Introduction to Gröbner Basis Special

Riley @Na2COOH_2

September 7, 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.

Figure 1: Bruno Buchberger

Table of Contents

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. https://sites.google.com/view/comm-ring-summer-school-2025/%E3%83%9B%E3%83%BC%E3%83%A0?authuser=0

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 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 minimal 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 $\mathrm{init}_{\leq}(f)$. 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 $f \in V$. ■

The Gröbner Basis

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. 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

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

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,

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

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 $\{f_1, \ldots, f_r\}$ of $I \setminus \{0\}$ such that $\mathrm{in}(I) = (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_r))$. Thus, $\{f_1, \ldots, f_r\}$ is a Gröbner basis of I. ■

Def 3.3: (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 $\mathrm{in}(f_1), \ldots, \mathrm{in}(f_m)$. □

The reason why we introduce this concept, reduction, is reffffff holds. Before showing this theorem, we prepare the following proposition.

Prop 3.4

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.

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

■

[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.