve(%, [x,y]);
(%o53) [[x = (-sqrt(2))-1,y = (-sqrt(2))-1]]

(%i55) g, z = sqrt(2)-1;
(%o55) [y+x+(sqrt(2)-1)^2-1,y^2-y+sqrt(2)-(sqrt(2)-1)^2-1,
        2*(sqrt(2)-1)^2*y+(sqrt(2)-1)^4-(sqrt(2)-1)^2,
        (sqrt(2)-1)^6-4*(sqrt(2)-1)^4+4*(sqrt(2)-1)^3-(sqrt(2)-1)^2]
(%i56) solve(%, [x,y]);
(%o56) [[x = sqrt(2)-1,y = sqrt(2)-1]]
```

Maxima can also solve these equations directly, and it's consistent:

```
(%i57) solve([x^2+y+z-1, x+y^2+z-1, x+y+z^2-1],[x,y,z]);
(%o57) [[x = 0,y = 0,z = 1],[x = sqrt(2)-1,y = sqrt(2)-1,z = sqrt(2)-1],
        [x = (-sqrt(2))-1,y = (-sqrt(2))-1,z = (-sqrt(2))-1],
        [x = 1,y = 0,z = 0],[x = 0,y = 1,z = 0]]
```

Here is the sketch of above process.

1. (Elimination) Find a polynomial which involved only one variable, say z.
2. (Extension) Putting each solution for above eliminated equation(s), extend these solutions of the original equations.

3.1.1 The elimination ideals

Given $I = \langle f_1, \cdots, f_s \rangle \subset \mathbb{K}[x_1, \cdots, x_n]$, the l-th elimination ideal I_l is the ideal defined by

$$I_l := I \cap \mathbb{K}[x_{l+1}, \cdots, x_n]. \tag{3.4}$$

That is I_l is an ideal which generated by $f_1 = \cdots = f_s = 0$ expressed in only $x_{l+1}, \cdots, x_n$.

Check

Since $0 \in I$ can be seen as a constant polynomial,

$$0 \in I_l. \tag{3.5}$$

$\forall f, g \in I_l \subset I$,

$$f + g \in I \tag{3.6}$$

and both f and g are functions only on $x_{l+1}, \cdots, x_n$, so $f+g \in \mathbb{K}[x_{l+1}, \cdots, x_n]$, i.e.,

$$f + g \in I_l. \tag{3.7}$$

Finally, $\forall f \in I_l \subset I, r \in \mathbb{K}[x_{l+1}, \cdots, x_n]$,

$$r * f \in I, \tag{3.8}$$

and $r * f \in \mathbb{K}[x_{l+1}, \cdots, x_n]$, that is

$$r * f \in I_l. \tag{3.9}$$

Therefore, I_l is an ideal of $\mathbb{K}[x_{l+1}, \cdots, x_n]$.
■

Note

More generally, the first elimination of $I_l \subset \mathbb{K}[x_{l+1}, \cdots, x_n]$ is I_{l+1}, since the first elimination of I_l is given by

$$I_l \cap \mathbb{K}[x_{l+2}, \cdots, x_n] \tag{3.10}$$

but

$$\begin{aligned} I_{l+1} &:= I \cap \mathbb{K}[x_{l+2}, \cdots, x_n] && (3.11)\\ &= (I \cap \mathbb{K}[x_{l+1}, \cdots, x_n]) \cap \mathbb{K}[x_{l+2}, \cdots, x_n] && (3.12)\\ &= I_l \cap \mathbb{K}[x_{l+2}, \cdots, x_n]. && (3.13) \end{aligned}$$

■

The Elimination Step

Thus a solution of the Elimination Step means giving a systematic procedure for finding elements of I_l. With the proper term ordering, Gröbner bases allow us to do this instantly.

3.1.2 The Elimination Theorem

Let $I \subset \mathbb{K}[x_1, \cdots, x_n]$ be an ideal and G be a Gröbner basis for I with $>_{lex}$, s.t.,

$$x_1 > x_2 > \cdots > x_n. \tag{3.14}$$

Then $0 \leq \forall l \leq n$, the set

$$G_l := G \cap \mathbb{K}[x_{l+1}, \cdots, x_n] \tag{3.15}$$

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

Proof

It suffices to show $\langle LT(G_l) \rangle \supset \langle LT(I_l) \rangle$ of eq.(2.147) "isGröbner".

Consider $\forall f \in I_l \subset I$. Since G is a Gröbner basis for I, there is some $g \in G$ whose leading term divides $LT(f)$:

$$LT(f) \sqsupseteq LT(g) \Leftrightarrow: LT(f) \in \langle LT(G) \rangle\,. \tag{3.16}$$

Now we have

$$f \in I_l := I \cap \mathbb{K}[x_{l+1}, \cdots, x_n] \Rightarrow f \in \mathbb{K}[x_{l+1}, \cdots, x_n] \tag{3.17}$$

and since we are using $>_{lex}$ with

$$x_1 > x_2 > \cdots > x_n, \tag{3.18}$$

any monomial involving $x_1, \cdots, x_l$ is greater than all monomials in $\mathbb{K}[x_{l+1}, \cdots, x_n]$, say f:

$$\forall h(x_1, \cdots, x_l) > f(x_{l+1}, \cdots, x_n). \tag{3.19}$$

Since $LT(f)$ is divisible by $LT(g)$ and from the above observation, we get

$$LT(g) \in \mathbb{K}[x_{l+1}, \cdots, x_n] \tag{3.20}$$

This implies that

$$g \in \mathbb{K}[x_{l+1}, \cdots, x_n], \tag{3.21}$$

and

$$g \in G \cap \mathbb{K}[x_{l+1}, \cdots, x_n] =: G_l. \tag{3.22}$$

Therefore this g is indeed in G_l and

$$g \in G_l, LT(f) \sqsupseteq LT(g) \Leftrightarrow LT(f) \in \langle LT(G_l) \rangle . \tag{3.23}$$

So $\forall f \in I_l$,

$$LT(f) \in \langle LT(I_l) \rangle \Rightarrow LT(f) \in \langle LT(G_l) \rangle . \tag{3.24}$$

■

3.1.3 ? The Extension Theorem

Let $I \subset \mathbb{C}[x_1, \cdots, x_n]$ be an ideal and I_1 be the 1st elimination ideal of I. $1 \leq \forall i \leq s$, write f_i in the form

$$f_i = g_i(x_2, \cdots, x_n) x_1^{N_i} + o(x_1^{N_i}), \tag{3.25}$$

where $N_i \geq 0$ and $g_i \in \mathbb{C}[x_2, \cdots, x_n]$ is nonzero, and $o(x_1^{N_i})$ stands for the terms in which x_1 has degree $< N_i$. Suppose that we have a partial solution $(a_2, \cdots, a_n) \in \mathbb{V}(I_1)$. If $(a_2, \cdots, a_n) \notin \mathbb{V}(g_1, \cdots, g_s)$, then there exists $a_1 \in \mathbb{C}$ s.t. $(a_1, \cdots, a_n) \in \mathbb{V}(I)$.

Note

The proof of this theorem uses resultant in §.

This extension theorem is especially easy to use when one of the leading coefficients is constant.

3.1.4 ? Corollary

Let $I = \langle f_1, \cdots, f_s \rangle \subset \mathbb{C}[x_1, \cdots, x_n]$, and assume that for some i, f_i is the form

$$f_i = cx_1^N + o(x_1^N), \tag{3.26}$$

where $c \in \mathbb{C}$ is nonzero and $N > 0$. If I_1 is the 1st elimination ideal of I and $(a_2, \cdots, a_n) \in \mathbb{V}(I_1)$, then there is $a_1 \in \mathbb{C}$ s.t. $(a_1, \cdots, a_n) \in \mathbb{V}(I)$.

Proof

This follows from the Extension Theorem; since this $g_i = c \neq 0$ implies

$$\mathbb{V}(g_1, \cdots, g_s) = \{a \,|g_1(a) = \cdots = g_s(a) = 0\} = \emptyset, \tag{3.27}$$

the if-statement

$$(a_2, \cdots, a_n) \notin \mathbb{V}(g_1, \cdots, g_s) \tag{3.28}$$

is True for all partial solutions.
■

3.2 The Geometry of Elimination

For simplicity, we will work over $\mathbb{C}$.

3.2.1 Projections of an affine variety

Suppose we have

$$V := \mathbb{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n. \tag{3.29}$$

To eliminate the first l variables, consider the projection map

$$\pi_l : \mathbb{C}^n \to \mathbb{C}^{n-l}; (a_1, \cdots, a_n) \mapsto (a_{l+1}, \cdots, a_n). \tag{3.30}$$

The image of $V \subset \mathbb{C}^n$ is in

$$\pi_l(V) \subset \mathbb{C}^{n-l}. \tag{3.31}$$

3.2.2 Lemma

Let

$$I_l := \langle f_1, \cdots, f_s \rangle \cap \mathbb{C}[x_{l+1}, \cdots, x_n] \tag{3.32}$$

be the l-th elimination ideal. Then

$$\pi_l(V) \subset \mathbb{V}(I_l)(\subset \mathbb{C}^{n-l}) \tag{3.33}$$

Proof

Let $\forall f \in I_l \subset \langle f_1, \cdots, f_s \rangle$ vanishes at $\forall (a_1, \cdots, a_n) \in V := \mathbb{V}(f_1, \cdots, f_s)$,

$$f(a_1, \cdots, a_n) = 0. \tag{3.34}$$

However, since $f \in I_l := I \cap \mathbb{K}[x_{l+1}, \cdots, x_n]$, f depends only on $x_{l+1}, \cdots, x_n$,

$$f(a_{l+1}, \cdots, a_n) = f \circ \pi_l(a_1, \cdots, a_n) = 0. \tag{3.35}$$

That is, f vanishes at all points in $\pi_l(V)$.
■

3.2.3 ? Geometric Extension Theorem

Geometrical interpretation of the Extension Theorem; given $V := \mathbb{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n$, let $g_i \in \mathbb{C}[x_2, \cdots, x_n]$ be as in the Extension Theorem. If I_1 is the 1st elimination ideal of $\langle f_1, \cdots, f_s \rangle$, then we have

$$\mathbb{V}(I_1) = \pi_1(V) \cup (\mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1)) \, (\subset \mathbb{C}^{n-1}), \tag{3.36}$$

where $\pi_1 : \mathbb{C}^n \to \mathbb{C}^{n-1}$ is the projection onto the last $n-1$ components.

Proof

Since we have shown that $\pi_1(V) \subset \mathbb{V}(I_1)$,

$$\mathbb{V}(I_1) \supset \pi_1(V) \cup (\mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1)) \tag{3.37}$$

Conversely, consider an arbitrary partial solution in $\mathbb{V}(I_1)$

$$(a_2, \cdots, a_n) \in \mathbb{V}(I_1). \tag{3.38}$$

From Fig.3.1, this partial solution is either in

$$(a_2, \cdots, a_n) \in \mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1) \tag{3.39}$$

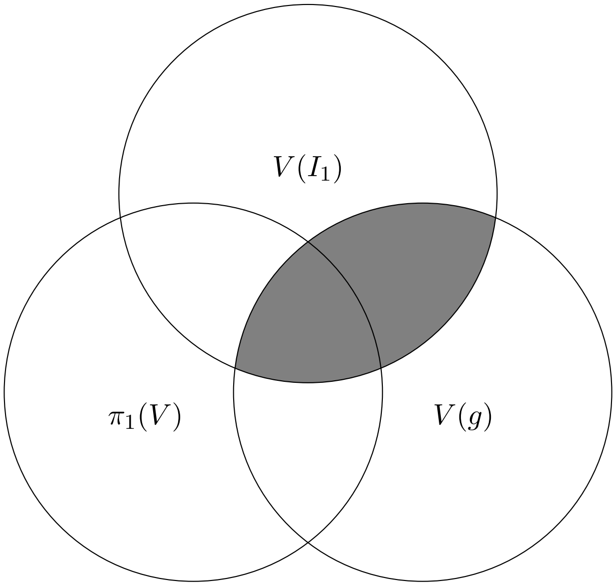

Figure 3.1: Three sets of $V(I_1), V(g)$, and $\pi_1(V)$

or in

$$(a_2, \cdots, a_n) \notin \mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1). \tag{3.40}$$

If $(a_2, \cdots, a_n) \in \mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1)$, then clearly

$$(a_2, \cdots, a_n) \in \pi_1(V) \cup (\mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1)). \tag{3.41}$$

Else $(a_2, \cdots, a_n) \notin \mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1)$, then we also have

$$(a_2, \cdots, a_n) \notin \mathbb{V}(g_1, \cdots, g_s) \tag{3.42}$$

and we can apply the Extension Theorem:

$$\exists a_1 \in \mathbb{C} \text{ s.t. } (a_1, a_2, \cdots, a_n) \in \mathbb{V}(I), \tag{3.43}$$

and

$$(a_2, \cdots, a_n) = \pi_1(a_1, a_2, \cdots, a_n) \in \pi_1(V). \tag{3.44}$$

Therefore, in either case

$$a \in V(I_1) \Rightarrow a \in \pi_1(V) \cup (\mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1)) \tag{3.45}$$

that is

$$\mathbb{V}(I_1) \subset \pi_1(V) \cup (\mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1)) \tag{3.46}$$

■

3.2.4 ? The Closure Theorem, a special case

Let $V := \mathbb{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n$ and let I_1 be the 1st elimination ideal of $\langle f_1, \cdots, f_s \rangle$. Then When $V \neq \emptyset$, there exists an affine variety $W \subsetneq \mathbb{V}(I_1)$ s.t., $\mathbb{V}(I_1) - W \subset \pi_1(V)$.[1]

Proof

Let

$$W' := \mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1) \tag{3.47}$$

and note that W is an affine variety by §1.2.2. The decomposition in §3.2.3

$$\begin{aligned} \mathbb{V}(I_1) &= \pi_1(V) \cup (\mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1)) && (3.48) \\ &= \pi_1(V) \cup W' && (3.49) \end{aligned}$$

implies

$$\mathbb{V}(I_1) - W' \subset \pi_1(V), \tag{3.50}$$

and if $W' \neq \mathbb{V}(I_1)$, then we are done.

If $W' = \mathbb{V}(I_1)$, we need to change the equations defining V s.t. W becomes smaller.

$W' = \mathbb{V}(I_1) \Rightarrow V = \mathbb{V}(f_1, \cdots, f_s, g_1, \cdots, g_s) \quad \because$ Since

$$f_1(a) = \cdots = f_s(a) = g_1(a) = \cdots = g_s = 0 \Rightarrow f_1(a) = \cdots = f_s(a) = 0 \tag{3.51}$$

one direction follows

$$\mathbb{V}(f_1, \cdots, f_s, g_1, \cdots, g_s) \subset V := \mathbb{V}(f_1, \cdots, f_s) \tag{3.52}$$

[1] This is an instance of the following general statement; let $V := \mathbb{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n$ and let I_l be the lth elimination ideal of $\langle f_1, \cdots, f_s \rangle$. Then

1. $\mathbb{V}(I_l)$ is the smallest affine variety containing $\pi_l(V) \subset \mathbb{C}^{n-l}$.
2. When $V \neq \emptyset$, there exists an affine variety $W \subsetneq \mathbb{V}(I_l)$ s.t. $\mathbb{V}(I_l) - W \subset \pi_l(V)$.

by definition in §1.2.1.

For the opposite direction, let

$$(a_1, a_2, \cdots, a_n) \in V := \mathbb{V}(f_1, \cdots, f_s). \tag{3.53}$$

Then from §3.2.2,

$$(a_2, \cdots, a_n) \in \pi_1(V) \subset \mathbb{V}(I_1) = W' := \mathbb{V}(g_1, \cdots, g_s) \cap \mathbb{V}(I_1) \tag{3.54}$$

and $\forall j$,

$$g_j(a_2, \cdots, a_n) = 0. \tag{3.55}$$

Thus

$$(a_1, a_2, \cdots, a_n) \in \mathbb{V}(f_1, \cdots, f_s, g_1, \cdots, g_s) \tag{3.56}$$

and

$$\mathbb{V}(f_1, \cdots, f_s, g_1, \cdots, g_s) \supset V := \mathbb{V}(f_1, \cdots, f_s). \tag{3.57}$$

Therefore

$$\mathbb{V}(f_1, \cdots, f_s, g_1, \cdots, g_s) = V := \mathbb{V}(f_1, \cdots, f_s). \tag{3.58}$$

■

Let

$$I := \langle f_1, \cdots, f_s \rangle \tag{3.59}$$

be our original ideal and

$$\tilde{I} := \langle f_1, \cdots, f_s, g_1, \cdots, g_s \rangle . \tag{3.60}$$

Then in general $I \subset \tilde{I}$, but we already have

$$\mathbb{V}(I) = \mathbb{V}(\tilde{I}). \tag{3.61}$$

? $\mathbb{V}(I_1) = \mathbb{V}(\tilde{I_1})$

Chapter 4

The Algebra-Geometry Dictionary

4.1 Hilbert's Nullstellensatz

Null(=Zero), Stellen(=Places), Satz(=Theorem).

4.1.1 ? The Weak Nullstellensatz

Let $\mathbb{K}$ be an algebraically closed filed and let $I \subset \mathbb{K}[x_1, \cdots, x_n]$ be an ideal. Then

$$\mathbb{V}(I) = \emptyset \Rightarrow I = \mathbb{K}[x_1, \cdots, x_n]. \tag{4.1}$$

Proof

The standard strategy is to show

$$1 \in I. \tag{4.2}$$

It is because, if $1 \in I$ then $\forall f \in \mathbb{K}[x_1, \cdots, x_n]$,

$$f = f * 1 \in I \Leftrightarrow \mathbb{K}[x_1, \cdots, x_n] \subset I. \tag{4.3}$$

We prove by induction.

$n = 1$ **case** From §1.5.5, every ideal I of $\mathbb{K}[x]$ is generated by a single polynomial f:

$$I = \langle f \rangle \tag{4.4}$$

Then the variety is the set of roots

$$\{a \in \mathbb{K} | \, f(a) = 0\} . \tag{4.5}$$

Since $\mathbb{K}$ is algebraically closed, i.e., $\forall f \in \mathbb{K}[x]$,

$$f \text{ is not a const. poly.} \Rightarrow \exists a \in \mathbb{K} \text{ s.t. } f(a) = 0, \tag{4.6}$$

if $\forall a \in \mathbb{K}, f(a) \neq 0$ then f is a non zero constant polynomial.

$$\mathbb{V}(\langle f \rangle) \Rightarrow f = c(\neq 0) \in \mathbb{K}. \tag{4.7}$$

Since $c \neq 0$,

$$\exists c^{-1} \in \mathbb{K}. \tag{4.8}$$

Therefore,

$$c^{-1} * f = c^{-1} * c = 1 \in I \tag{4.9}$$

and

$$\forall I \subset \mathbb{K}[x], \mathbb{V}(I) = \emptyset \Rightarrow I = \mathbb{K}[x]. \tag{4.10}$$

$(n-1)$ **case** $\Rightarrow n$ **case** Assume $(n-1)$ case

$$\forall J \subset \mathbb{K}[x_2, \cdots, x_n], \mathbb{V}(J) = \emptyset \Rightarrow J = \mathbb{K}[x_2, \cdots, x_n] \tag{4.11}$$

and consider an arbitrary ideal

$$I := \langle f_1, \cdots, f_s \rangle \subset \mathbb{K}[x_1, \cdots, x_n] \tag{4.12}$$

for which $\mathbb{V}(I) = \emptyset$. Since can assume f_1 is not a constant,[1] suppose f_1 has total degree $N \geq 1$.

Consider the following linear transformation:

$$\begin{aligned} x_1 &= y_1, \\ x_2 &= y_2 + a_2 * y_1, \\ &\vdots \\ x_n &= y_n + a_n * y_1, \end{aligned} \tag{4.13}$$

where $a_2, \cdots, a_n$ are constants in $\mathbb{K}$. Then f_1 bocomes

$$\begin{aligned} f_1(x_1, \cdots, x_n) &= f_1(y_1, y_2 + a_2 * y_1, \cdots, y_n + a_n * y_1) & (4.14) \\ &= c(a_2, \cdots, a_n) * y_1^N + O(y_1^{N-1}) & (4.15) \end{aligned}$$

[1] If f_1 is a non zero constant polynomial, then using the same argument in $n = 1$ case, we can show $1 \in I$.

? Lemma ($c(a_2, \cdots, a_n)$ is not constantly 0) Consider a polynomial $f \in \mathbb{K}[x_1, \cdots, x_n]$ under the linear transform in eq.(4.13). When we write f as a sum

$$f = h_N + \cdots + h_1 + h_0 \tag{4.16}$$

of homogeneous polynomials

$$h_m(x_1, \cdots, x_n) = \sum_{|\alpha|=m} c_\alpha x^\alpha, c_\alpha \in \mathbb{K}. \tag{4.17}$$

Note that, under the linear transform in eq.(4.13), the degree of above h_m is unchanged.

Define

$$\begin{aligned} \tilde{f}(y_1, \cdots, y_n) &:= f(y_1, y_2 + a_2 y_1, \cdots, y_n + a_n y_1) & (4.18) \\ &= c(a_2, \cdots, a_n) * y_1^N + O(y_1^{N-1}) & (4.19) \end{aligned}$$

If we put $y_2 = \cdots = y_n = 0$,

$$\begin{aligned} \tilde{f}(y_1, y_2 = \cdots = y_n = 0) &= f(y_1, a_2 y_1, \cdots, a_n y_1) & (4.20) \\ &= h_N(y_1, a_2 y_1, \cdots, a_n y_1) + O(y_1^{N-1}) & (4.21) \\ &= h_N(1, a_2, \cdots, a_n) * y_1^N + O(y_1^{N-1}), & (4.22) \end{aligned}$$

since h_N has homogeneous degree N.

Chapter 5

Polynomial and Rational Functions on a Variety

5.1 Polynomial Mappings

5.1.1 Definition of polynomial mappings

Let $V \subset \mathbb{K}^m, W \subset \mathbb{K}^n$ be varieties. A function

$$\phi : V \to W \tag{5.1}$$

is a polynomial mapping (or regular mapping) iff there exist polynomials

$$f_1, \cdots, f_n \in \mathbb{K}[x_1, \cdots, x_m] \tag{5.2}$$

s.t., $\forall (a_1, \cdots, a_m) \in V$,

$$\phi(a_1, \cdots, a_m) = (f_1(a_1, \cdots, a_m), \cdots, f_n(a_1, \cdots, a_m)) \,. \tag{5.3}$$

We call this n-tuple of polynomials

$$(f_1, \cdots, f_n) \in (\mathbb{K}[x_1, \cdots, x_m])^n \tag{5.4}$$

represents ϕ.

5.1.2 Proposition

Let $V \subset \mathbb{K}^m$ be an affine variety. Then

1. $f, g \in \mathbb{K}[x_1, \cdots, x_m]$ represent the same polynomial function of V iff $f - g \in \mathbb{I}(V)$.

2. $(f_1, \cdots, f_n)$ and $(g_1, \cdots, g_n)$ represent the same polynomial mapping from V to $\mathbb{K}^n$ iff $f_i - g_i \in \mathbb{I}(V)$ for each $1 \leq i \leq n$.

Proof

It suffices to show the 1st case.

If f and g represent the same function, then $\forall a \in V$,

$$f(a) = g(a) \Leftrightarrow (f-g)(a) = 0. \tag{5.5}$$

Thus

$$f - g \in \mathbb{I}(V) \tag{5.6}$$

Conversely, if

$$f - g \in \mathbb{I}(V), \tag{5.7}$$

then $\forall a = (a_1, \cdots, a_m) \in V$,

$$(f-g)(a) = f(a) - g(a) = 0. \tag{5.8}$$

Hence, f and g represent the same function on V.
■

5.1.3 Definition of $\mathbb{K}[V]$

Let us define

$$\mathbb{K}[V] := \{\phi : V \to \mathbb{K} \,|\, \phi \text{ is a polynomial function}\} \tag{5.9}$$

the set of polynomial functions.[1]

$\mathbb{K}[V]$ is a commutative ring

$\forall \phi, \psi \in \mathbb{K}[V]$, the addition

$$(\phi + \psi)(p) := \phi(p) + \psi(p), \quad \forall p \in V, \tag{5.11}$$

and the multiplication

$$(\phi * \psi)(p) := \phi(p) * \psi(p), \quad \forall p \in V. \tag{5.12}$$

[1] I prefer the exponential notion

$$\mathbb{K}^V := \mathbb{K}[V]. \tag{5.10}$$

Identities are constant functions, e.g.,

$$0 : V \to \mathbb{K}; p \to 0. \tag{5.13}$$

Associativity and distributive laws come from that of $\mathbb{K}$, e.g., $\forall p \in V$,

$$\begin{aligned}(\phi + (\psi + \chi))(p) &= \phi(p) + (\psi + \chi)(p) &(5.14)\\ &= \phi(p) + \psi(p) + \chi(p) &(5.15)\\ &= (\phi(p) + \psi(p)) + \chi(p) &(5.16)\\ &= ((\phi + \psi) + \chi)(p). &(5.17)\end{aligned}$$

5.1.4 ? Proposition

Let $V \subset \mathbb{K}^n$ be an affine variety. The following statements are equivalent.

1. V is irreducible.
2. $\mathbb{I}(V)$ is a prime ideal.
3. $\mathbb{K}[V]$ is an integral domain.

5.2 Quotients of polynomial Rings

5.2.1 Congruent modulo I

Let $I \subset \mathbb{K}[x_1, \cdots, x_m]$ be an ideal, and let $f, g \in \mathbb{K}[x_1, \cdots, x_m]$. We say f and g are congruent modulo I,

$$f \equiv g \mod I :\Leftrightarrow f - g \in I. \tag{5.18}$$

This congruence modulo I is an equivalence relation on $\mathbb{K}[x_1, \cdots, x_n]$.

1. (reflexive) $\forall f \in I$,
$$f - f = 0 \in I. \tag{5.19}$$
2. (symmetry) $\forall f, g \in I$,
$$f - g \in I \Rightarrow g - f = -(f - g) \in I. \tag{5.20}$$
3. (transitivity) $\forall f, g, h \in I$,
$$f - g \in I, g - h \in I \Rightarrow f - h = (f - g) + (g - h) \in I. \tag{5.21}$$

We denote the equivalence class which is represented by $f \in I$,

$$[f] := \{g \in \mathbb{K}[x_1, \cdots, x_m] | \, g \equiv f \mod I\} \tag{5.22}$$

5.2.2 ? Proposition

The distinct polynomial functions in $\mathbb{K}[V]$ are in one-to-one correspondence with the equivalence classes of polynomials under congruence modulo $\mathbb{I}(V)$.

Proof

Consider an arbitrary polynomial functions $\phi : V \to \mathbb{K}$, and its representation

$$f \in (\mathbb{K}[x_1, \cdots, x_m]) \tag{5.23}$$

s.t., $\forall (a_1, \cdots, a_m) \in V$,

$$\phi(a_1, \cdots, a_m) = f(a_1, \cdots, a_m). \tag{5.24}$$

We claim that

$$[f] \overset{\Phi}{\mapsto} \phi \tag{5.25}$$

is the one-to-one correspondence.

Since every polynomial functions have its representation (see §5.1.1), this correspondence is surjective:

$$\forall \phi : V \to \mathbb{K}, \exists f \in (\mathbb{K}[x_1, \cdots, x_m]) \text{ is a rep.} \Rightarrow \exists [f]. \tag{5.26}$$

Next, if we suppose

$$\Phi([f]) = \Phi([g]) : V \to \mathbb{K}, \tag{5.27}$$

then both f and g is a representation of this map. Therefore, $\forall p \in V$,

$$f(p) = g(p) \Rightarrow (f - g)(p) = 0 \tag{5.28}$$

i.e., the difference is in $\mathbb{I}(V)$:

$$f - g \in \mathbb{I}(V) \Leftrightarrow [f] = [g]. \tag{5.29}$$

So this correspondence is injective.

■

5.2.3 Quotients

The quotient of $\mathbb{K}[x_1, \cdots, x_m]$ modulo I,

$$\mathbb{K}[x_1, \cdots, x_m]/I, \tag{5.30}$$

is the set of equivalence classes of congruence modulo I:

$$\mathbb{K}[x_1, \cdots, x_m]/I := \{[f] \,|\, f \in \mathbb{K}[x_1, \cdots, x_m]\} \tag{5.31}$$

$\mathbb{K}[x_1, \cdots, x_m]/I$ is a commutative ring. The addition

$$[f] + [g] := [f + g] \tag{5.32}$$

is well defined, since $\forall f' \in [f], g' \in [g]$, there exists some elements in I and

$$f' = f + i, g' = g + j, i, j \in I. \tag{5.33}$$

So

$$f' + g' \quad = \quad f + g + (i + j) \tag{5.34}$$

and $(i + j) \in I$. This means

$$f' + g' \in [f + g]. \tag{5.35}$$

Similarly, the multiplication

$$[f] * [g] := [f * g] \tag{5.36}$$

is also well defined:

$$(f' + i) * (g' + j) = f' * g' + f' * j + i * g' + i * j, \tag{5.37}$$

and $f' * j + i * g' + i * j \in I$, and

$$f' * g' \in [f * g]. \tag{5.38}$$

Identities

$$[0], [1] \tag{5.39}$$

are also well defined, and associativity and the distributive laws are from that of $\mathbb{K}[x_1, \cdots, x_n]$.

■

5.2.4 Theorem

The one-to-one correspondence between two commutative rings

$$\Phi : \mathbb{K}[x_1, \cdots, x_n]/\mathbb{I}(V) \overset{\cong}{\to} \mathbb{K}[V] \tag{5.40}$$

given in §5.2.2, preserves sums and products. That is, Φ is a ring homomorphism. One-to-one homomorphisms are called isomorphisms.

Proof

Let $[f], [g] \in \mathbb{K}[x_1, \cdots, x_n]/\mathbb{I}(V)$, then

$$\Phi([f]) = \exists! \phi \in \mathbb{K}[V], \Phi([g]) = \exists! \psi \in \mathbb{K}[V] \tag{5.41}$$

hold. Therefore

$$\Phi([f+g]) := \phi + \psi = \Phi([f]) + \Phi([g]) \tag{5.42}$$

is well defined.

Similarly, we can prove the multiplication law, and that of inverse Φ^{-1}.
■

5.2.5 Definition of ring isomorphisms

Let R, S be commutative rings.

1. A mapping $\phi : R \to S$ is a ring homomorphism iff ϕ preserves sums and products:

$$\phi(r + r') = \phi(r) + \phi(r'), \quad \phi(r * r') = \phi(r) * \phi(r'). \tag{5.43}$$

   In addition,

$$1_R \overset{\phi}{\mapsto} 1_S. \tag{5.44}$$

2. A mapping $\phi : R \to S$ is a ring isomorphism iff

   (a) $\phi : R \to S$ is a ring homomorphism.

   (b) $\phi : R \to S$ is bijective.

3. Two rings R, S are isomorphic iff there exists an isomorphism,

$$R \overset{\phi}{\cong} S. \tag{5.45}$$

5.2.6 Definition of ideal

A subset I of a commutative ring R is an ideal in R iff

1. $0_R \in I$

2. $\forall a, b \in I \Rightarrow a + b \in I$

3. $\forall a \in I, r \in R \Rightarrow r * a \in I$

5.2.7 Proposition

Let I be an ideal in $\mathbb{K}[x_1, \cdots, x_n]$. The ideals in the quotient ring $\mathbb{K}[x_1, \cdots, x_n]/I$ are in one-to-one correspondence with the ideals of $\mathbb{K}[x_1, \cdots, x_n]$ containing I, i.e. the ideal J s.t. $I \subset J \subset \mathbb{K}[x_1, \cdots, x_n]$.

Proof

Consider $I \subset \forall J \subset \mathbb{K}[x_1, \cdots, x_n]$. We claim that

$$J \mapsto J/I := \{\, [j] \in \mathbb{K}[x_1, \cdots, x_n]/I |\, j \in J\} \tag{5.46}$$

is the one-to-one correspondence.

We prove J/I is an ideal; since $0 \in J$,

$$[0] \in J/I \tag{5.47}$$

$\forall [j], [k] \in J/I$, the addition is guaranteed by that of $\mathbb{K}[x_1, \cdots, x_n]/I$:

$$[j] + [k] := [j + k] \in J/I, \tag{5.48}$$

since $\forall j, k \in J, j + k \in J$. Similarly,

$$[j] * [k] := [j * k] \in J/I. \tag{5.49}$$

Finally, if $[j] \in J/I, [r] \in \mathbb{K}[x_1, \cdots, x_n]/I$, then

$$[r] * [j] := [r * j], \tag{5.50}$$

but $\forall j \in J, r \in \mathbb{K}[x_1, \cdots, x_n], r * j \in J$ and

$$[r] * [j] := [r * j] \in J/I. \tag{5.51}$$

Thus, J/I is an ideal.

So $J \mapsto J/I$ is surjective, and clearly injective:

$$J = K \Rightarrow J/I = K/I. \tag{5.52}$$

Therefore

$$J \mapsto J/I \tag{5.53}$$

is one-to-one.

Let us consider the inverse, for arbitrary $\tilde{J} \in \mathbb{K}[x_1, \cdots, x_n]/I$, define

$$J := \left\{ j \in \mathbb{K}[x_1, \cdots, x_n] |\, [j] \in \tilde{J} \right\}. \tag{5.54}$$

$\forall i \in I$,

$$[i] = [0] \in \tilde{J} \text{ i.e. } i \in J \tag{5.55}$$

so this J contain I:

$$I \subset J. \tag{5.56}$$

Since I is an ideal,

$$0 \in I \subset J. \tag{5.57}$$

$\forall j, k \in J$,

$$[j], [k] \in \tilde{J} \tag{5.58}$$

by definition, and

$$[j + k] := [j] + [k] \in \tilde{J}, \tag{5.59}$$

so

$$j + k \in J. \tag{5.60}$$

Finally, $\forall j \in J, r \in \mathbb{K}[x_1, \cdots, x_n]$,

$$[j] \in \tilde{J} \tag{5.61}$$

and by definition in §5.2.3,

$$[r] \in \mathbb{K}[x_1, \cdots, x_n]/I. \tag{5.62}$$

Therefore,

$$[r * j] := [r] * [j] \in \tilde{J} \Leftrightarrow r * j \in J. \tag{5.63}$$

Thus, J is an ideal, and this mapping $J \leftarrow\!\shortmid J$ is the inverse.[2]

Schematically,

$$\begin{aligned} \{J | I \subset J \subset \mathbb{K}[x_1, \cdots, x_n]\} & \qquad \{\tilde{J} \subset \mathbb{K}[x_1, \cdots, x_n]/I\} & (5.64) \\ J & \mapsto \quad J/I := \{\, [j] \in \mathbb{K}[x_1, \cdots, x_n]/I | \, j \in J\} & (5.65) \\ J := \left\{ j \in \mathbb{K}[x_1, \cdots, x_n] | \, [j] \in \tilde{J} \right\} & \leftarrow\!\shortmid \quad \tilde{J} & (5.66) \end{aligned}$$

■

5.2.8 Corollary

Every ideal in the quotient ring $\mathbb{K}[x_1, \cdots, x_n]/I$ is finitely generated.

Proof

From above, every ideal in $\mathbb{K}[x_1, \cdots, x_n]/I$ can be uniquely written as

$$J/I \tag{5.67}$$

of some $I \subset J \subset \mathbb{K}[x_1, \cdots, x_n]$.

The Hilbert Basis Theorem in §2.5.4 implies this J is finitely generated:

$$J = \langle f_1, \cdots, f_s \rangle , \tag{5.68}$$

and $\forall j \in J$,

$$\exists h_i \in \mathbb{K}[x_1, \cdots, x_n], j = \sum_i h_i * f_i. \tag{5.69}$$

Therefore, $\forall [j] \in J/I$,

$$\begin{aligned} [j] &= \left[\sum_i h_i * f_i \right] & (5.70) \\ &= \sum_i [h_i] * [f_i] & (5.71) \end{aligned}$$

that is

$$J/I = \langle [f_1], \cdots, [f_s] \rangle . \tag{5.72}$$

So, the classes $[f_1], \cdots, [f_s]$ generate J/I.

■

[2] Since we have shown $J \mapsto J/I$ is bijective, if exists, the inverse is uniquely determined.