Introduction to Gröbner Basis Special

Riley @Na2COOH_2

September 21, 2025

Abstract

This document is an introduction to Gröbner basis for beginners. The Gröbner basis used in the computer science mainly, but this document is for people in the commutative algebra. To read this document, you need to know the basic concepts of undergraduate mathematics.
This document has MIT License. You can use, copy, modify, and redistribute it freely. However, please do not use or distribute this document without MIT License.

Figure 1: Bruno Buchberger

Table of Contents

1 Introduction

The Gröbner basis is said to be introduced by Bruno Buchberger, a computer scientist, in 1965, and named them after his advisor Wolfgang Gröbner. As its name, it is like a basis of an ideal of a polynomial ring. We will show that we can compute the generators of a given ideal by using the Gröbner basis. By using this computation, mathematicians often use the Gröbner basis to compute the generators of an ideal by using a computer. However, the Gröbner basis is not only useful for such a computational tool. It is also useful for theoretical aspects. For example, we will show that many of concepts in polynomial rings is invariant under taking an *initial*.

This document is based on the 20th summer school of commutative ring theory in Osaka university in 2025. In this summer school, we read [BCRV22] mainly. You can access the site of the summer school.

And [HH11] is our friendly book about the Gröbner basis.

 © Riley

2 Monomial Orders

In this section, let K be a field and $R = K[x_1, \ldots, x_n]$ be the polynomial ring in n variables over K.

Def 2.1: (Monomial and Monomial Order)

A *monomial* in R is a product of powers of variables, i.e., a polynomial of the form

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

where a_i are non negative integers.
We call a *term* a form of $a\mu$ where $a \in K \setminus \{0\}$ and μ is a monomial. We denote the set of all monomials in R by $\mathrm{Mon}(R)$.

$$\mathrm{Mon}(R) = \{\mu | \mu \text{ is a monomial in } R\}$$

A *monomial order* on R is a total order $\leq$ on $\mathrm{Mon}(R)$ such that

1. $\forall \mu, \nu, \xi \in \mathrm{Mon}(R), \quad \mu \leq \nu \implies \mu\xi \leq \nu\xi$
2. $\forall \mu \in \mathrm{Mon}(R), \quad 1 \leq \mu$

□

Def 2.2: (Support)

For a non zero polynomial $f \in R$, we define the *support* of f by

$$\mathrm{Supp}(f) = \{\mu \in \mathrm{Mon}(R) | \text{the coefficient of } \mu \text{ in } f \text{ is not } 0\}$$

□

Of course, $\mathrm{Supp}(f)$ is a finite set. And we can express f uniquely as

$$f = \sum_{\mu \in \mathrm{Supp}(f)} a_\mu \mu$$

where $a_\mu \in K \setminus \{0\}$ is the coefficient of μ in f.

Ex 2.3: (Examples of Monomial Orders)

For monomials $\mu = x_1^{a_1} \cdots x_n^{a_n}$ and $\nu = x_1^{b_1} \cdots x_n^{b_n}$, we define the following monomial orders.

1. *lexicographic order* (lex):
   $\mu \leq_{\mathrm{lex}} \nu$ if and only if there is k which satisfies $a_i = b_i$ for $i < k$ and $a_k < b_k$.
2. *degree lexicographic order* (deglex):
   $\mu \leq_{\mathrm{deglex}} \nu$ if and only if $\deg \mu = \sum a_i < \sum b_i = \deg \nu$ or $\sum a_i = \sum b_i$ and $\mu \leq_{\mathrm{lex}} \nu$.
3. (degree) reverse lexicographic order (degrevlex):
   $\mu \leq_{\mathrm{degrevlex}} \nu$ if and only if $\deg \mu = \sum a_i < \sum b_i = \deg \nu$ or $\sum a_i = \sum b_i$ and there is k which satisfies $a_i = b_i$ for $i > k$ and $a_k > b_k$.

□

We can easily check these relations are indeed monomial orders. We often use a lex order.
The order of monomials can change if we choose a different monomial order as follows.

Ex 2.4

Let $R = K[x, y, z]$ and consider the lex order with $x > y > z$. Then, we have

$$x^2 > xz > y^2$$

in lex order. However, in degrevlex order, we have

$$x^2 > y^2 > xz$$

□

The readers may know Hilbert's basis theorem. By using this theorem, we can show the following important proposition, Prop 2.6. This proposition gurantees the halting of algorithms. Before showing Prop 2.6, we prepare the following proposition.

Prop 2.5

Let A be a commutative noetherian ring with 1, I be an ideal of A and E be a generator system of I. Then, there exists a finite subset F of E such that F is also a generator system of I. □

pf.) Since A is noetherian, there exists a maximal element of the following set.

$$\{(J) | J \subset E \text{ is a finite subset. } \}$$

where (J) is the ideal generated by J. Let F be a maximal element of this set. We will show that $I = (F)$. If not, there exists $f \in I \setminus (F)$. Then, $(F \cup \{f\})$ is strictly larger than (F), which contradicts the maximality of (F). Thus, we have $I = (F)$. ■

Prop 2.6: (Monomial Order is well-order)

The monomial order on R is a well-order, i.e., every non empty subset of $\mathrm{Mon}(R)$ has the minimum element. In particular, there is no infinite descending chain

$$\mu_1 > \mu_2 > \mu_3 > \cdots$$

□

pf.) We take $\emptyset \neq N \subset \mathrm{Mon}(R)$ and it is enough to show N has the minimum element. Let I be the ideal generated by N. And R is noetherian by Hilbert's basis theorem, and by Prop 2.5, we can write $I = (f_1, \cdots, f_r) \quad (f_i \in N)$. Assume f_1 is the minimum element of $\{f_1, \ldots, f_r\}$. We will show that f_1 is the minimum element of N. $\forall \mu \in N$, $\mu = s_1 f_1 + \cdots + s_r f_r$ using $s_i \in R$. Since $\mu, f_1, \cdots, f_r$ are monomials, we have $\mu = s f_i$ for some i and $s \in R$. (Think about the computation of the right hand side.) Then, $\mu = s f_i \geq f_i \geq f_1$. Thus, f_1 is the minimum element of N. ■

As the last of this section, we define the following important concepts.

Def 2.7: (Initial and Initial ideal)

For a non zero polynomial $f \in R$, we define the *initial* of f by

$$\mathrm{in}_{\leq}(f) = \max_{\leq} \mathrm{Supp}(f)$$

Note that $\mathrm{in}_{\leq}(f)$ is a monomial with coefficient 1. And we define the *initial term* of f is the largest term of f under the monomial order. We write this $\mathrm{init}_{\leq}(f)$. And let $\mathrm{inic}(f)$ be the coefficient of this. We often

omit the subscript $\leq$ if there is no confusion.
We can easily check that $\mathrm{in}(fg) = \mathrm{in}(f)\mathrm{in}(g)$, $\mathrm{in}(f+g) \leq \max(\mathrm{in}(f), \mathrm{in}(g))$ for $f, g \in R \setminus \{0\}$.
For an ideal I of R, we define the *initial ideal* of I by

$$\mathrm{in}_{\leq}(I) = (\mathrm{in}_{\leq}(f) | f \in I \setminus \{0\})$$

We often omit the subscript $\leq$ if there is no confusion, $\mathrm{in}(I)$. □

In the later sections, we will see that many of concepts in polynomial rings is invariant under taking an initial. And we show the following proposition. This proposition may be used to extend the results for ideals to vector spaces. When we consider an ideal I as K-vector space, we may define $\mathrm{in}(I)$ as a K- vector space generated by $\{\mathrm{in}(f) | f \in I \setminus \{0\}\}$ not as an ideal. However, these two ways of taking initials, as a K-vector space and as an ideal, actually coincide.

Prop 2.8

For an ideal I of R, the initial ideal $\mathrm{in}(I)$ is equal to the K-vector space generated by $\{\mathrm{in}(f) | f \in I \setminus \{0\}\}$.
□

pf.) Let V be the K-vector space generated by $\{\mathrm{in}(f) | f \in I \setminus \{0\}\}$. It is enough to show $V \subset \mathrm{in}(I)$. Take $f = g_1\mu_1 + \cdots + g_r\mu_r \in \mathrm{in}(I)$. Here, $g_i \in R$. Assume $\mu_i = \mathrm{in}(f_i) \quad (f_i \in I)$ and

$$g_i = a_{i1}\mu_{i1} + \cdots + a_{ir_i}\mu_{ir_i} \quad (a_{ij} \in K \setminus \{0\}, \mu_{ij} \in \mathrm{Mon}(R))$$

Then, we have

$$\begin{aligned} f &= \sum_{i=1}^{r} g_i\mu_i \\ &= \sum_{i=1}^{r} \left(\sum_{j=1}^{r_i} a_{ij}\mu_{ij} \right) \mu_i \\ &= \sum_{i=1}^{r} \sum_{j=1}^{r_i} a_{ij}\mu_{ij}\mathrm{in}(f_i) \\ &= \sum_{i=1}^{r} \sum_{j=1}^{r_i} a_{ij}\mathrm{in}(\mu_{ij}f_i) \in V \end{aligned}$$

And we can see that $\mu_{ij}f_i \in I$. Thus, we have $f \in V$. ■

3 The Gröbner Basis

In this section, let K be a field and $R = K[x_1, \dots, x_n]$ be the polynomial ring in n variables over K. And we fix a monomial order $\leq$ on R.
Let us now define the Gröbner basis.

Def 3.1: (Gröbner Basis)

For an ideal I of R, a finite subset $\{f_1, \dots, f_r\}$ of $I \setminus \{0\}$ is called a *Gröbner basis* of I if

$$\mathrm{in}(I) = (\mathrm{in}(f_1), \dots, \mathrm{in}(f_r))$$

holds. □

Note that we call such a set basis though it may not be a linearly independent set. When this set is a generator system of $\mathrm{in}(I)$, we call it a *Gröbner basis* of I.
Of course, in general,

$$\mathrm{in}(I) \supset (\mathrm{in}(f_1), \dots, \mathrm{in}(f_r))$$

holds. Thus, to check whether a given finite subset of I is a Gröbner basis or not, we have to check the opposite inclusion. However, it is not easy to check this inclusion directly. When does the given finite subset become a Gröbner basis? How to find the Gröbner basis? We will answer these questions in the next section.
As the first step, we show some theoretic properties of the Gröbner basis. The first one is the existence of the Gröbner basis.

Prop 3.2: (Existence of the Gröbner Basis)

For any ideal I of R, there exists a Gröbner basis of I. □

pf.) Since R is noetherian by Hilbert's basis theorem, $\mathrm{in}(I)$ is finitely generated. And by Prop 2.5, there exists a finite subset $\{f_1, \dots, f_r\}$ of $I \setminus \{0\}$ such that $\mathrm{in}(I) = (\mathrm{in}(f_1), \dots, \mathrm{in}(f_r))$. Thus, $\{f_1, \dots, f_r\}$ is a Gröbner basis of I. ■

The reason why the Gröbner basis is important is the followwing theorem holds. By the following, we can compute the generators of an given ideal if we can get the Gröbner basis of the ideal.

Th 3.3: (The Gröbner Basis is a Generator System)

Let n' be a positive integer such that $n' \leq n$ and $R' = K[x_1, \dots, x_{n'}] \subset R$. For an ideal I of R, if $S = \{f_1, \dots, f_r\}$ is a Gröbner basis of I, then $I \cap R' = (f_1, \dots, f_r) \cap R'$. In particular, the Gröbner basis of I is a generator system of $I \cap R$. Let the monomial order be with $x_1 < x_2 < \cdots < x_n$. □

pf.) Let $f \in I \cap R'$. Then we have $\mathrm{in}(f) \in \mathrm{in}(I) = (\mathrm{in}(f_1), \cdots, \mathrm{in}(f_r))\, R$. Thus, we can take i such that $\mathrm{in}(f_i) | \mathrm{in}(f)$, i.e. $\mathrm{in}(f) = cq \cdot \mathrm{in}(f_i)$ for some $c \in K, q \in \mathrm{Mon}(R')$. Clearly $\mathrm{in}(f) \in R'$. Thus, $\mathrm{in}(f_i) \in R'$. Because of $x_1 < \cdots x_n$, f_i has only variables $x_1, \dots, x_{n'}$. Thus, $f_i \in R'$. We consider $f - cqf_i$. If $f - cqf_i = 0$, then we have $f \in (f_1, \dots, f_r) \cap R'$. If not, we have $\mathrm{in}(f - cqf_i) < \mathrm{in}(f)$ and $f - cqf_i \in I \cap R'$. Thus, we can repeat the same argument for $f - cqf_i$ instead of f. By Prop 2.6, this algorithm halts in finite steps. Therefore, we have $f \in (f_1, \dots, f_r) \cap R'$. ■

By above theorem, Let $S = \{f_1, \cdots, f_r\}$ be the Gröbner basis of a given ideal I of R. i.e.

$$\mathrm{in}(I) = (\mathrm{in}(f_1), \dots, \mathrm{in}(f_r))$$

holds. Then, we have $I = (f_1, \dots, f_r)$.

Def 3.4: (Reduction)

Let $f, f_1, \ldots, f_m \in R \setminus \{0\}$. We say that r is the *reduction* of g mod $f_1, \ldots, f_m$ if there exist $q_1, \ldots, q_m \in R$ such that

1. $g = q_1 f_1 + \cdots + q_m f_m + r$
2. $\forall i, \quad \mathrm{in}(q_i f_i) \leq \mathrm{in}(g)$
3. $\mathrm{Supp}(r) \cap (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_m)) = \emptyset$

The last condition is in other words, no term of r is divisible by any of $\mathrm{in}(f_1), \ldots, \mathrm{in}(f_m)$. □

We can use to the proof of the existence of *reduced Gröbner basis*. Before showing these properties, we prepare the following proposition.

Prop 3.5

There is the reduction $r \in R$ of $\forall g \in R$ mod $f_1, \ldots, f_m \in R \setminus \{0\}$. □

pf.) We put $J = (\mathrm{in}(f_1), \cdots, \mathrm{in}(f_m))$ and $r = g$ at first. And then we use the reduction algorithm.

1. If $\mathrm{Supp}(r) \cap J = \emptyset$, then r satisfy the conditions of the reduction. Thus, we finish the algorithm.
2. If not, we can find $\mu \in \mathrm{Supp}(r) \cap J$. We take the maximum μ under $\leq$. And we can find i such that $\mathrm{in}(f_i) | \mu$. We put $r' = r - \dfrac{a_\mu \mu}{\mathrm{init}(f_i)} f_i$ where a_μ is the coefficient of μ in r. i.e. we kill the term μ in r by using f_i.

This algorithm halts in finite steps because μ took in step 2 strictly decreases under $\leq$ and there is no infinite descending chain by Prop 2.6. More precisely, in the next step, you may use r' instead of r. And we have

$$r' = r - \frac{a_\mu \mu}{\mathrm{init}(f_i)} f_i = (r - a_\mu \mu) - \frac{a_\mu \mu}{\mathrm{init}(f_i)} (f_i - \mathrm{init}(f_i))$$

On the former term, $(r - a_\mu \mu)$, this has only monomials which is strictly less than that of r. And we have

$$\mathrm{in}\left(\frac{a_\mu \mu}{\mathrm{init}(f_i)} (f_i - \mathrm{init}(f_i)) \right) < \mathrm{in}\left(\frac{a_\mu \mu}{\mathrm{init}(f_i)} \mathrm{in}(f_i) \right) = \mu$$

Therefore, when we go to the next step, $\mu \in \mathrm{Supp}(r') \cap J$ took from step 2 strictly decreases under $\leq$. Thus, this algorithm halts in finite steps.
The algorithm proceeds as follow.

0. $r_0 = g$
1. $r_1 = r_0 - \dfrac{a_{\mu_1} \mu_1}{\mathrm{init}(f_{i_1})} f_{i_1}$
2. $r_2 = r_1 - \dfrac{a_{\mu_2} \mu_2}{\mathrm{init}(f_{i_2})} f_{i_2}$

   $\vdots$

k. $r_k = r_{k-1} - \dfrac{a_{\mu_k} \mu_k}{\mathrm{init}(f_{i_k})} f_{i_k}$

   $\mathrm{Supp}(r_k) \cap J = \emptyset$ i.e. Algorithm halts.

So, by simplifying above, we have $g = q_1 f_1 + \cdots + q_m f_m + r_k$. Let $r = r_k$ eventually. And q is finite summation of the form $\dfrac{a_{\mu_j} \mu_j}{\mathrm{init}(f_{i_j})}$. So we can check

$$\mathrm{in}(q_i f_i) \leq \mathrm{in}(g)$$

holds. Thus, r is the reduction of g mod $f_1, \ldots, f_m$. ■

As the last of this section, we introduce the concept of the *reduced Gröbner basis* and we show the existence and uniqueness of this.

Def 3.6: (Reduced Gröbner Basis)

A Gröbner basis $G = \{g_1, \dots, g_t\}$ of an ideal I of R is called a *reduced Gröbner basis* if the following conditions hold.

1. $\forall i$, the coefficient of $\mathrm{in}(g_i)$ in g_i is 1.
2. If $i \neq j$, then none of the monomials of $\mathrm{Supp}(g_i)$ is divisible by $\mathrm{in}(g_j)$.

□

The second condition is equivalent to that $\mathrm{Supp}(g_i) \cap (\mathrm{in}(g_j)) = \emptyset$ for all $j \neq i$.
The reduced Gröbner basis may be truely basis under the meaning of the following theorem.

Th 3.7: (Existence and Uniqueness of the Reduced Gröbner Basis)

For any ideal I of R, there exists uniquely a reduced Gröbner basis of I. □

pf.) (Existence) We can take a Gröbner basis of I, $G = \{g_1, \dots, g_s\}$ owing to Prop 3.2. And we can assume $\{\mathrm{in}(g_1), \cdots, \mathrm{in}(g_s)\}$ is a minimal generator system of $\mathrm{in}(I)$.
At first, we can take the reduction h_1 of g_1 mod $g_2, \dots, g_s$ by Prop 3.5.

$$\begin{aligned} g_1 &= q_{12}g_2 + \cdots + q_{1s}g_s + h_1 \\ \mathrm{in}(q_{1i}g_i) &\leq \mathrm{in}(g_1) \quad (i = 2, \dots, s) \\ \mathrm{Supp}(h_1) &\cap (\mathrm{in}(g_2), \dots, \mathrm{in}(g_s)) = \emptyset \end{aligned}$$

Clearly, $h_1 \in (g_1, \cdots, g_s) \subset I$. And we have

$$\begin{aligned} \mathrm{in}(g_1) &= \mathrm{in}(q_{12}g_2 + \cdots + q_{1s}g_s + h_1) \\ &\leq \max(\mathrm{in}(q_{12}g_2), \dots, \mathrm{in}(q_{1s}g_s), \mathrm{in}(h_1)) \end{aligned}$$

If we have $\max(\mathrm{in}(q_{12}g_2), \dots, \mathrm{in}(q_{1s}g_s), \mathrm{in}(h_1)) = \mathrm{in}(q_{1i}g_i)$ for some i, then $\mathrm{in}(g_1) \leq \mathrm{in}(q_{1i}g_i) \leq \mathrm{in}(g_1)$. Thus, $\mathrm{in}(g_1) = \mathrm{in}(q_{1i}g_i)$, which contradicts the minimality of G. Therefore, we have

$$\max(\mathrm{in}(q_{12}g_2), \dots, \mathrm{in}(q_{1s}g_s), \mathrm{in}(h_1)) = \mathrm{in}(h_1)$$

Thus, we have $\mathrm{in}(g_1) = \mathrm{in}(h_1)$. then, we replace g_1 by h_1. And we can repeat the same argument for g_2. Namely, we have the follows.

$$\begin{aligned} g_2 &= q_{21}h_1 + q_{23}g_3 + \cdots + q_{2s}g_s + h_2 \\ \mathrm{in}(q_{2i}g_i) &\leq \mathrm{in}(g_2) \quad (i = 1, 3, \dots, s) \\ \mathrm{Supp}(h_2) &\cap (\mathrm{in}(h_1), \mathrm{in}(g_3), \dots, \mathrm{in}(g_s)) = \emptyset \end{aligned}$$

In this point, $Supp(h_1) \cap (\mathrm{in}(h_2), \mathrm{in}(g_3), \dots, \mathrm{in}(g_s)) = \emptyset$ is still hold. So we can replace g_2 by h_2 similar to g_1. And we can repeat this argument for $g_3, \dots, g_s$. Finally, we replace the replaced g_i by $\dfrac{1}{\text{the coefficient of } \mathrm{in}(g_i) \text{ in } g_i} g_i$ for all i to set the initial coefficients to 1. These g_i satisfy follows.

1. $\mathrm{in}(I) = (\mathrm{in}(g_1), \dots, \mathrm{in}(g_s))$
2. The coefficient of $\mathrm{in}(g_i)$ in g_i is 1 for all i.
3. $\mathrm{Supp}(g_i) \cap (\mathrm{in}(g_1), \dots, \mathrm{in}(g_{i-1}), \mathrm{in}(g_{i+1}), \dots, \mathrm{in}(g_s)) = \emptyset$ for all i.

It is nothing else but this is a reduced Gröbner basis of I.
(Uniqueness) Let $G = \{g_1, \dots, g_s\}$ and $G' = \{g'_1, \dots, g'_t\}$ be reduced Gröbner basis of I. Then, we have $\mathrm{in}(I) =$

$(\mathrm{in}(g_1), \dots, \mathrm{in}(g_s)) = (\mathrm{in}(g'_1), \dots, \mathrm{in}(g'_t))$. Thus, we have $s = t$ (Actually, a finite graded R-module M and $\mathfrak{m}$ satisfy NAK, Nakayama's Lemma. So the number of minimal generator of $\mathrm{in}(I)$ is constant. See The Stacks Project [Sta25]) And by minimality, we can assume $\mathrm{in}(g_i) = \mathrm{in}(g'_i)$ for all i. We will show $g_i = g'_i$ for all i. We take i arbitrarily. If $g_i \neq g'_i$, then we can take $0 \neq g_i - g'_i \in I$. We have $\mathrm{in}(g_i - g'_i) \in \mathrm{in}(I)$. And we have $\mathrm{in}(g_i - g'_i) < \mathrm{in}(g_i)$ because initial terms of g_i and g'_i are killed each other. In particular, $\mathrm{in}(g_i - g'_i)$ can not be divisible by $\mathrm{in}(g_i)$. In other case, $j \neq i$, since $\mathrm{Supp}(g_i - g'_i) \subset \mathrm{Supp}(g_i) \cup \mathrm{Supp}(g'_i)$ and none of the monomials of $\mathrm{Supp}(g_i) \cup \mathrm{Supp}(g'_i)$ can not be divisible by $\mathrm{in}(g_j)$. Thus, $\mathrm{in}(g_i - g'_i)$ is fortiori unable to be divisible by $\mathrm{in}(g_j)$. Therefore, $\mathrm{in}(g_i - g'_i) \notin \mathrm{in}(I)$. This is a contradiction. Thus, we have $g_i = g'_i$ for all i. ■

By using above theorem, we can see that the inclusion or equality of two ideals is stable under taking initials.

Cor 3.8

For ideals I, J of R, the following holds.

1. $I \subset J \iff \mathrm{in}(I) \subset \mathrm{in}(J)$
2. $I = J \iff \mathrm{in}(I) = \mathrm{in}(J)$

□

pf.) (1) The direction $\Longrightarrow$ is clear. We will show the direction $\Longleftarrow$. Let $G = \{g_1, \dots, g_s\}$ be the reduced Gröbner basis of I. By definition of the reduced Gröbner basis, Def 3.6, G is a part of the reduced Gröbner basis of J. Thus, by extending G if necessary, we can take the reduced Gröbner basis of J, $G' = \{g_1, \dots, g_s, g_{s+1}, \dots, g_t\}$. Then, we have $I = (g_1, \dots, g_s) \subset (g_1, \dots, g_s, g_{s+1}, \dots, g_t) = J$ by Th 3.3.
(2) This follows from (1). ■

In the next section, we see the Buchberger's criterion and algorithm. it is said that you should go to and learn them if you study the theory of the Gröbner basis.

4 The Buchberger's Criterion and Algorithm

In this section, let K be a field and $R = K[x_1, \dots, x_n]$ be the polynomial ring in n variables over K. And we fix a monomial order $\leq$ on R.

In the previous sections, we saw the definition and some basic properties of the Gröbner basis. However, those are the properties when we can get the Gröbner basis. So, how can we find the Gröbner basis of a given ideal? The Buchberger's criterion and algorithm answer this question. in this theory, the concept of the S-polynomial is important.

Def 4.1: (S-polynomial)

For $f, g \in R \setminus \{0\}$, we define the *$S$-polynomial* of f and g by

$$S(f,g) = \frac{\mathrm{lcm}(\mathrm{in}(f), \mathrm{in}(g))}{\mathrm{init}(f)} f - \frac{\mathrm{lcm}(\mathrm{in}(f), \mathrm{in}(g))}{\mathrm{init}(g)} g$$

Here, $\mathrm{lcm}(\mu, \nu)$ is the least common multiple of monomials μ and ν. □

The S-polynomial of f and g is a polynomial which is made by being canceled the initial terms of f and g each other. The following example may be helpful to understand the construction of the S-polynomial.

Ex 4.2

Let $R = \mathbb{Q}[x, y, z]$ and consider the lex order with $x > y > z$. We take $f = 4x^2yz + 2xy^2 + xz^2, g = 3yz^2 - z + 5$. Then, we have $\mathrm{in}(f) = x^2yz, \mathrm{in}(g) = yz^2$ and $\mathrm{lcm}(\mathrm{in}(f), \mathrm{in}(g)) = x^2yz^2$. Thus, we have

$$\begin{aligned} S(f,g) &= \frac{x^2yz^2}{4x^2yz} f - \frac{x^2yz^2}{3yz^2} g \\ &= \frac{1}{4} z(4x^2yz + 2xy^2 + xz^2) - \frac{1}{3} x^2(3yz^2 - z + 5) \\ &= x^2yz^2 + \frac{1}{2} xyz^2 + \frac{1}{4} xz^3 - x^2yz^2 + \frac{1}{3} x^2z - \frac{5}{3} x^2 \\ &= \cancel{x^2yz^2} + \frac{1}{2} xyz^2 + \frac{1}{4} xz^3 - \cancel{x^2yz^2} + \frac{1}{3} x^2z - \frac{5}{3} x^2 \\ &= \frac{1}{2} xyz^2 + \frac{1}{4} xz^3 + \frac{1}{3} x^2z - \frac{5}{3} x^2 \end{aligned}$$

□

We can use the Th 4.4, Buchberger's criterion, to check whether a given finite subset of an ideal I is a Gröbner basis of I or not.
To show this theorem, we need the following lemma.

Lem 4.3

Let $\mu \in \mathrm{Mon}(R)$, $g_1, \cdots, g_t \in R \setminus \{0\}$, $c_1, \cdots, c_t \in K$. Assume that $\mathrm{in}(g_1), \cdots, \mathrm{in}(g_t) = \mu$. If $\mathrm{in}\left(\sum_i c_i g_i\right) < \mu$, then $\sum_i c_i g_i$ can be written as a linear combination of $S(g_i, g_j)$'s with coefficients in K. □

pf.) We can assume $\mathrm{init}(g_i) = \mu$ for all i. Then, we have

$$S(g_i, g_j) = g_i - g_j$$

And by in $\left(\sum_i c_i g_i\right) < \mu$, we have $\sum_i c_i = 0$. Thus, we have

$$\sum_i c_i g_i = \sum_i c_i (g_i - g_1) = \sum_i c_i S(g_i, g_1)$$

■

Th 4.4: (Buchberger's Criterion)

For an ideal I of R and a finite system of generators $G = \{g_1, \dots, g_t\}$ of $I \setminus \{0\}$, the following are equivalent.

1. G is a Gröbner basis of I.
2. $\forall i, j, \quad S(g_i, g_j)$ has the reduction 0 mod G.

□

pf.) (1) $\Longrightarrow$ (2): Let the following be the reduction of $S(g_i, g_j)$ mod G.

$$S(g_i, g_j) = q_1 g_1 + \cdots + q_t g_t + r$$

and $r \neq 0$. $S(g_i, g_j) \in I$ gives $r \in I$. Thus, we have $\mathrm{in}(r) \in \mathrm{in}(I) = (\mathrm{in}(g_1), \dots, \mathrm{in}(g_t))$. So, we can take k such that $\mathrm{in}(g_k) | \mathrm{in}(r)$. However, this contradicts the condition of the reduction. Thus, we have $r = 0$.
(2) $\Longrightarrow$ (1): Let $f \in I \setminus \{0\}$. We will show $\mathrm{in}(f) \in (\mathrm{in}(g_1), \dots, \mathrm{in}(g_t))$. We define δ_f as follows.

$$\begin{aligned} \mathcal{H}_f &:= \left\{(h_1, \dots, h_t) \in R^t \middle| f = h_1 g_1 + \cdots + h_t g_t\right\} \\ \delta_{(h_1,\dots,h_t)} &= \max_{(h_1,\cdots,h_t) \in \mathcal{H}_f} \{\mathrm{in}(h_1 g_1), \dots, \mathrm{in}(h_t g_t)\} \\ \delta_f &= \min_{(h_1,\dots,h_t) \in \mathcal{H}_f} \delta_{(h_1,\dots,h_t)} \end{aligned}$$

By Prop 2.6, this minimum is exactly takeable. Clearly, $\mathrm{in}(f) \leq \delta_f$.
If $\mathrm{in}(f) = \delta_f$ for all $f \in I$, we can conclude G is a Gröbner basis of I. In fact, if this is true for all $f \in I$, $\mathrm{in}(f) = \delta_f = \delta_{\exists(h_1,\cdots,h_t)} = \exists \mathrm{in}(h_i g_i) \in (\mathrm{in}(g_1), \cdots, \mathrm{in}(g_t))$. Thus, we have $\mathrm{in}(I) \subset (\mathrm{in}(g_1), \dots, \mathrm{in}(g_t))$. And the opposite inclusion is clear.
So, we will show $\mathrm{in}(f) = \delta_f$ for all $f \in I$. Suppose that there exists $f \in I$ such that $\mathrm{in}(f) < \delta_f$. We take such f and $(h_1, \dots, h_t) \in \mathcal{H}_f$ such that $\delta_f = \delta_{(h_1,\dots,h_t)}$. Then,

$$\begin{aligned} f &= h_1 g_1 + \cdots + h_t g_t \\ &= \sum_{\mathrm{in}(h_i g_i) = \delta_f} h_i g_i + \sum_{\mathrm{in}(h_i g_i) < \delta_f} h_i g_i \\ &= \sum_{\mathrm{in}(h_i g_i) = \delta_f} \mathrm{init}(h_i) g_i + \sum_{\mathrm{in}(h_i g_i) = \delta_f} (h_i - \mathrm{init}(h_i)) g_i + \sum_{\mathrm{in}(h_i g_i) < \delta_f} h_i g_i \end{aligned}$$

Since $\mathrm{in}(f) < \delta_f$, we have

$$\mathrm{in}\left(\sum_{\mathrm{in}(h_i g_i) = \delta_f} \mathrm{init}(h_i) g_i\right) < \delta_f$$

Thus, by Lem 4.3, this sum is a linear combination of $S(\mathrm{in}(h_j) g_j, \mathrm{in}(h_k) g_k)$ with coefficients in K and with $\mathrm{in}(h_j g_j) = \mathrm{in}(h_k g_k) = \delta_f$. We can easily compute $S(\mathrm{in}(h_j) g_j, \mathrm{in}(h_k) g_k)$ as follows.

$$S(\mathrm{in}(h_j) g_j, \mathrm{in}(h_k) g_k) = \frac{\mathrm{lcm}(\mathrm{in}(h_j)\mathrm{in}(g_j), \mathrm{in}(h_k)\mathrm{in}(g_k))}{\cancel{\mathrm{in}(h_j)}\mathrm{init}(g_j)} \cancel{\mathrm{in}(h_j)} g_j - \frac{\mathrm{lcm}(\mathrm{in}(h_j)\mathrm{in}(g_j), \mathrm{in}(h_k)\mathrm{in}(g_k))}{\cancel{\mathrm{in}(h_k)}\mathrm{init}(g_k)} \cancel{\mathrm{in}(h_k)} g_k$$

$$
\begin{aligned}
&= \frac{\delta_f}{\mathrm{init}(g_j)} g_j - \frac{\delta_f}{\mathrm{init}(g_k)} g_k \\
&= \frac{\delta_f}{\mathrm{lcm}(\mathrm{in}(g_j), \mathrm{in}(g_k))} \left(\frac{\mathrm{lcm}(\mathrm{in}(g_j), \mathrm{in}(g_k))}{\mathrm{init}(g_j)} g_j - \frac{\mathrm{lcm}(\mathrm{in}(g_j), \mathrm{in}(g_k))}{\mathrm{init}(g_k)} g_k \right) \\
&= \frac{\delta_f}{\mathrm{lcm}(\mathrm{in}(g_j), \mathrm{in}(g_k))} S(g_j, g_k)
\end{aligned}
$$

Let $u_{jk} = \dfrac{\delta_f}{\mathrm{lcm}(\mathrm{in}(g_j), \mathrm{in}(g_k))}$. Then, we have

$$
\sum_{\mathrm{in}(h_i g_i) = \delta_f} \mathrm{init}(h_i) g_i = \sum_{j,k} c_{jk} u_{jk} S(g_j, g_k)
$$

with some $c_{jk} \in K$. We note that

$$
\mathrm{in}(u_{jk} S(g_j, g_k)) < \delta_f
$$

By using the assumption of (2), there is an expression

$$
S(g_j, g_k) = \sum_i p_i^{jk} g_i \quad (p_i^{jk} \in R)
$$

And note that

$$
\mathrm{in}(p_i^{jk} g_i) \leq \mathrm{in}(S(g_j, g_k))
$$

So we have eventually

$$
\sum_{\mathrm{in}(h_i g_i) = \delta_f} \mathrm{init}(h_i) g_i = \sum_{\mathrm{in}(h_j g_j) = \mathrm{in}(h_k g_k) = \delta_f} c_{jk} u_{jk} \left(\sum_i p_i^{jk} g_i \right)
$$

When we rearrange the right hand side with respect to g_i, let the equation be

$$
\sum_i h_i' g_i
$$

Then, we have $\mathrm{in}(h_i' g_i) < \delta_f$ for all i. Finally, we have

$$
\begin{aligned}
f &= \sum_{\mathrm{in}(h_i g_i) = \delta_f} \mathrm{init}(h_i) g_i + \sum_{\mathrm{in}(h_i g_i) = \delta_f} (h_i - \mathrm{init}(h_i)) g_i + \sum_{\mathrm{in}(h_i g_i) < \delta_f} h_i g_i \\
&= \sum_i h_i' g_i + \sum_{\mathrm{in}(h_i g_i) = \delta_f} (h_i - \mathrm{init}(h_i)) g_i + \sum_{\mathrm{in}(h_i g_i) < \delta_f} h_i g_i
\end{aligned}
$$

Then, we find all the terms in this equation satisfy $\mathrm{in}(h_i'' g_i) < \delta_f$ for all i. This contradicts the definition of δ_f. Thus, we have $\mathrm{in}(f) = \delta_f$ for all $f \in I$. ■

And then, we can compute the Gröbner basis of a given ideal by using the Buchberger's algorithm. Let $I = (g_1, g_2, \ldots, g_t)$ be an ideal of R. If there is i, j such that $S(g_i, g_j)$ does not have the reduction $h_{ij} \neq 0 \bmod \{g_1, \ldots, g_t\}$, then we add h_{ij} to $\{g_1, \ldots, g_t\}$. By the definition of the reduction, $\mathrm{in}(h_{ij}) \notin (\mathrm{in}(g_1), \ldots, \mathrm{in}(g_t))$. this process halts in finite steps by Prop 2.6. And when this process halts, the resulting set is a Gröbner basis of I by Th 4.4.

 © Riley

[BCRV22] Winfried Bruns, Aldo Conca, Claudiu Raicu, and Matteo Varbaro. *Determinants, Gröbner Bases and Cohomology*. Springer Monographs in Mathematics. Springer Cham, 1 edition, 2022. Published: 03 December 2022. Series ISSN: 1439-7382, Series E-ISSN: 2196-9922. Copyright: Springer Nature Switzerland.

[HH11] Jürgen Herzog and Takayuki Hibi. *Monomial Ideals*, volume 260 of *Graduate Texts in Mathematics*. Springer Verlag, London, United Kingdom, 2011. In English and Japanese. Topics: Ideals (Algebra), Commutative algebra, Combinatorial analysis.

[Sta25] The Stacks project authors. The stacks project, tag 0ekb. https://stacks.math.columbia.edu/tag/0EKB, 2025.

 © Riley