# Introduction to Gröbner Basis Special

Riley @Na2COOH\_2

September 17, 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	3
2	Monomial Orders	4
3	The Gröbner Basis	7
4	The Buchberger's Criterion and Algorithm	11

#### Introduction 1

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.

## 2 Monomial Orders

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.

## 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  $\mu$  is a monomial. We denote the set of all monomials in R by Mon(R).

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

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

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

## Def 2.2: (Support)

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

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

Of course, Supp(f) is a finite set. And we can express f uniquely as

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

where  $a_{\mu} \in K \setminus \{0\}$  is the coefficient of  $\mu$  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):  $\mu \leq_{\text{lex}} \nu$  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):  $\mu \leq_{\text{deglex}} \nu$  if and only if  $\deg \mu = \sum a_i < \sum b_i = \deg \nu$  or  $\sum a_i = \sum b_i$  and  $\mu \leq_{\text{lex}} \nu$ .
- 3. (degree) reverse lexicographic order (degrevlex):  $\mu \leq_{\text{degrevlex}} \nu$  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.  $\Box$ 

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 Mon(R) has the minimum element. In particular, there is no infinite descending chain

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

pf.) We take  $\emptyset \neq N \subset \text{Mon}(R)$  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  $I=(f_1,\cdots,f_r)\ (f_i\in N)$ . 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.  $\forall \mu\in N$ ,  $\mu=s_1f_1+\cdots+s_rf_r$  using  $s_i\in R$ . Since  $\mu,f_1,\cdots,f_r$  are monomials, we have  $\mu=sf_i$  for some i and  $s\in R$ . (Think about the computation of the right hand side. ) Then,  $\mu=sf_i\geq f_i\geq f_1$ . 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

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

Note that  $\text{in}_{\leq}(f)$  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  $\text{init}_{\leq}(f)$ . We often omit the subscript  $\leq$  if there is no confusion.

We can easily check that  $\operatorname{in}(fg) = \operatorname{in}(f)\operatorname{in}(g), \ \operatorname{in}(f+g) \leq \operatorname{max}(\operatorname{in}(f), \operatorname{in}(g)) \ \text{for} \ f, g \in \mathbb{R} \setminus \{0\}.$ For an ideal I of R, we define the *initial ideal* of I by

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

We often omit the subscript  $\leq$  if there is no confusion, 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 in(I) as a K-vector space generated by  $\{\inf(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 in(I) is equal to the K-vector space generated by  $\{\inf(f)|f\in I\setminus\{0\}\}$ .

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

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

Then, we have

$$f = \sum_{i=1}^{r} g_i \mu_i$$

$$= \sum_{i=1}^{r} \left( \sum_{j=1}^{r_i} a_{ij} \mu_{ij} \right) \mu_i$$

$$= \sum_{i=1}^{r} \sum_{j=1}^{r_i} a_{ij} \mu_{ij} \operatorname{in}(f_i)$$

$$= \sum_{i=1}^{r} \sum_{j=1}^{r_i} a_{ij} \operatorname{in}(\mu_{ij} f_i) \in V$$

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  $R = K[x_1, ..., x_n]$  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  $\{f_1, \ldots, f_r\}$  of  $I \setminus \{0\}$  is called a *Gröbner basis* of I if

$$in(I) = (in(f_1), \dots, in(f_r))$$

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  $\operatorname{in}(I)$ , we call it a *Gröbner basis* of I.

Of course, in general,

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

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,  $\operatorname{in}(I)$  is finitely generated. And by Prop 2.5, there exists a finite subset  $\{f_1,\ldots,f_r\}$  of  $I\setminus\{0\}$  such that  $\operatorname{in}(I)=(\operatorname{in}(f_1),\ldots,\operatorname{in}(f_r))$ . Thus,  $\{f_1,\ldots,f_r\}$  is a Gröbner basis of I

The reason why the Gröbner basis is important is the following 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: (Th e Gröbner Basis is a Generator System)

Let n' be a positive integer such that  $n' \leq n$  and  $R' = K[x_1, \ldots, x_{n'}] \subset R$ . For an ideal I of R, if  $S = \{f_1, \ldots, f_r\}$  is a Gröbner basis of I, then  $I \cap R' = (f_1, \ldots, f_r) \cap R'$ . 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  $\operatorname{in}(f) \in \operatorname{in}(I) = (\operatorname{in}(f_1), \dots, \operatorname{in}(f_r)) R$ . Thus, we can take i such that  $\operatorname{in}(f_i)|\operatorname{in}(f)$ , i.e.  $\operatorname{in}(f) = cq \cdot \operatorname{in}(f_i)$  for some  $c \in K, q \in \operatorname{Mon}(R')$ . Clearly  $\operatorname{in}(f) \in R'$ . Thus,  $\operatorname{in}(f_i) \in R'$ . 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  $\operatorname{in}(f - cqf_i) < \operatorname{in}(f)$  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  $S = \{f_1, \dots, f_r\}$  be the Gröbner basis of a given ideal I of R. i.e.

$$in(I) = (in(f_1), \dots, in(f_r))$$

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

## 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. 
$$g = q_1 f_1 + \dots + q_m f_m + r$$

2. 
$$\forall i$$
,  $\operatorname{in}(q_i f_i) < \operatorname{in}(q)$ 

3. Supp
$$(r) \cap (\operatorname{in}(f_1), \dots, \operatorname{in}(f_m)) = \emptyset$$

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

The reason why we introduce this concept, reduction, is reffffff holds. And we can use to the proof of the existence of reduced Gröbner basis, reffffff. 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  $J = (in(f_1), \dots, in(f_m))$  and r = g at first. And then we use the reduction algorithm.
  - 1. If  $\operatorname{Supp}(r) \cap J = \emptyset$ , then r satisfy the conditions of the reduction. Thus, we finish the algorithm.
  - 2. If not, we can find  $\mu \in \operatorname{Supp}(r) \cap J$ . We take the maximum  $\mu$  under  $\leq$ . And we can find i such that  $\operatorname{in}(f_i)|\mu$ . We put  $r' = r \frac{a_{\mu}\mu}{\operatorname{init}(f_i)} f_i$  where  $a_{\mu}$  is the coefficient of  $\mu$  in r. i.e. we kill the term  $\mu$  in r by using  $f_i$ .

This algorithm halts in finite steps because  $\mu$  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

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

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

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

Therefore, when we go to the next step,  $\mu \in \operatorname{Supp}(r') \cap J$  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. 
$$r_1 = r_0 - \frac{a_{\mu_1} \mu_1}{\operatorname{init}(f_{i_1})} f_{i_1}$$

2. 
$$r_2 = r_1 - \frac{a_{\mu_2}\mu_2}{\operatorname{init}(f_{i_2})} f_{i_2}$$

:

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

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

So, by simplifying above, we have  $g=q_1f_1+\cdots+q_mf_m+r_k$ . Let  $r=r_k$  eventually. And q is finite summation of the form  $\frac{a_{\mu_j}\mu_j}{\mathrm{init}(f_{i_j})}$ . So we can check

$$in(q_i f_i) \leq in(q)$$

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

To show the theorem reffffff, we need to study the Buchberger's criterion and Algorithm. So, this is proved in the next section.

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

The second condition is equivalent to that  $\operatorname{Supp}(g_i) \cap (\operatorname{in}(g_j)) = \emptyset$  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,  $G = \{g_1, \ldots, g_s\}$  owing to Prop 3.2. And we can assume  $\{\operatorname{in}(g_1), \cdots, \operatorname{in}(g_s)\}$  is a minimal generator system of  $\operatorname{in}(I)$ . At first, we can take the reduction  $h_1$  of  $g_1 \mod g_2, \ldots, g_s$  by Prop 3.5.

$$g_1 = q_{12}g_2 + \dots + q_{1s}g_s + h_1$$
  

$$\operatorname{in}(q_{1i}g_i) \le \operatorname{in}(g_1) \quad (i = 2, \dots, s)$$
  

$$\operatorname{Supp}(h_1) \cap (\operatorname{in}(g_2), \dots, \operatorname{in}(g_s)) = \emptyset$$

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

$$in(g_1) = in(q_{12}g_2 + \dots + q_{1s}g_s + h_1)$$
  

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

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

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

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

$$g_2 = q_{21}h_1 + q_{23}g_3 + \dots + q_{2s}g_s + h_2$$
  

$$in(q_{2i}g_i) \le in(g_2) \quad (i = 1, 3, \dots, s)$$
  

$$Supp(h_2) \cap (in(h_1), in(g_3), \dots, in(g_s)) = \emptyset$$

In this point,  $Supp(h_1) \cap (\operatorname{in}(h_2), \operatorname{in}(g_3), \dots, \operatorname{in}(g_s)) = \emptyset$  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  $\frac{1}{\operatorname{the coefficient of in}(g_i) \operatorname{in} g_i} g_i$  for all i to set the initial coefficients to 1. These  $g_i$  satisfy follows.

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

(Uniqueness) Let  $G = \{g_1, \ldots, g_s\}$  and  $G' = \{g'_1, \ldots, g'_t\}$  be reduced Gröbner basis of I. Then, we have  $\operatorname{in}(I) = (\operatorname{in}(g_1), \ldots, \operatorname{in}(g_s)) = (\operatorname{in}(g'_1), \ldots, \operatorname{in}(g'_t))$ . 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  $\operatorname{in}(I)$  is constant. See The Stacks Project [Sta25]) And by minimality, we can assume  $\operatorname{in}(g_i) = \operatorname{in}(g'_i)$  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  $\operatorname{in}(g_i - g'_i) \in \operatorname{in}(I)$ . And we have  $\operatorname{in}(g_i - g'_i) < \operatorname{in}(g_i)$  because initial terms of  $g_i$  and  $g'_i$  are killed each other. In particular,  $\operatorname{in}(g_i - g'_i)$  can not be divisible by  $\operatorname{in}(g_i) \cup \operatorname{Supp}(g'_i)$  and none of the monomials of  $\operatorname{Supp}(g_i) \cup \operatorname{Supp}(g'_i)$  can not be divisible by  $\operatorname{in}(g_j)$ . Thus,  $\operatorname{in}(g_i - g'_i)$  is fortiori unable to be divisible by  $\operatorname{in}(g_j)$ . Therefore,  $\operatorname{in}(g_i - g'_i) \notin \operatorname{in}(I)$ . 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. 
$$I \subset J \iff \operatorname{in}(I) \subset \operatorname{in}(J)$$

2. 
$$I = J \iff \operatorname{in}(I) = \operatorname{in}(J)$$

pf.) (1) The direction  $\Longrightarrow$  is clear. We will show the direction  $\longleftarrow$ . Let  $G = \{g_1, \ldots, g_s\}$  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,  $G' = \{g_1, \ldots, g_s, g_{s+1}, \ldots, g_t\}$ . Then, we have  $I = (g_1, \ldots, g_s) \subset (g_1, \ldots, g_s, g_{s+1}, \ldots, g_t) = J$  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  $R = K[x_1, ..., x_n]$  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

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

Here,  $lcm(\mu, \nu)$  is the least common multiple of monomials  $\mu$  and  $\nu$ .

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  $\operatorname{in}(f) = x^2yz$ ,  $\operatorname{in}(g) = yz^2$  and  $\operatorname{lcm}(\operatorname{in}(f), \operatorname{in}(g)) = x^2yz^2$ . Thus, we have

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

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