An Introduction to Gröbner Bases

Anwyn Woodyatt

June 1, 2023

Abstract

The aim of this paper is to provide an undergraduate friendly introduction to the concept of Gröbner bases and demonstrate an elementary application. After motivating the subject we build a solid foundation before formally defining, proving the existence of, and providing the original Buchberger's algorithm to compute, said Gröbner basis. Although this paper is designed to be readable without reference, if needed we direct the reader to [1] for more background information on the construction of Gröbner bases and to [2] for algebraic definitions and theory. This paper summarizes the beginning of a diverse Directed Reading Program (DRP) project at McGill University.

1 Prerequisites

Amongst a general understanding of multi-variable polynomial rings and ideals, this paper will use, in proof, the following results from an undergraduate course in ring theory:

Definition 1. A *monomial* in $K[x_1, ..., x_n]$ is represented by x^α where $x = (x_1, ..., x_n)$ and $\alpha = (a_1, ..., a_n) \in \mathbb{Z}^n_{\geq 0}$.

Lemma 1. (cf. [1]) Let $I = \langle x^\alpha \mid \alpha \in S \subseteq \mathbb{Z}^n_{\geq 0} \rangle$ be a monomial ideal. Then a monomial x^β is an element of I if and only if $x^\alpha \mid x^\beta$ for some $\alpha \in S$.

Definition 2. A commutative ring with unity K is called *Noetherian* if and only if for every increasing chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ of K, $\exists\, N \in \mathbb{Z}_{\geq 0}$ such that $I_n = I_N \;\forall\, n \geq N$.

We have an equivalent definition of *Noetherian*:

Definition 2. A commutative ring with unity K is called *Noetherian* if and only if every ideal I of K is finitely generated.

Theorem 1 (Hilbert Basis Theorem). (cf. [2]) If K is a Noetherian ring then $K[x]$ is a Noetherian ring. Inductively, $K[x_1, ..., x_n]$ is a Noetherian ring.

Proposition 1. (cf. [2]) Every field is Noetherian.

2 Introduction

In his 1965 Ph.D. thesis, Bruno Buchberger introduced the new concept of a *Gröbner basis*, named after his advisor Wolfgang Gröbner. He provided the *Buchberger Algorithm* to compute them (the one we will state and prove in this paper) at the same time (cf. [3]).

We acknowledge that many years earlier in 1913, Nikolai Günther of Russia made a similar discovery; his work published in Russian journals but ignored internationally until it was recognized in the 1980s (cf. [3]).

The Buchberger algorithm is motivated by what is known as the *Ideal Membership Problem* (cf. 6) which asks: given a field K and an ideal I of $K[x_1, ...x_n]$, how can we determine if $f \in K[x_1, ..., x_n]$ is an element of I? We know that for a commutative ring, we can write an element of I as a linear combination of the generators. Thus, as one would do in the single variable case, it would be intuitive to divide our polynomial by the generators of I simultaneously using the division algorithm for multi-variable polynomial rings (cf. 3), and if the algorithm terminates with zero remainder, we have an element of I. Alas, we will show in the following section that we run into several issues using this method. Namely, unlike the division algorithm in one variable, the multi-variable division algorithm does not output a unique remainder unless the order of divisors is fixed. Consequently, an element of I can have a non-zero remainder. This dilemma says that zero remainder is *sufficient* for ideal membership but not *necessary*. We are left to wonder: can we find a basis such that the unique remainder is independent of divisor order, thus providing a sufficient *and* necessary way to determine elements of I? Indeed! The Gröbner basis of I!

This relatively modern idea has led to many fascinating applications and discoveries in mathematics and science.

3 Ordering and Division Algorithm in $K[x_1, ..., x_n]$

In one variable, we are familiar with the terms *degree* of a *monomial*, and *degree* of a *polynomial*. How do these definitions change for multi-variable polynomials?

Let us consider the two variable case: $\mathbf{x} = (x, y)$. Suppose you have the monomials x^2y and xy^2. Both have the same *total degree* $(1 + 2 = 2 + 1 = 3)$. Which one would you define as *greater* than the other? In fact, it depends on the definition of *monomial ordering* you choose. We provide a few common examples of monomial orderings before outlining the formal criteria.

Definition 3. (Lexicographic Order) Let $\alpha = (a_1, ..., a_n)$, $\beta = (b_1, ..., b_n) \in \mathbb{Z}^n_{\geq 0}$. If $\alpha - \beta$ has a positive leftmost non-zero entry, then we say $\alpha >_{lex} \beta$, i.e. the degree α is greater than degree β with respect to lexicographic ordering. We can equivalently say that x^α is greater than x^β as monomials.

Example. $x > y > z$ since $x = x^1y^0z^0$, $y = x^0y^1z^0$, $z = x^0y^0z^1$ and
$(1, 0, 0) - (0, 1, 0) = (1, -1, 0)$, $(0, 1, 0) - (0, 0, 1) = (0, 1, -1)$, i.e. we have alphabetical ordering.

Definition 4. (Graded Lex Order) Let α, β as above. If

$$|\alpha| = \sum_{i=1}^{n} a_i > |\beta| = \sum_{i=1}^{n} b_i$$

or

$$|\alpha| = |\beta| \; and \; \alpha >_{lex} \beta,$$

then we say $\alpha >_{grlex} \beta$.
$|\alpha|$ is denoted the *total degree.*

Example. We first notice that again we have alphabetical ordering of the variables. Another example is $x^4y^7z >_{grlex} x^4y^2z^3$ since $|(4,7,1)| = 12 > 9 = |(4,2,3)|$.

Definition 5. (Graded Reverse Lex Order) Let α, β as above. If

$$|\alpha| = \sum_{i=1}^{n} a_i > |\beta| = \sum_{i=1}^{n} b_i$$

or

$$|\alpha| = |\beta| \; and \; the \; rightmost \; nonzero \; entry \; of \; \alpha - \beta \; is \; negative,$$

then we say $\alpha >_{grevlex} \beta$.

Example. We have the same example as above: $x^4y^7z >_{grevlex} x^4y^2z^3$ because *grevlex* and *grlex* both order by total degree first, but break ties in different ways.
Another example is $(2,3,2) >_{grevlex} (0,0,7)$ since $(2,3,2) - (0,0,7) = (2,3,-5)$.

Definition 6. We call $>$ a *monomial ordering* on the set of monomials $\{x^\alpha | x = (x_1, ..., x_n), \alpha \in \mathbb{Z}^n_{\geq 0}\}$ in $K[x_1, ..., x_n]$ if it is a relation satisfying the following conditions:
(i) $>$ is a *total* (linear) ordering, i.e. exactly one of

$$x^\alpha > x^\beta, \; x^\alpha = x^\beta, \; x^\beta > x^\alpha$$

is true and the ordering in *transitive*.
(ii) If $x^\alpha > x^\beta, \gamma \in \mathbb{Z}^n_{\geq 0}$, then $x^{\alpha+\gamma} > x^{\beta+\gamma}$
(iii) $>$ is a *well-ordering*, i.e. there exists a (not necessarily unique) minimal monomial.

You may be wondering... Do we *have* to impose an ordering? If we do not, then we also run into uniqueness of remainder problems as mentioned in the introduction.

We need just a few more pieces of terminology before we have the foundation to discuss Gröbner bases.

Definition 7. Let $f = \sum_{i=1}^{n} c_i x^{\alpha_i} \in K[x_1, ..., x_n]$ (without loss of generality, none of the α_i are equal, otherwise combine them). The *leading term* of f is $LT(f) = c_k x^{\alpha_k}$ such that $\alpha_k > \alpha_i \; \forall \, i$. c_k is denoted the *leading coefficient.*

Definition 8. As above, let $f = \sum_{i=1}^{n} c_i x^{\alpha_i} \in K[x_1, ..., x_n]$. The *leading monomial* of f is $LM(f) = x^{\alpha_k}$ such that $\alpha_k > \alpha_i \; \forall \, i$.

For the definition and proof of the ***division algorithm*** in $K[x_1, ..., x_n]$, we reference [1] (chapter 2.3). It is easy to grasp by examples, which follow. Like normal division, we have a divisor, dividend, quotient and remainder; what's different is that we can have multiple divisors and quotients. Essentially, we start by dividing the leading term (determined by the choice of ordering) of the dividend by divisor one (top most), which builds quotient one, and if in any particular step we cannot divide by divisor one, we move to divisor two and build quotient two, etc. If at any step we cannot divide the leading term by any of the divisors, that leading term becomes the remainder of that step (bold in below examples) and we continue the division by carrying down the remaining terms. At the end, we add the remainders of each step for a total remainder.

As we will see in the coming examples, the choice of ordering can simplify or complicate polynomial division in $K[x_1, ..., x_n]$ (sometimes greatly). We also see that, unless order of divisors is fixed, the remainder is not unique — even with a chosen ordering.

The following problems and the worked example in 4 are taken from [1], where additional examples and exercises can be found, but worked out independently.

Example. Order of divisors matters. We use *lex* ordering in the following two divisions.

$$
\begin{array}{rr}
 & \scriptstyle q_1=x+y \\
 & \scriptstyle q_2=1 \\ \cline{2-2}
\begin{smallmatrix} xy-1 \\ y^2-1 \end{smallmatrix}\Big) & x^2y+xy^2+y^2 \\
 & -\ (x^2y-x) \quad \\ \cline{2-2}
 & xy^2+x+y^2 \\
 & -\ (xy^2-y) \\ \cline{2-2}
 & \mathbf{x}+y^2+y \\ \cline{2-2}
 & y^2+y \\
 & -\ (y^2-1) \\ \cline{2-2}
 & \mathbf{y}+1 \\ \cline{2-2}
 & \mathbf{1}
\end{array}
$$

With remainder $\mathbf{x}+\mathbf{y}+\mathbf{1}$.
We conclude that $x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1$.

On the other hand, switching the order of divisors gives

$$
\begin{array}{rr}
 & \scriptstyle q_1=x+1 \\
 & \scriptstyle q_2=x \\ \cline{2-2}
\begin{smallmatrix} y^2-1 \\ xy-1 \end{smallmatrix}\Big) & x^2y+xy^2+y^2 \\
 & -\ (x^2y-x) \quad \\ \cline{2-2}
 & xy^2+x+y^2 \\
 & -\ (xy^2-x) \\ \cline{2-2}
 & \mathbf{2x}+y^2 \\ \cline{2-2}
 & y^2 \\
 & -\ (y^2-1) \\ \cline{2-2}
 & \mathbf{1}
\end{array}
$$

With remainder **2x+1**.
We conclude that $x^2y + xy^2 + y^2 = (x+1)\cdot(y^2-1) + x\cdot(xy-1) + 2x + 1$ — a different remainder!

We now compute the second division again, this time using *grlex* ordering:

$$
\begin{array}{r r}
 & {\scriptstyle q_1 = x+1} \\
 & {\scriptstyle q_2 = x} \\ \cline{2-2}
{\scriptstyle y^2-1 \atop xy-1} \big) & x^2y + xy^2 + y^2 \\
 & -\quad (x^2y - x) \\ \cline{2-2}
 & xy^2 + y^2 + x \\
 & -\quad (xy^2 - x) \\ \cline{2-2}
 & y^2 + 2x \\
 & -\quad (y^2 - 1) \\ \cline{2-2}
 & \mathbf{2x+1}
\end{array}
$$

We highlight that we were able to continue dividing by f_1 at step 3, unlike before, because $y^2 >_{grlex} 2x$ whereas $2x >_{lex} y^2$.

4 Algorithm to Construct Gröbner Bases and Proof of Existence

The preceding section brings to light the obstacle that the Ideal Membership Problem faces. With a fixed ordering, we now construct a new basis from our original basis of I such that division in any order of this new basis results in a unique remainder.

Definition 9. Let K be a field. Let $I \lhd K[x_1, ..., x_n]$. We say the set $G = \{g_1, ..., g_n\}$ is a *Gröbner basis* for I if $\langle LT(g_1), ...LT(g_n)\rangle = \langle LT(I)\rangle$, where $\langle LT(I)\rangle$ is the ideal generated by the set of leading terms of elements of I. It follows that $\langle g_1, ..., g_n\rangle = I$.

Definition 10. Let x^α, x^β be monomials. Let $\operatorname{lcm}(x^\alpha, x^\beta) = x^\gamma$, $\gamma = (c_1, ...c_n)$, $c_i = max\{a_i,\ b_i\}$. We define $S(f,g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$ where $x^\gamma = \operatorname{lcm}(LM(f), LM(g))$.

Theorem 1 (Buchberger's Criterion). Let $I \lhd K[x_1, ..., x_n]$ such that $I = \langle g_1, ...g_d\rangle$. Then $G = \{g_1, ..., g_d\}$ is a Gröbner basis if and only if $\overline{S(g_i, g_j)}^G = 0\, \forall\, i, j \in \{1, ..., d\}$, where $\overline{S(g_i, g_j)}^G$ denotes the remainder of $S(g_i, g_j)$ divided by the set G.

Proof. ($\Leftarrow$:) We need to show that $\langle LT(g_1), ...LT(g_d)\rangle = \langle LT(I)\rangle$.

$\langle LT(g_1), ...LT(g_d)\rangle \subseteq \langle LT(I)\rangle$ is clear since g_i in $I \Rightarrow LT(g_i) \in \langle LT(I)\rangle \forall i \in \{1, ..., d\}$. Thus $\langle LT(g_1), ...LT(g_d)\rangle \subseteq \langle LT(I)\rangle$ since $\langle LT(I)\rangle$ is closed under finite linear combinations and an arbitrary element of $\langle LT(g_1), ...LT(g_d)\rangle$ is $f_1 LT(g_1) + ... + f_d LT(g_d)$ for $f_i \in K[x_1, ..., x_n]$.

It remains to show that $\langle LT(I)\rangle \subseteq \langle LT(g_1), ...LT(g_d)\rangle$, and by the same reasoning as above, it is sufficient to show that $LT(I) \subseteq \langle LT(g_1), ...LT(g_d)\rangle$. Let f be arbitrary $\in I$,

$LT(f) = a_n x^{\alpha_n} \in LT(I)$. Write:

$$f = a_n x^{\alpha_n} + a_{n-1} x^{\alpha_{n-1}} + ... + a_0 = \sum_{i=1}^{d} h_i g_i, h_i \in K[x_1, ..., x_n]$$

We can write f this way since it is assumed that $I = \langle g_1, ..., g_d \rangle$.
By Lemma 1, we need to show that $a_n x^{\alpha_n}$ is divisible by one of $LT(g_i), ..., LT(g_d)$. Let $\delta = max(deg(h_i g_i))$. There are two cases:

1. $\delta = deg(f) = \alpha_n$, the case with no cancellation in the sum of f.

2. $\delta > deg(f)$, the case with cancellation in the sum of f.

Let's deal with case 1 first, then we will produce $f = \sum_{i=1}^{d} h_i' g_i$ such that $max(deg(h_i' g_i)) = \delta' < \delta$, so we can inductively reduce to case 1.

Suppose $f = h_1 g_1 + ... + h_d g_d$ with $deg(f) = \delta$ and $deg(h_i g_i) \leq \delta$ (at least one equality). Then for some $i \in \{1, ..., d\}, LM(f) = LM(h_i g_i) = LM(g_i) LM(h_i)$. So in this case, $LM(g_i) | LM(f)$ and hence $LT(g_i) | LT(f)$ since

$$LM(f) = x^\delta = LM(h_i) LM(g_i)$$

$$\begin{aligned} \Rightarrow a_n x^\delta &= a_n LM(h_i) LM(g_i) \\ &= \frac{a_n}{b_i} LM(h_i) \cdot b_i LM(g_i) \\ &:= \frac{a_n}{b_i} LM(h_i) LT(g_i) \end{aligned}$$

where $b_i \neq 0$ since $LT(g_i) \neq 0$. This gives case 1.

We now look at **case 2**. We will need a lemma which we state and prove now.

<u>Lemma 2.</u> If $deg(p_i) = \delta \, \forall \, i$ and $deg(\sum_{i=1}^{n} p_i) < \delta$, then $\exists \, a_{ij} \in K$ such that $\sum_{i=1}^{n} p_i = \sum_{i,j}^{n} a_{ij} S(p_i, p_j)$.

Proof. $S(p_i, p_j) = \frac{x^\delta}{LT(p_i)} \cdot p_i - \frac{x^\delta}{LT(p_j)} \cdot p_j$ where $LT(p_i) = b_i x^\delta$ and $LT(p_j) = b_j x^\delta$.

Fix j. Then,

$$\begin{aligned} \sum_{\substack{i=1 \\ i \neq j}}^{n} b_i \left(\frac{p_i}{b_i} - \frac{p_j}{b_j}\right) &= \sum_{\substack{i=1 \\ i \neq j}}^{n} \left(p_i - \frac{b_i}{b_j} p_j\right) \\ &= \sum_{\substack{i=1 \\ i \neq j}}^{n} p_i - \frac{p_j}{b_j} \sum_{\substack{i=1 \\ i \neq j}}^{n} b_i \\ &= \sum_{i=1}^{n} p_i \end{aligned}$$

Where $(\frac{p_i}{b_i} - \frac{p_j}{b_j}) = S(p_i, p_j)$ and $\sum_{\substack{i=1 \\ i \neq j}}^{n} b_i = 0$ since the sum has degree $< \delta$.

$\square$

Now write:

$$f = \sum_{deg(h_i g_i) > deg(f)} h_i g_i + \sum_{deg(h_i g_i) \leq deg(f)} h_i g_i$$

$deg(h_i g_i) = \delta \Rightarrow deg(LT(h_i)g_i) = \delta$ by well-ordering, so we have

$$\begin{aligned} &= \sum_{deg(h_i g_i) = \delta} LT(h_i) g_i + \sum_{deg(h_i g_i) = \delta} (h_i - LT(h_i)) g_i \\ &+ \sum_{deg(f) < deg(h_i g_i) < \delta} h_i g_i + \sum_{deg(h_i g_i) \leq deg(f)} h_i g_i \end{aligned}$$

Where the first sum must have degree $< \delta$ and the second sum subtracts $LT(h_i)$, thus has degree $< \delta$.

So, using the above Lemma 2, there exists a_{ij} such that

$$\begin{aligned} \sum_{deg(h_i g_i) = \delta} LT(h_i) g_i &= \sum_{i,j}^{d} a_{ij}\, S(LT(h_i)g_i, LT(h_j)g_j) \\ &= \sum_{i,j}^{d} a_{ij}\, (\frac{x^\delta}{LT(h_i g_i)} LT(h_i) g_i - \frac{x^\delta}{LT(h_j g_j)} LT(h_j) g_j\ ) \\ &= \sum_{i,j}^{d} a_{ij}\, (\frac{x^\delta}{LT(h_i) LT(g_i)} LT(h_i) g_i - \frac{x^\delta}{LT(h_j) LT(g_j)} LT(h_j) g_j\ ) \\ &= \sum_{i,j}^{d} a_{ij}\, (\frac{x^\delta}{x^{\alpha_{ij}}} \frac{x^{\alpha_{ij}} g_i}{LT(g_i)} - \frac{x^\delta}{\alpha_{ij}} \frac{x^{\alpha_{ij}} g_j}{LT(g_j)}\ ) \\ &= \sum_{i,j}^{d} \frac{x^\delta}{x^{\alpha_{ij}}}\, a_{ij}\, S(g_i, g_j) \end{aligned}$$

Where we use that $LT(LT(h_k g_k)) = LT(h_k g_k)$ and $LT(h_k g_k) = LT(h_k)LT(g_k)$ by well-ordering, and $x^{\alpha_{ij}} = \text{lcm}(LM(g_i)LM(g_j))$.

Now by assumption, $\overline{S(g_i, g_j)}^G = 0$, so $S(g_i, g_j) = \sum_{k=1}^{d} p_k g_k$ with $deg(p_k g_k) \leq deg(S(g_i, g_j)) < \alpha_{ij}$, where the first inequality follows from the division algorithm and the second since $S(g_i, g_j)$ cancels the leading term.

So, continuing we have,

$$\begin{aligned} \sum_{deg(h_i g_i) = \delta} LT(h_i) g_i &= \sum_{i,j}^{d} \frac{x^\delta}{x^{\alpha_{ij}}}\, a_{ij} \sum_{k=1}^{d} p_k g_k \\ &= \sum_{i,j}^{d} \sum_{k=1}^{d} \frac{x^\delta}{x^{\alpha_{ij}}} p_k g_k \end{aligned}$$

With degree strictly less than δ.

This concludes case 2 and the reverse direction.

($\Rightarrow$:) We need to show that $\overline{S(g_i, g_j)}^G = 0 \, \forall \, g_i, g_j \in G$ under the assumption that $G = \{g_1, ..., g_d\}$ is Gröbner.

$$S(g_i, g_j) = \frac{x^\gamma}{LT(g_i)} \cdot g_i - \frac{x^\gamma}{LT(g_j)} \cdot g_j \in I$$
$$\Rightarrow LT(S(g_i, g_j)) \in \langle LT(I) \rangle = \langle LT(g_i), ..., LT(g_d) \rangle$$

So we can move to next step of division algorithm without remainder by dividing by some $LT(g_k)$ (by Lemma 1, since $LT(S(g_i, g_j))$ is a monomial in a monomial generated ideal).

The next step is dividing $S(g_i, g_j) - (\frac{LT(S(g_i,g_j))}{LT(g_k)} \cdot g_k) \in I$ by G. By same reasoning as above, we can move to the next step.

The division algorithm terminates by well-ordering, thus we conclude that

$$\overline{S(g_i, g_j)}^G = 0.$$

This concludes the proof.

□

This suggests an algorithm (Buchberger's Algorithm) to construct a Gröbner basis from an original generating set G by adding $\overline{S(g_i, g_j)}^G \neq 0$ to G, and repeating the process with this newly defined G until $\overline{S(g_i, g_j)}^G = 0 \quad \forall \, i, j \in \{1, ..., n\}$.

Proposition 2. The Buchberger Algorithm terminates.

Proof. Let $G = \{g_1, ...g_d\}$ be a potential Gröbner basis. If $\overline{S(g_i, g_j)}^G \neq 0$, let $G' = G \cup \{\overline{S(g_i, g_j)}^G\}$. We note that

$$S(g_i, g_j) = \sum_{i=1}^{d} p_i g_i + \overline{S(g_i, g_j)}^G \Rightarrow \overline{S(g_i, g_j)}^G \in I.$$

So $G \subsetneq G'$, and we also have that $\langle LT(G) \rangle \subsetneq \langle LT(G') \rangle$ otherwise $\overline{S(g_i, g_j)}^G$ would not be the remainder. Suppose that the algorithm never terminates. But this would imply that

$$\langle LT(G) \rangle \subsetneq \langle LT(G') \rangle \subsetneq \langle LT(G'') \rangle \subsetneq ...$$

which contradicts that $K[x_1, ..., x_n]$ is Notherian.

Thus, the Buchberger Algorithm terminates.

□

Corollary 1. A Gröbner basis always exists.

Proof. Directly follows from Theorem 1 and Proposition 2.

$\square$

We provide a working example of the construction of a Gröbner basis using *grlex* ordering.

Example. Let $G_1 = \{x^3 - 2xy, x^2y - 2y^2 + x\}$, $f_1 := x^3 - 2xy$, $f_2 := x^2y - 2y^2 + x$, our potential Gröbner basis. We test this hypothesis:

$S(f_1, f_2) = y \cdot (x^3 - 2xy) - x \cdot (x^2y - 2y^2 + x) = -x^2 := f_3$
$\overline{S(f_1, f_2)}^{G_1} = f_3 \neq 0$ (we omit this division calculation since the remainder occurs immediately)

Let $G_2 = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2\}$
$\overline{S(f_1, f_2)}^{G_2} = 0$ (due to above)
$S(f_1, f_3) = (x^3 - 2xy) - (-x) \cdot (-x^2) = -2xy := f_4$
$\overline{S(f_1, f_3)}^{G_2} = f_4 \neq 0$ (we omit this division calculation since the remainder occurs immediately)

Let $G_3 = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy\}$
$\overline{S(f_1, f_2)}^{G_3} = 0$ (as before)
$\overline{S(f_1, f_3)}^{G_3} = 0$ (due to above)
$S(f_1, f_4) = y \cdot (x^3 - 2xy) - (-\frac{1}{2}x^2) \cdot (-2xy) = -2xy^2$
$\overline{S(f_1, f_4)}^{G_3} = 0$ (we omit this division calculation since it is only one step)
$S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x := f_5$
$\overline{S(f_2, f_3)}^{G_3} = f_5 \neq 0$ (we omit this division calculation since the remainder occurs immediately)

Let $G_4 = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$
$\overline{S(f_1, f_2)}^{G_4} = \overline{S(f_1, f_3)}^{G_4} = \overline{S(f_1, f_4)}^{G_4} = 0$ as before.
By adding f_5 we have $\overline{S(f_2, f_3)}^{G_4} = 0$.
It remains to check that
$\overline{S(f_1, f_5)}^{G_4}, \overline{S(f_2, f_4)}^{G_4}, \overline{S(f_2, f_5)}^{G_4}, \overline{S(f_3, f_4)}^{G_4}, \overline{S(f_3, f_5)}^{G_4}, \overline{S(f_4, f_5)}^{G_4} = 0$.
Note that we do not need to check $S(f_2, f_1)$ etc. since $S(f_i, f_j) = -S(f_j, f_i)$, $1 \leq i < j \leq 5$, and -1 clearly does not affect divisibility as a unit.

$S(f_1, f_5) = y^2 \cdot (x^3 - 2xy) - (-\frac{1}{2}x^3) \cdot (-2y^2 + x) = -2xy + \frac{1}{2}x^4$
We now compute $\overline{S(f_1, f_5)}^{G_4}$:

$$
\begin{array}{r}
q_1=\tfrac{1}{2}x \\
q_2=-1 \\
q_3=0 \\
q_4=1 \\
q_5=1 \\
\begin{smallmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{smallmatrix}
\big)\overline{\; -2xy + \tfrac{1}{2}x^4} \\
\underline{-\quad (-2xy)\qquad} \\
\tfrac{1}{2}x^4 \\
\underline{-\quad (\tfrac{1}{2}x^4 - x^2y)} \\
-x^2y \\
\underline{-\quad (-x^2y + 2y^2 - x)} \\
-2y^2 + x \\
\underline{-\quad (-2y^2 + x)} \\
0
\end{array}
$$

Note that this is not the only way to solve $\overline{S(f_1, f_5)}^{G_4}$. Since we are free to choose the order of divisors to compute the remainder, we see that we also get 0 remainder for

$$
\begin{array}{r}
q_4=1 \\
q_3=-\tfrac{1}{2}x^2 \\
\cdots \\
\begin{smallmatrix} f_4 \\ f_3 \\ \cdots \end{smallmatrix}
\big)\overline{\; -2xy + \tfrac{1}{2}x^4} \\
\underline{-\quad (-2xy)\qquad} \\
\tfrac{1}{2}x^4 \\
\underline{-\quad (\tfrac{1}{2}x^4)} \\
0
\end{array}
$$

Similarly, one can show the remaining $\overline{S(f_i, f_j)}^{G_4} = 0$, so we conclude that G_4 is a Gröbner basis for $\langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$ with respect to *grlex*.

5 Minimal and Reduced Gröbner Basis

We briefly state and discuss the concept of a minimal and reduced Gröbner basis.

<u>Definition 11.</u> A *minimal Gröbner basis* is one such that all leading coefficients equal 1, and for any g_i such that $LT(g_i)$ is in $\langle LT(G\backslash\{g_i\})\rangle$, g_i is removed. $G\backslash\{g_i\}$ is still a Gröbner basis since $\langle LT(G)\rangle = \langle LT(G\backslash\{g_i\})\rangle$.

An ideal I does not have a unique minimal Gröbner basis, although given a minimal Gröbner basis G, $\langle LT(G)\rangle$ forms the unique minimal basis of $\langle LT(I)\rangle$ (cf. [1]).

However, for $I \neq \{0\}$, I does have a unique *reduced* Gröbner basis for a given monomial ordering (cf. [1]):

Definition 12. A *reduced Gröbner basis* G is one such that all leading coefficients equal 1, and for any g_i in G, no monomial of g_i is an element of $\langle LT(G \backslash \{g_i\} \rangle$.

6 The Ideal Membership Problem

How does the existence of a Gröbner basis solve the classical Ideal Membership problem introduced in 2?

Proposition 3. As usual, let $I \lhd K[x_1, ..., x_n]$ and $f \in K[x_1, ..., x_n]$. The remainder of f after dividing by Gröbner basis $G = \{g_1, ..., g_d\}$ of I yields 0 if and only if $f \in I$.

Proof. ($\Rightarrow$:) Remainder 0 gives $f = p_1 g_1 + ... + p_d g_d$ for p_i in $K[x_1, ..., x_n]$ and g_i in G, so f is an element of I as written as a linear combination of elements of G.

($\Leftarrow$:) f being an element of I gives that $LT(f)$ is in $\langle LT(g_1), ..., LT(g_d) \rangle$. So, as in the proof of the Buchberger algorithm terminating, we can continue at each step of division and thus are left with remainder 0. □

7 Acknowledgements

I would like to extend a big thank you to Hugues Bellemare for his guidance and support throughout the DRP project this semester.

References

[1] Cox, David, Little, John, and O'Shea, Donal. *Ideals, Varieties, and Algorithms an Introduction to Algebraic Geometry and Commutative Algebra.* Fourth edition, Berlin, Heidelberg, Springer, 1998.

[2] Dummit, David, and Foote, Richard. *Abstract Algebra.* Third edition, John Wiley and Sons, Inc, 2004.

[3] "Gröbner basis". Wikipedia, The Free Encyclopedia, Wikimedia Foundation, 29 January 2023, `https://en.wikipedia.org/wiki/Gröbner_basis`.