

5 Gröbner bases

A symmetric function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ is a function satisfying $f(X, Y) = f(Y, X)$ for every $(X, Y) \in \mathbb{R}^2$. Simple examples of symmetric functions are $s_1(X, Y) = X + Y$ and $s_2(X, Y) = XY$. Polynomials in X and Y are functions built from addition and multiplication of the variables X and Y , such as $f(X, Y) = X^5Y + X + Y$. The polynomial $f(X, Y) = X^2 + Y^2$ is an example of a polynomial that is a symmetric function. We call it a symmetric polynomial. A special case of a classical result due to Newton (1643–1727) says that every symmetric polynomial is a polynomial in s_1 and s_2 . For example,

$$X^2 + Y^2 = (X + Y)^2 - 2XY = s_1^2 - 2s_2$$

and

$$X^3 + Y^3 = (X + Y)^3 - 3(X + Y)XY = s_1^3 - 3s_1s_2.$$

You may want to continue the list with $X^4 + Y^4$ or to wait until you have digested the rudiments of the theory of Gröbner bases and can understand “Newton revisited” (Section 5.5). In this chapter we will develop the theory of Gröbner bases in polynomial rings in several variables. The original impetus for this recent development of algebra was the desire to solve equations. Systems of linear equations such as

$$\begin{aligned} 5x + y + z &= 17, \\ x + y - z &= 1, \\ x + y + z &= 9 \end{aligned}$$

can be solved using Gaussian elimination. However, many problems lead to systems of non-linear equations, such as

$$\begin{aligned} y^2 - x^3 + x &= 0, \\ y^3 - x^2 &= 0, \end{aligned}$$

where the variables occur with powers greater than 1. The theory of Gröbner bases is a far-reaching generalization of Gaussian elimination. It can be applied for solving systems of non-linear (polynomial) equations such as above. Gröbner bases were invented independently by Buchberger (1942–) and Hironaka (1931–) in the sixties. Hironaka used the term “standard bases” in connection with his work on resolution of singularities in algebraic geometry (1964). Buchberger used the term Gröbner bases in his Ph.D. thesis (1966), in honor of his advisor W. Gröbner (1899–1980). In accordance with most modern mathematical literature we will use this term. Gröbner bases have some remarkable (mathematical) properties and turn out to be useful also in areas not confined to the world of mathematics, for example in optimization, robotics and theoretical computer science.

5.1 Polynomials in several variables

So far we have only encountered and defined polynomials in one variable. We need to define formally polynomials in more than one variable. Fortunately it is very easy to modify our formal construction of polynomials in one variable. Recall that the ring of polynomials $R[X]$ with coefficients in a (commutative) ring R was defined as

$$R[X] = R[\mathbb{N}] = \{f : \mathbb{N} \rightarrow R \mid f(n) = 0, n \gg 0\}$$

with obvious addition and not so obvious multiplication (see Section 4.1). A polynomial $f \in R[X]$ in one variable can be expressed in the usual notation as

$$f = a_n X^n + \cdots + a_1 X + a_0, \quad a_i \in R,$$

and addition and multiplication coincide with well known operations (but with coefficients in an arbitrary ring). Polynomials in several variables should correspond to algebraic expressions like $X^2 + XY + Y + Y^3 + X^5$ (in the case of two variables X and Y). We define the polynomial ring $R[X_1, \dots, X_n]$ in n variables X_1, \dots, X_n as

$$R[X_1, \dots, X_n] = R[\mathbb{N}^n] = \{f : \mathbb{N}^n \rightarrow R \mid f(v) = 0, |v| \gg 0\},$$

where $v = (v_1, \dots, v_n) \in \mathbb{N}^n$ and $|v| = v_1 + \cdots + v_n$. A polynomial $f \in R[X_1, \dots, X_n]$ is the same as a function $f : \mathbb{N}^n \rightarrow R$ that is non-zero for only

finitely many $v \in \mathbb{N}^n$. We let $X^v \in R[\mathbb{N}^n]$ denote the function given by

$$X^v(w) = \begin{cases} 1 & \text{if } v = w, \\ 0 & \text{if } v \neq w. \end{cases}$$

With this notation, every polynomial $f \in R[\mathbb{N}^n]$ can be written as a (finite) sum

$$f = \sum_{v \in \mathbb{N}^n} a_v X^v,$$

where $a_v \in R$ (an element $r \in R$ is identified with the function mapping the zero vector to r and everything else to $0 \in R$). If $f, g \in R[\mathbb{N}^n]$ we define $f + g$ by $(f + g)(v) = f(v) + g(v)$ and fg by the (finite) sum

$$(fg)(v) = \sum_{v_1 + v_2 = v} f(v_1)g(v_2),$$

where $v_1, v_2 \in \mathbb{N}^n$. The complete proof that $R[\mathbb{N}^n]$ is a ring with these compositions is left to the reader (see Exercise 5.1), as it is very similar to the one-variable case. We note that $0 \in R$ is the neutral element for $+$ and that the function $X^{(0,0,\dots,0)}$, mapping the zero vector in \mathbb{N}^n to $1 \in R$ and everything else to 0 , is the neutral element for multiplication. In the notation $R[X_1, \dots, X_n]$ for $R[\mathbb{N}^n]$, X_1 refers to $X^{(1,0,\dots,0)}$, X_2 to $X^{(0,1,0,\dots,0)}$, \dots and X_n to $X^{(0,\dots,0,1)}$.

A *term* is a polynomial $rX^v \in R[\mathbb{N}^n]$, where $r \in R \setminus \{0\}$ is called the *coefficient*.

Example 5.1.1 The formal definition of polynomials in several variables is a precise mathematical model for polynomial expressions in variables X, Y, Z, \dots . Be sure that you understand how to go from the formal expressions to the “real-world” expressions in X, Y, Z, \dots and back. As an example, let

$$f = 2X^{(0,0,0)} + 2X^{(1,0,3)} + X^{(2,1,0)} - X^{(0,1,1)} + 3X^{(1,1,1)} \in \mathbb{Z}[\mathbb{N}^3].$$

Translating X to $X^{(1,0,0)}$, Y to $X^{(0,1,0)}$ and Z to $X^{(0,0,1)}$ we get

$$f = 2 + 2XZ^3 + X^2Y - YZ + 3XYZ \in \mathbb{Z}[X, Y, Z]$$

as the corresponding polynomial expression in X, Y and Z . Multiplying polynomials in several variables corresponds to the natural way of multiplying and collecting terms, e.g.

$$\begin{aligned} (X + 2Y - Z)(X + Y - Z) &= X^2 + XY - XZ + 2XY + 2Y^2 - 2YZ \\ &\quad - XZ - YZ + Z^2 = X^2 + 3XY - 2XZ + 2Y^2 - 3YZ + Z^2. \end{aligned}$$

5.1.1 Term orderings

In one variable it is natural that a term like X^5 is bigger than X^3 . In more than one variable there is no obvious way of ordering the individual terms. In two variables, how should we compare terms like X^2Y and X^3 ? This is formalized in the notion of a term ordering. The price we pay for comparing terms in more than one variable is that there are infinitely many natural ways of doing it (see Remark 5.1.4). Before reading on, you should consult Appendix A for the definitions of a partial and a total ordering on a set.

Definition 5.1.2 The set \mathbb{N}^n of n -tuples of natural numbers carries a natural component-wise addition $+$ with zero vector $0 = (0, \dots, 0)$. A partial ordering \leq on \mathbb{N}^n is called a *term ordering* if

- (i) \leq is a total ordering,
- (ii) $0 \leq v$,
- (iii) $v_1 \leq v_2 \Rightarrow v_1 + v \leq v_2 + v$

for every $v, v_1, v_2 \in \mathbb{N}^n$.

Example 5.1.3 We will give a few examples of term orderings.

- (1) A term ordering on $\mathbb{N} = \mathbb{N}^1$ has to be the usual total ordering on \mathbb{N} (why?).
- (2) Define the *lexicographic ordering* \leq_{lex} on \mathbb{N}^n by

$$(v_1, \dots, v_n) \leq_{\text{lex}} (w_1, \dots, w_n)$$

if one of the following applies:

$$\begin{aligned} &(v_1 < w_1) \quad \text{or} \\ &(v_1 = w_1) \quad \text{and} \quad (v_2 < w_2) \quad \text{or} \\ &(v_1 = w_1) \quad \text{and} \quad (v_2 = w_2) \quad \text{and} \quad (v_3 < w_3) \quad \text{or} \dots \\ &(v_1 = w_1) \quad \text{and} \quad (v_2 = w_2) \quad \text{and} \quad \dots \quad \text{and} \quad (v_n = w_n). \end{aligned}$$

This is nothing but “alphabetic” ordering on tuples of natural numbers; for example, $(1, 2, 3) \geq_{\text{lex}} (1, 1, 3)$ since $2 > 1$ and $(4, 5, 1) \leq_{\text{lex}} (4, 5, 3)$ since $1 < 3$.

- (3) Let $|v| = v_1 + v_2 + \dots + v_n$, where $v = (v_1, \dots, v_n) \in \mathbb{N}^n$. Define the *graded lexicographic ordering* by $v \leq_{\text{grlex}} w$ if $|v| < |w|$ or $|v| = |w|$ and $v \leq_{\text{lex}} w$. Notice that, for example, $(1, 2, 3) \geq_{\text{grlex}} (2, 1, 1)$ (since $1 + 2 + 3 > 2 + 1 + 1$) but $(1, 2, 3) \leq_{\text{lex}} (2, 1, 1)$.

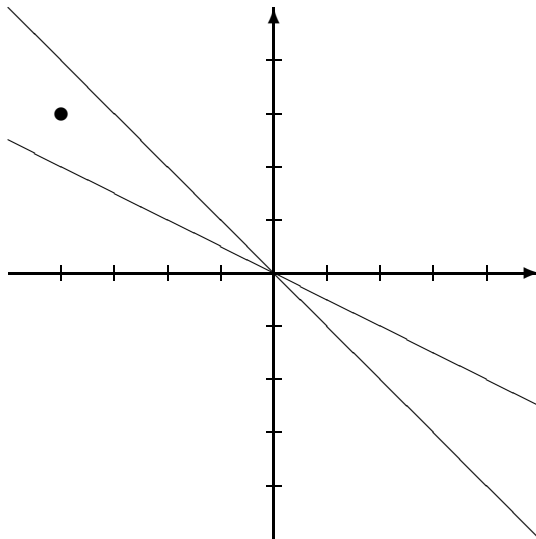
You should check immediately that \leq_{lex} and \leq_{grlex} are partial orderings and that they satisfy the three rules defining a term ordering (see Exercise 5.7).

A fruitful way of studying term orderings is through a little geometry. For a vector $v \in \mathbb{R}^n$ of real numbers ≥ 0 one can construct a term ordering \leq_v on \mathbb{N}^n defined as $u_1 \leq_v u_2$ if and only if

$$v \cdot u_1 < v \cdot u_2 \quad \text{or} \quad (v \cdot u_1 = v \cdot u_2 \text{ and } u_1 \leq_{\text{lex}} u_2), \quad (5.1)$$

where $u_1, u_2 \in \mathbb{N}^n$ and \cdot refers to the usual inner product on \mathbb{R}^n (see Exercise 5.8).

Remark 5.1.4 There is a fundamental difference between \mathbb{N} and \mathbb{N}^2 . On \mathbb{N} there is only one term ordering. On \mathbb{N}^2 there are infinitely many (in fact uncountably many). Let \leq_r denote the term ordering on \mathbb{N}^2 given by the vector $(1, r)$ as in (5.1), where r is a positive real number. If $s \neq r$ is another positive real number, we may find $v \in \mathbb{Z}^2$ such that $(1, r) \cdot v > 0$ and $(1, s) \cdot v < 0$. You can see this by drawing the lines through $(0, 0)$ orthogonal to $(1, r)$ and $(1, s)$. Any point with integer coordinates between the two diagonal lines will do.



A vector in \mathbb{Z}^2 can always be written as the difference of two vectors in \mathbb{N}^2 (e.g. $(1, -1) = (1, 0) - (0, 1)$, $(-1, -1) = (0, 0) - (1, 1)$ and $(1, 1) = (1, 1) - (0, 0)$). Write $v = v_1 - v_2$, where $v_1, v_2 \in \mathbb{N}^2$. Then $v_1 \geq_r v_2$ but $v_1 \leq_s v_2$. Thus for every positive real number r we have defined a term ordering \leq_r such

that if s is another positive real number then $\leq_r \neq \leq_s$. This shows that there are infinitely (uncountably) many term orderings on \mathbb{N}^2 .

For a given vector $v \in \mathbb{N}^n$ we let

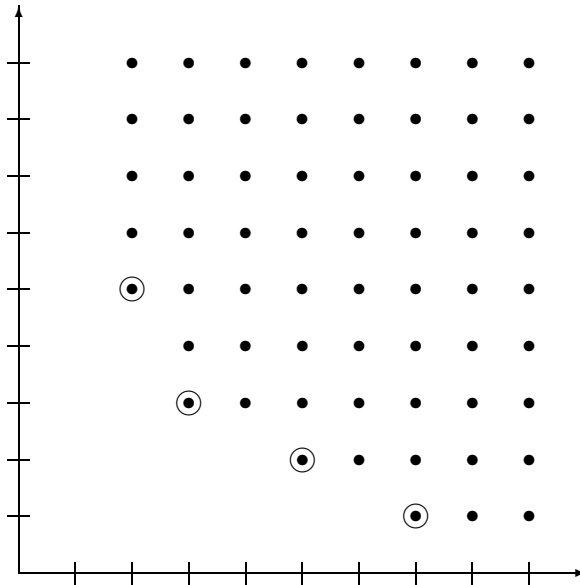
$$v + \mathbb{N}^n = \{v + w \mid w \in \mathbb{N}^n\}.$$

We will need the following crucial result, known as Dickson's lemma (L. E. Dickson (1874–1954)). It originally appeared in a paper on number theory ([7], Lemma A).

Lemma 5.1.5 (Dickson) *Let S be a subset of \mathbb{N}^n . Then there is a finite set of vectors $v_1, \dots, v_r \in S$ such that*

$$S \subseteq (v_1 + \mathbb{N}^n) \cup \dots \cup (v_r + \mathbb{N}^n).$$

Example 5.1.6 The idea of the proof is really quite simple and comes from the case of the subsets of \mathbb{N}^2 . In the figure below we show a certain infinite subset $S \subseteq \mathbb{N}^2$ (extended infinitely in the positive x - and y - directions).



The marked points are the interesting points for the subset S , in that

$$S \subseteq ((2, 5) + \mathbb{N}^2) \cup ((3, 3) + \mathbb{N}^2) \cup ((5, 2) + \mathbb{N}^2) \cup ((7, 1) + \mathbb{N}^2).$$

Proof of Lemma 5.1.5. The proof proceeds by induction on n . If $n = 1$ and $S \subseteq \mathbb{N}$ is a subset, we let s be the first element in S . Then $S \subseteq s + \mathbb{N}$. Suppose now for the induction step that $n > 1$ and we know that Lemma 5.1.5 is true for $m < n$. Let $\pi : \mathbb{N}^n \rightarrow \mathbb{N}^{n-1}$ denote the map given by

$$\pi(x_1, x_2, \dots, x_n) = (x_2, \dots, x_n).$$

Using the induction hypothesis on the subset

$$\pi(S) = \{\pi(s) \mid s \in S\} \subseteq \mathbb{N}^{n-1}$$

we get the existence of $s_1, \dots, s_r \in S$ such that

$$\pi(S) \subseteq (\pi(s_1) + \mathbb{N}^{n-1}) \cup \dots \cup (\pi(s_r) + \mathbb{N}^{n-1}).$$

It is in general not true that $S \subseteq (s_1 + \mathbb{N}^n) \cup \dots \cup (s_r + \mathbb{N}^n)$ (you can see this in Example 5.1.6). We need more vectors in S .

Let M be the largest number occurring as a first coordinate in our vectors s_1, \dots, s_r . Define

$$S_i = \{s \in S \mid \text{the first coordinate of } s = i\} \quad \text{for } 0 \leq i < M$$

and

$$S_{\geq M} = \{s \in S \mid \text{the first coordinate of } s \text{ is } \geq M\}.$$

Then $S = S_0 \cup \dots \cup S_{M-1} \cup S_{\geq M}$ and

$$S_{\geq M} \subseteq (s_1 + \mathbb{N}^n) \cup \dots \cup (s_r + \mathbb{N}^n).$$

Since the first coordinate of the vectors in S_i is fixed, we can identify S_i with a subset of \mathbb{N}^{n-1} and by induction find finitely many vectors $s_1^i, \dots, s_{r_i}^i \in S_i$ such that

$$S_i \subseteq (s_1^i + \mathbb{N}^n) \cup \dots \cup (s_{r_i}^i + \mathbb{N}^n).$$

Gathering up these finitely many vectors for S_0, \dots, S_{M-1} and throwing in the vectors s_1, \dots, s_r we get the result. \square

Make sure you understand how the proof of Lemma 5.1.5 works for the subset $S \subseteq \mathbb{N}^2$ in Example 5.1.6.

Corollary 5.1.7 *A term ordering \leq on \mathbb{N}^n is a well ordering.*

Proof. Let $S \subseteq \mathbb{N}^n$ be a non-empty subset. By Lemma 5.1.5 there are finitely many elements $v_1, \dots, v_r \in S$ such that

$$S \subseteq (v_1 + \mathbb{N}^n) \cup \dots \cup (v_r + \mathbb{N}^n).$$

If $v \in v_i + \mathbb{N}^n$ then $v = v_i + w$ for some $w \in \mathbb{N}^n$. This implies that $v - v_i \in \mathbb{N}^n$. Since $v - v_i \geq 0$ by Definition 5.1.2(ii), it follows that $v = (v - v_i) + v_i \geq v_i$ by Definition 5.1.2(iii). This means that the smallest element among v_1, \dots, v_r will be the smallest element in S , showing that \leq is a well ordering. \square

5.2 The initial term of a polynomial

Definition 5.2.1 Let

$$f = \sum_{v \in \mathbb{N}^n} a_v X^v$$

be a non-zero polynomial in $R[\mathbb{N}^n]$ and \leq a term order on \mathbb{N}^n . The initial term of f with respect to \leq is defined as

$$\text{in}_{\leq}(f) = a_w X^w,$$

where $w = \max_{\leq} \{v \in \mathbb{N}^n \mid a_v \neq 0\}$ (see Definition A.3.6 for the definition of \max_{\leq}). In an abuse of notation we will sometimes compare two terms and write $aX^u \leq bX^v$ if $u \leq v$.

Example 5.2.2 Let $f = X^2 + XY + Y + Y^3 + X^5 \in \mathbb{Z}[X, Y]$, where X corresponds to $X^{(1,0)}$ and Y to $X^{(0,1)}$ in $\mathbb{Z}[\mathbb{N}^2]$. This means that

$$f = X^{(2,0)} + X^{(1,1)} + X^{(0,1)} + X^{(0,3)} + X^{(5,0)} \in \mathbb{Z}[\mathbb{N}^2].$$

Putting $\leq = \leq_{\text{lex}}$ (Example 5.1.3), we obtain

$$(5, 0) \geq (2, 0) \geq (1, 1) \geq (0, 3) \geq (0, 1).$$

In the ordering \leq one should write $f = X^5 + X^2 + XY + Y^3 + Y$. The initial term of f is therefore $\text{in}_{\leq}(f) = X^5$.

Remark 5.2.3 Let R be a domain and f, g non-zero polynomials in $R[X_1, \dots, X_n]$. Then $\text{in}_{\leq}(fg) = \text{in}_{\leq}(f) \text{in}_{\leq}(g)$ (see Exercise 5.11). This formula is the analogue of $\deg(fg) = \deg(f) + \deg(g)$ in one variable (see Proposition 4.2.2),

5.3 The division algorithm

In several variables there is an analogue of division with remainder (Proposition 4.2.4). Now everything is with respect to a fixed term ordering (in the case of one variable, there is only one term ordering; in more than one variable there are infinitely many (Remark 5.1.4)). The proof of the following proposition is based on the division algorithm in several variables. This algorithm is very similar to the one-variable algorithm given in the proof of Proposition 4.2.4. In order not to separate the algorithm from its mathematical surroundings it is embedded in the proof. To learn the algorithm and prove its correctness you will have to read through the proof and immerse yourself in several examples and exercises. We will assume for the rest of this chapter that R is a domain.

Proposition 5.3.1 (The division algorithm) *Fix a term ordering \leq on \mathbb{N}^n . Let $f \in R[X_1, \dots, X_n] \setminus \{0\}$ and suppose that $f_1, \dots, f_m \in R[X_1, \dots, X_n]$ is a sequence of non-zero polynomials. Then there exist $a_1, \dots, a_m, r \in R[X_1, \dots, X_n]$ such that*

$$f = a_1 f_1 + \dots + a_m f_m + r$$

and either $r = 0$ or none of the terms in r is divisible by $\text{in}_{\leq}(f_1), \dots, \text{in}_{\leq}(f_m)$. Furthermore, $\text{in}_{\leq}(a_i f_i) \leq \text{in}_{\leq}(f)$ if $a_i f_i \neq 0$.

Proof. The proof is basically a correctness proof of the division algorithm for polynomials in several variables. This algorithm is similar to the algorithm in one variable as described in the proof of Proposition 4.2.4. You should compare the two. Here is the division algorithm in several variables. To begin put $a_1 := 0, \dots, a_m := 0, r := 0$ and $s := f$ giving

$$f = a_1 f_1 + \dots + a_m f_m + (r + s). \quad (5.2)$$

This expression will serve as an invariant throughout the algorithm. Proceed as follows in successive steps of the algorithm. If $s = 0$ we are done. If not, there are two cases. If $\text{in}_{\leq}(s)$ is divisible by some $\text{in}_{\leq}(f_i)$ then pick the *smallest* i with this property and let

$$\begin{aligned} s &:= s - \frac{\text{in}_{\leq}(s)}{\text{in}_{\leq}(f_i)} f_i, \\ a_i &:= a_i + \frac{\text{in}_{\leq}(s)}{\text{in}_{\leq}(f_i)}. \end{aligned} \quad (5.3)$$

Notice that (5.2) still holds after the assignments in (5.3) – we have simply subtracted and added the same thing. However, if $\text{in}_{\leq}(s)$ is not divisible by any

$\text{in}_{\leq}(f_i)$ we add the initial term to r and subtract it from s :

$$\begin{aligned} r &:= r + \text{in}_{\leq}(s), \\ s &:= s - \text{in}_{\leq}(s). \end{aligned} \tag{5.4}$$

Of course, after the assignments in (5.4) $r + s$ is unchanged and (5.2) still holds. If $s = 0$ we are done. If not, the initial term of s is strictly decreased after the assignment in (5.3), because $\text{in}_{\leq}(s) t \prec \text{in}_{\leq}(s) \text{in}_{\leq}(f_i)$ for a term t in f_i different from $\text{in}_{\leq}(f_i)$. The initial term of s is also strictly decreased after the assignment in (5.4). In this way the sequence formed by $\text{in}_{\leq}(s)$ in successive steps of the algorithm is strictly decreasing with respect to the term ordering \leq . Since \leq is a well ordering by Corollary 5.1.7, such a sequence must be finite (see Lemma A.3.8). Therefore the division algorithm eventually terminates with $s = 0$. Then (5.2) is the desired expression. We have seen that $\text{in}_{\leq}(s) \leq \text{in}_{\leq}(f)$ holds if $s \neq 0$, since s initially takes the value of f . Since $\text{in}_{\leq}((a_i + \text{in}_{\leq}(s)/\text{in}_{\leq}(f_i))f_i) = \text{in}_{\leq}(a_i \text{in}_{\leq}(f_i) + \text{in}_{\leq}(s)) \leq \max(\text{in}_{\leq}(a_i f_i), \text{in}_{\leq}(s))$ (see Exercise 5.12) for $a_i \neq 0$ we must have $\text{in}_{\leq}(a_i f_i) \leq \text{in}_{\leq}(f)$ after the assignment in (5.3). This proves that $\text{in}_{\leq}(a_i f_i) \leq \text{in}_{\leq}(f)$ if $a_i f_i \neq 0$ in (5.2) when reaching $s = 0$. \square

Definition 5.3.2 Suppose that $f \in R[X_1, \dots, X_n]$ and let $F = (f_1, \dots, f_m)$ be a sequence of non-zero polynomials in $R[X_1, \dots, X_n]$. We let f^F denote the remainder r coming from dividing f by F using the division algorithm.

Example 5.3.3 Let $\leq = \leq_{\text{lex}}$ with $Y \leq X$, $f = X^4 + Y^4$, $f_1 = X^2 + Y$ and $f_2 = X^2Y + 1$. The division algorithm is shown in the diagram below; we are trying to mimic the diagram for division of polynomials in one variable. Here, though, the result is represented by not just one polynomial but a set (a_1, a_2) of polynomials. The initial terms of f_1 , f_2 and s are underlined. If the initial term of s is not divisible by either $\text{in}_{\leq}(f_1)$ or $\text{in}_{\leq}(f_2)$ then we transfer the initial term to the remainder r . This is indicated, for example, as $Y^4 + Y^2 \rightarrow Y^4$.

$$\begin{array}{l} \underline{X^4} + Y^4 : (\underline{X^2} + Y, \underline{X^2Y} + 1) = (X^2 - Y, 0) \\ \underline{X^4} + \underline{X^2Y} \\ \quad \underline{-X^2Y} + Y^4 \\ \quad \underline{-X^2Y - Y^2} \\ \quad \quad \underline{Y^4} + Y^2 \longrightarrow Y^4 \\ \quad \quad \underline{Y^2} \longrightarrow Y^4 + Y^2 \\ \quad \quad \quad 0 \end{array}$$

The division algorithm above shows that

$$X^4 + Y^4 = (X^2 - Y)(X^2 + Y) + Y^4 + Y^2$$

and $(X^4 + Y^4)^{(X^2+Y, X^2Y+1)} = Y^4 + Y^2$. However, suppose that we switch f_1 and f_2 (so that we divide by (f_2, f_1) instead of (f_1, f_2)). Then

$$\begin{array}{r} \underline{X^4 + Y^4} : (\underline{X^2Y + 1}, \underline{X^2 + Y}) = (-1, X^2) \\ \underline{X^4 + X^2Y} \\ - X^2Y + Y^4 \\ \underline{-X^2Y - 1} \\ \underline{Y^4 + 1} \longrightarrow Y^4 \\ \underline{1} \longrightarrow Y^4 + 1 \\ 0 \end{array}$$

This shows that

$$X^4 + Y^4 = X^2(X^2 + Y) - (X^2Y + 1) + Y^4 + 1$$

and $(X^4 + Y^4)^{(X^2Y+1, X^2+Y)} = Y^4 + 1$.

5.4 Gröbner bases

In Example 5.3.3 we saw that the remainder coming from the division algorithm depends on the order of f_1, \dots, f_m in Proposition 5.3.1. We would like to have a generating set of an ideal with the property that the remainder coming from the division algorithm is independent of the order of its elements. This is possible. Such a set of generators is called a Gröbner basis. In the rest of this chapter we will assume that R is a field denoted by k , in order to simplify the definition of a Gröbner basis (the definition for arbitrary domains is a little more complicated).

Definition 5.4.1 A set of non-zero polynomials

$$F = (f_1, \dots, f_m) \subseteq k[X_1, \dots, X_n]$$

is called a *Gröbner basis for an ideal I* in $k[X_1, \dots, X_n]$ with respect to a term ordering \leq if $F \subseteq I$ and, for every $f \in I \setminus \{0\}$,

$$\text{in}_{\leq}(f_i) \mid \text{in}_{\leq}(f)$$

for some $i = 1, \dots, m$. The set F is called a *Gröbner basis* with respect to a term ordering \leq if it is a Gröbner basis for the ideal $\langle f_1, \dots, f_m \rangle$ with respect to \leq .

This definition may seem strange at first. But it is exactly to the point. As a motivating example consider the ideal $I = \langle X^2 + Y, X^2Y + 1 \rangle$ in the polynomial ring $\mathbb{Q}[X, Y]$. Recall that I consists of all the polynomials you get as “linear” combinations (see subsection 3.1.1) of $X^2 + Y$ and $X^2Y + 1$:

$$I = \{a(X, Y)(X^2 + Y) + b(X, Y)(X^2Y + 1) \mid a(X, Y), b(X, Y) \in \mathbb{Q}[X, Y]\}.$$

Thus $f = X^3 - Y + XY - X^2Y^2 \in I$ since $f = X(X^2 + Y) - Y(X^2Y + 1)$. In general, how do we decide whether a given polynomial lies in the ideal I ? Here Gröbner bases and the division algorithm are very helpful.

Proposition 5.4.2 *Let $G = (f_1, \dots, f_m)$ be a Gröbner basis with respect to a term ordering \leq . For a polynomial $f \in k[X_1, \dots, X_n]$ we have*

$$f \in I \iff f^G = 0,$$

where $I = \langle f_1, \dots, f_m \rangle$.

Proof. If $f^G = 0$ then $f = a_1f_1 + \dots + a_mf_m$ and $f \in I = \langle f_1, \dots, f_m \rangle$. Let $f = a_1f_1 + \dots + a_mf_m + f^G$ be the output from the division algorithm. Taking $r = f^G$ this gives an expression for f as in Proposition 5.3.1. Clearly

$$r = f - a_1f_1 - \dots - a_mf_m \in I.$$

If $r \neq 0$ then there is some $\text{in}_{\leq}(f_i)$ dividing $\text{in}_{\leq}(r)$, since (f_1, \dots, f_m) was assumed to be a Gröbner basis for I . This contradicts that r is the remainder coming from division by G . Thus $r = 0$. \square

Example 5.4.3 Let $F = (X^2 + Y, X^2Y + 1)$ and fix the lexicographic ordering \leq on terms in $k[X, Y]$ given by $X \geq Y$. Then

$$Y^2 - 1 = Y(X^2 + Y) - (X^2Y + 1)$$

so that $Y^2 - 1 \in \langle X^2 + Y, X^2Y + 1 \rangle$. But the remainder from the division algorithm is $(Y^2 - 1)^F = Y^2 - 1$. Using Proposition 5.4.2 we see that F is not a Gröbner basis for $\langle X^2 + Y, X^2Y + 1 \rangle$. Of course this could also be checked by using the definition of a Gröbner basis. It is not too difficult to show that F is not a Gröbner basis for any term ordering (see Exercise 5.14).

Example 5.4.4 A generator (f) for a principal ideal $I \subseteq R = k[X_1, \dots, X_n]$ is always a Gröbner basis for I . Consider a polynomial $g \in I$. Since f generates I we may find $a \in R$ such that $g = af$. Therefore $\text{in}_{\leq}(g) = \text{in}_{\leq}(a) \text{in}_{\leq}(f)$ by Remark 5.2.3 and $\text{in}_{\leq}(f)$ divides $\text{in}_{\leq}(g)$.

Corollary 5.4.5 Let $G = (f_1, \dots, f_m) \subseteq R = k[X_1, \dots, X_n]$ be a Gröbner basis for the ideal $I \subseteq R$ with respect to some term ordering. Then $I = \langle f_1, \dots, f_m \rangle$.

Proof. Since $f_1, \dots, f_m \in I$ we obtain $\langle f_1, \dots, f_m \rangle \subseteq I$. However, if $f \in I$ then $f^G = 0$ by Proposition 5.4.2 and $f = a_1 f_1 + \dots + a_m f_m$ for suitable $a_1, \dots, a_m \in k[X_1, \dots, X_n]$ by the division algorithm. This proves that $I \subseteq \langle f_1, \dots, f_m \rangle$. \square

Proposition 5.4.6 Let $G = (f_1, \dots, f_m)$ be a Gröbner basis in $R = k[X_1, \dots, X_n]$ with respect to a term ordering \leq . Then the remainder r in $f = a_1 f_1 + \dots + a_m f_m + r$ as in Proposition 5.3.1 is unique for every $f \in R$. The remainder from the division algorithm is independent of the order of the elements f_1, \dots, f_m in G .

Proof. Let $f \in R$ and assume we have two expressions $f = a_1 f_1 + \dots + a_m f_m + r_1 = a'_1 f_1 + \dots + a'_m f_m + r_2$, as in Proposition 5.3.1. Then

$$r_2 - r_1 = (a_1 - a'_1)f_1 + \dots + (a_m - a'_m)f_m.$$

Therefore $r_2 - r_1 \in \langle f_1, \dots, f_m \rangle$. If $r_2 - r_1 \neq 0$ then there exists i such that $\text{in}_{\leq}(f_i)$ divides $\text{in}_{\leq}(r_2 - r_1)$. This implies that $\text{in}_{\leq}(f_i)$ divides a term in r_2 or r_1 , which is a contradiction.

A permutation G' of the elements in G leads to an expression $f = b_1 f_1 + \dots + b_m f_m + f^{G'}$, as in Proposition 5.3.1. This implies that $f^{G'} = f^G$, since we have just proved that the remainder in Proposition 5.3.1 is unique. \square

5.4.1 Hilbert's basis theorem

We will prove the existence of Gröbner bases for every ideal in $k[X_1, \dots, X_n]$. In the late nineteenth century the German mathematician David Hilbert (1862–1943) surprised the mathematical community by showing that every ideal in a polynomial ring $k[X_1, \dots, X_n]$ is finitely generated [13]. This is now referred to as Hilbert's basis theorem. His proof did not give explicit generators and

his contemporaries were skeptical. Here is the fascinating history from the MacTutor History of Mathematics Archive.¹

Hilbert's first work was on invariant theory and, in 1888, he proved his famous Basis Theorem. Twenty years earlier Gordan had proved the finite basis theorem for binary forms using a highly computational approach. Attempts to generalise Gordan's work to systems with more than two variables failed since the computational difficulties were too great. Hilbert himself tried at first to follow Gordan's approach but soon realised that a new line of attack was necessary. He discovered a completely new approach which proved the finite basis theorem for any number of variables but in an entirely abstract way. Although he proved that a finite basis existed his methods did not construct such a basis. Hilbert submitted a paper proving the finite basis theorem to *Mathematische Annalen*. However, Gordan was the expert on invariant theory for *Mathematische Annalen* and he found Hilbert's revolutionary approach difficult to appreciate. He refereed the paper and sent his comments to Klein:

The problem lies not with the form ... but rather much deeper. Hilbert has scorned to present his thoughts following formal rules, he thinks it suffices that no one contradict his proof ... he is content to think that the importance and correctness of his propositions suffice. ... for a comprehensive work for the *Annalen* this is insufficient.

However, Hilbert had learnt through his friend Hurwitz about Gordan's letter to Klein and Hilbert wrote himself to Klein in forceful terms:

... I am not prepared to alter or delete anything, and regarding this paper, I say with all modesty, that this is my last word so long as no definite and irrefutable objection against my reasoning is raised.

Using the machinery of Gröbner bases, Hilbert's result follows in a remarkable way. In fact reading through the proof one tends to forget the controversies of the late nineteenth century.

Theorem 5.4.7 *Let k be a field, \leq a term ordering and $I \subseteq k[X_1, \dots, X_n]$ an ideal. Then I has a Gröbner basis with respect to \leq .*

Proof. Let $S = \{v \in \mathbb{N}^n \mid X^v = \text{in}_{\leq}(f) \text{ for some } f \in I\} \subseteq \mathbb{N}^n$. Dickson's lemma (Lemma 5.1.5) applied to the subset S of \mathbb{N}^n shows that there are finitely many $f_1, \dots, f_m \in I$ such that

$$S \subseteq (v_1 + \mathbb{N}^n) \cup \dots \cup (v_m + \mathbb{N}^n),$$

where $X^{v_i} = \text{in}_{\leq}(f_i)$ for $i = 1, \dots, m$. Suppose that $aX^w = \text{in}_{\leq}(f)$, where $f \in I$. Then $w = v_j + v$ for a suitable $j = 1, \dots, m$ and $v \in \mathbb{N}^n$. This proves that $X^w = X^{v_j} X^v$ and therefore that $\text{in}_{\leq}(f_j) \mid \text{in}_{\leq}(f)$. This is exactly the statement that (f_1, \dots, f_m) is a Gröbner basis for I . \square

¹ <http://www-groups.dcs.st-and.ac.uk/history>

Corollary 5.4.8 (Hilbert) *Let I be an arbitrary ideal in $k[X_1, \dots, X_n]$. Then there are finitely many polynomials $f_1, \dots, f_m \in I$ such that every polynomial $f \in I$ can be written*

$$f = a_1 f_1 + \dots + a_m f_m$$

for suitable $a_1, \dots, a_m \in k[X_1, \dots, X_n]$ ($I = \langle f_1, \dots, f_m \rangle$).

Proof. This follows from Theorem 5.4.7 and Corollary 5.4.5. □

5.5 Newton revisited

Let us return to the question in the introduction to this chapter. Is there a systematic way of writing $X^4 + Y^4$ as a polynomial in $X + Y$ and XY ? The answer is yes, and it is a nice consequence of the theory of Gröbner bases. In a more general setting we let $f, f_1, \dots, f_r \in k[X_1, \dots, X_n]$. We wish to decide whether the polynomial f can be written as $P(f_1, \dots, f_r)$, where $P \in k[T_1, \dots, T_r]$, and find P if this is the case. Consider the polynomial ring $A = k[X_1, \dots, X_n, T_1, \dots, T_r]$. If we can write

$$f = a_1(T_1 - f_1) + \dots + a_r(T_r - f_r) + h, \quad (5.5)$$

where $h \in k[T_1, \dots, T_r]$ and $a_1, \dots, a_r \in A$, then we may put $T_i = f_i$ so that $f = h(f_1, \dots, f_r)$ and we can take $P = h$. Let $I \subseteq A$ be the ideal $\langle T_1 - f_1, \dots, T_r - f_r \rangle$. If $f = P(f_1, \dots, f_r)$, where $P \in k[T_1, \dots, T_r]$, then (see Exercise 5.17)

$$f(X_1, \dots, X_n) - P(T_1, \dots, T_r) \in I. \quad (5.6)$$

Therefore

$$f = a_1(T_1 - f_1) + \dots + a_r(T_r - f_r) + P$$

for suitable $a_1, \dots, a_r \in A$. How do we find the polynomial P ? This is where the theory of Gröbner bases comes in handy. It gives the following surprising result.

Theorem 5.5.1 *Let $f, f_1, \dots, f_r \in k[X_1, \dots, X_n]$. Let I be the ideal*

$$I = \langle T_1 - f_1, \dots, T_r - f_r \rangle$$

in the polynomial ring $A = k[X_1, \dots, X_n, T_1, \dots, T_r]$ and \leq the lexicographic ordering given by

$$X_1 \geq \dots \geq X_n \geq T_1 \geq \dots \geq T_r.$$

Let G be a Gröbner basis of I with respect to \leq . Then f can be written as a polynomial in f_1, \dots, f_r if and only if

$$f^G \in k[T_1, \dots, T_r].$$

In this case $f = f^G(f_1, \dots, f_r)$.

Proof. Let $G = (g_1, \dots, g_N)$ be a Gröbner basis for I with respect to \leq . Then the division algorithm gives

$$f = a'_1 g_1 + \dots + a'_N g_N + f^G$$

for $a'_1, \dots, a'_N \in A$. Since $\langle g_1, \dots, g_N \rangle = I$, we can find $a_1, \dots, a_r \in A$ such that

$$f = a_1(T_1 - f_1) + \dots + a_r(T_r - f_r) + f^G.$$

If $f^G \in k[T_1, \dots, T_r]$ then it follows that $f = f^G(f_1, \dots, f_r)$ by (5.5).

If, however, there is a polynomial $P \in k[T_1, \dots, T_r]$ such that $f = P(f_1, \dots, f_r)$ then

$$f = a_1(T_1 - f_1) + \dots + a_r(T_r - f_r) + P, \quad (5.7)$$

where $a_1, \dots, a_r \in A$, by (5.6). We will prove that $f^G \in k[T_1, \dots, T_r]$ in this case. This is done by running through the division algorithm with f and the Gröbner basis G . We may rewrite (5.7) as

$$f = b_1 g_1 + \dots + b_N g_N + P$$

for suitable $b_1, \dots, b_N \in A$. Notice that the invariant expression (5.2) of the division algorithm (Proposition 5.3.1) is satisfied by $s = P$ and $r = 0$ (using b_1, \dots, b_N as values for the coefficients of g_1, \dots, g_N). If $\text{in}_{\leq}(g_j)$ divides the $\text{in}_{\leq}(s)$ entering (5.3) of the division algorithm (see the proof of Proposition 5.3.1), then $\text{in}_{\leq}(g_j) \leq \text{in}_{\leq}(s)$. This implies that $\text{in}_{\leq}(g_j) \in k[T_1, \dots, T_r]$. Therefore $g_j \in k[T_1, \dots, T_r]$ if $s \in k[T_1, \dots, T_r]$. Here it is important that the term ordering is lexicographic with $X_1 \geq \dots \geq X_n \geq T_1 \geq \dots \geq T_r$. So the assignment in (5.3) satisfies $s - (\text{in}_{\leq}(s)/\text{in}_{\leq}(g_j))g_j \in k[T_1, \dots, T_r]$. Since we are

$$\begin{array}{l}
\underline{X^4 + Y^4} \quad : \quad (\underline{-X - Y + T_1}, \underline{Y^2 - YT_1 + T_2}) \\
\underline{X^4 + X^3Y - X^3T_1} \\
\underline{-X^3Y + X^3T_1 + Y^4} \\
\underline{-X^3Y - X^2Y^2 + X^2YT_1} \\
\underline{X^3T_1 + X^2Y^2 - X^2YT_1 + Y^4} \\
\underline{X^3T_1 + X^2YT_1 - X^2T_1^2} \\
\underline{X^2Y^2 - 2X^2YT_1 + X^2T_1^2 + Y^4} \\
\underline{X^2Y^2 + XY^3 - XY^2T_1} \\
\underline{-2X^2YT_1 + X^2T_1^2 - XY^3 + XY^2T_1 + Y_4} \\
\underline{-2X^2YT_1 - 2XY^2T_1 + 2XYT_1^2} \\
\underline{X^2T_1^2 - XY^3 + 3XY^2T_1 - 2XYT_1^2 + Y^4} \\
\underline{X^2T_1^2 + XYT_1^2 - XT_1^3} \\
\underline{-XY^3 + 3XY^2T_1 - 3XYT_1^2 + XT_1^3 + Y^4} \\
\underline{-XY^3 - Y^4 + Y^3T_1} \\
\underline{3XY^2T_1 - 3XYT_1^2 + XT_1^3 + 2Y^4 - Y^3T_1} \\
\underline{3XY^2T_1 + 3Y^3T_1 - 3Y^2T_1^2} \\
\underline{-3XYT_1^2 + XT_1^3 + 2Y^4 - 4Y^3T_1 + 3Y^2T_1^2} \\
\underline{-3XYT_1^2 - 3Y^2T_1^2 + 3YT_1^3} \\
\underline{XT_1^3 + 2Y^4 - 4Y^3T_1 + 6Y^2T_1^2 - 3YT_1^3} \\
\underline{XT_1^3 + YT_1^3 - T_1^4} \\
\underline{2Y^4 - 4Y^3T_1 + 6Y^2T_1^2 - 4YT_1^3 + T_1^4} \\
\underline{2Y^4 - 2Y^3T_1 + 2Y^2T_2} \\
\underline{-2Y^3T_1 + 6Y^2T_1^2 - 2Y^2T_2 - 4YT_1^3 + T_1^4} \\
\underline{-2Y^3T_1 + 2Y^2T_1^2 - 2YT_1T_2} \\
\underline{4Y^2T_1^2 - 2Y^2T_2 - 4YT_1^3 + 2YT_1T_2 + T_1^4} \\
\underline{4Y^2T_1^2 - 4YT_1^3 + 4T_1^2T_2} \\
\underline{-2Y^2T_2 + 2YT_1T_2 + T_1^4 - 4T_1^2T_2} \\
\underline{-2Y^2T_2 + 2YT_1T_2 - 2T_2^2} \\
\underline{T_1^4 - 4T_1^2T_2 + 2T_2^2}
\end{array}$$

Figure 5.1

moving terms from s to the remainder, in the division algorithm in (5.4), we will eventually end up with a remainder f^G in $k[T_1, \dots, T_r]$. \square

Example 5.5.2 Let us return to the problem of writing $X^4 + Y^4$ as a polynomial in $X + Y$ and XY . Using Theorem 5.5.1 to address this we must find a Gröbner basis of $I = \langle T_1 - X - Y, T_2 - XY \rangle$ with respect to the lexicographic ordering \leq given by $X \geq Y \geq T_1 \geq T_2$. You will see in the next section how to compute a Gröbner basis using Buchberger's algorithm. Let me reveal that a Gröbner basis for I with respect to \leq is $G = (T_1 - X - Y, T_2 - T_1Y + Y^2)$. Now we can use the division algorithm to find $(X^4 + Y^4)^G$. There are quite a number of steps, but (miraculously) we end with an expression involving only T_1 and T_2 as the remainder. Figure 5.1 shows the computation.

The computation in the figure shows that $(X^4 + Y^4)^G = T_1^4 - 4T_1^2T_2 + 2T_2^2$. Without looking for clever algebraic tricks we have found a mechanical procedure. In this case the division algorithm shows that

$$X^4 + Y^4 = (X + Y)^4 - 4(X + Y)^2XY + 2(XY)^2.$$

Notice that given any symmetric polynomial $f(X, Y)$ we can use the division algorithm to find $P = f^G$ such that $f = P(X + Y, XY)$. Theorem 5.5.1 is useful in that it gives a straightforward algorithm.

5.6 Buchberger's S -criterion

Theorem 5.4.7 shows the existence of a Gröbner basis for an ideal in a polynomial ring but gives no hint how to find it. There is a very nice (finite) criterion for a set of polynomials $F = (f_1, \dots, f_m)$ to be a Gröbner basis. To a pair of polynomials f, g we associate the S -polynomial $S(f, g)$, which depends on the term ordering \leq . The S -polynomial $S(f, g)$ cancels initial terms in f and g according to the term ordering \leq . For example, $S(X^2 + Y, YX + 1) = Y(X^2 + Y) - X(YX + 1) = Y^2 - X$, where \leq is the lexicographic ordering with $Y \leq X$. Buchberger's S -criterion says that F is a Gröbner basis for I if and only if $S(f_i, f_j)^F = 0$ for $1 \leq i < j \leq m$.

This turns out to be very useful in practice. It is also the basis of Buchberger's algorithm for finding Gröbner bases. If an S -polynomial S does not give a remainder S^F equal to zero then you simply add the remainder S^F to the list of polynomials and use Buchberger's S -criterion on this new list. This will eventually terminate (Buchberger's criterion will succeed).

A word of advice: no complicated or abstract mathematics is involved, just (very) clever calculations with polynomials. As a first approach to understanding Buchberger's algorithm you can go straight to subsection 5.6.2 after reading the statement of Theorem 5.6.8 and understanding the definition of S -polynomials (Definition 5.6.5). In the following, a term ordering \leq is fixed on $R = k[X_1, \dots, X_n]$.

5.6.1 The S -polynomials

Suppose we wish to check whether $(f_1, \dots, f_m) \subseteq R \setminus \{0\}$ is a Gröbner basis. Let

$$f = a_1 f_1 + \dots + a_m f_m \in \langle f_1, \dots, f_m \rangle,$$

where $a_1, \dots, a_m \in R$. Does $\text{in}_{\leq}(f_i)$ divide $\text{in}_{\leq}(f)$ for some $i = 1, \dots, m$? Put $aX^v = \text{in}_{\leq}(f)$, $c_i X^{u_i} = \text{in}_{\leq}(a_i)$ and $d_i X^{v_i} = \text{in}_{\leq}(f_i)$ for $i = 1, \dots, m$. Now introduce

$$\delta = \max_{\leq} \{v_i + u_i \mid i = 1, \dots, m\}.$$

Then it is impossible that $v \geq v_i + u_i$ for every $i = 1, \dots, m$, since the initial term of f has to be a k -linear combination of the initial terms $\text{in}_{\leq}(a_i f_i)$ for $a_i f_i \neq 0$. Therefore $v \leq \delta$. If $\delta = v$, we may assume that $\delta = v_1 + u_1 = \dots = v_r + u_r$, where $r \leq m$ and $a_i f_i \neq 0$ for $i = 1, \dots, r$. Then

$$aX^v = (c_1 d_1 + \dots + c_r d_r) X^{u_1 + v_1}.$$

In this case $d_1 X^{v_1} = \text{in}_{\leq}(f_1)$ divides $aX^v = \text{in}_{\leq}(f)$. However, if $v < \delta$ there is cancellation of maximal terms on the right hand side, and $\text{in}_{\leq}(f)$ is not necessarily divisible by $\text{in}_{\leq}(f_i)$, for $i = 1, \dots, m$. This is illustrated by the following example.

Example 5.6.1 Let \leq be the lexicographic ordering given by $X \geq Y$, $I = \langle X^2 + Y, X^2 Y + 1 \rangle \subseteq k[X, Y]$ and $f = Y^2 - 1 = Y(X^2 + Y) - (X^2 Y + 1) \in I$. Then $\text{in}_{\leq}(f) = Y^2$ but $X^2 \nmid Y^2$ and $X^2 Y \nmid Y^2$.

Our discussion leads to the following definition and proposition.

Definition 5.6.2 We say that $f \in R$ reduces to zero modulo $F = (f_1, \dots, f_m) \subseteq R \setminus \{0\}$ if there exist $a_1, \dots, a_m \in R$ such that

$$f = a_1 f_1 + \dots + a_m f_m \tag{5.8}$$

and $\text{in}_{\leq}(a_i f_i) \leq \text{in}_{\leq}(f)$ if $a_i f_i \neq 0$. This is denoted

$$f \rightarrow_F 0.$$

Remark 5.6.3 Observe that $f \rightarrow_F 0$ if and only if the maximal initial terms in the summands on the right hand side of (5.8) do not cancel. Notice also that $f \rightarrow_F 0$ if $f^F = 0$. This is the last part of Proposition 5.3.1. However, one may have $f \rightarrow_F 0$ even though $f^F \neq 0$ (see Exercise 5.18).

Proposition 5.6.4 Let $F = (f_1, \dots, f_m)$ and $I = \langle f_1, \dots, f_m \rangle$. If $f \rightarrow_F 0$ for every $f \in I$ then F is a Gröbner basis for I . If F is a Gröbner basis for I then $f^F = 0$ if and only if $f \rightarrow_F 0$ for $f \in I$.

Proof. Let $f \in I \setminus \{0\}$. The discussion at the beginning of this subsection shows that if $f \rightarrow_F 0$ then $\text{in}_{\leq}(f)$ is divisible by $\text{in}_{\leq}(f_j)$ for some $f_j \in F$. So if $f \rightarrow_F 0$ for every $f \in I$ it follows that F is a Gröbner basis for I . We have seen that $f^F = 0$ implies that $f \rightarrow_F 0$ by the last part of Proposition 5.3.1. If F is a Gröbner basis for I and $f \rightarrow_F 0$ then $f^F = 0$ since $f \in I$ (this is Proposition 5.4.2). \square

This is really not a useful test for a Gröbner basis. We need to check that every $f \in I$ reduces to zero. Using some clever manipulations one may find finitely many polynomials $S_1, \dots, S_N \in I$ such that F is a Gröbner basis if and only if $S_i \rightarrow_F 0$ for $i = 1, \dots, N$. We can in fact replace $S_i \rightarrow_F 0$ with $S_i^F = 0$, by Proposition 5.6.4. In this way we have an effective criterion for a Gröbner basis via the division algorithm provided that we can find S_1, \dots, S_N . Let us see how to do this. Suppose that

$$f = a_1 f_1 + \dots + a_m f_m \in I,$$

where $a_1, \dots, a_m \in R$. Use the notation from the beginning of this subsection. Then

$$f = C + (a_1 - \text{in}_{\leq}(a_1))f_1 + \dots + (a_r - \text{in}_{\leq}(a_r))f_r + a_{r+1}f_{r+1} + \dots + a_m f_m,$$

where $C = \text{in}_{\leq}(a_1)f_1 + \dots + \text{in}_{\leq}(a_r)f_r$. One crucial point to notice is that f is the sum of C and certain polynomials all of whose initial terms are $\leq \delta$. If on the one hand $c_1 d_1 + \dots + c_r d_r \neq 0$ then no cancellation among the initial terms occurs and $\text{in}_{\leq}(f)$ is divisible by $\text{in}_{\leq}(f_i)$ for some $i = 1, \dots, m$, as we have already seen.

Assume on the other hand that $c_1d_1 + \cdots + c_rd_r = 0$ (cancellation occurs among the initial terms). Put $g_i = X^{u_i}f_i/d_i$ and watch the following nice computational trick evolve:

$$\begin{aligned} C &= c_1d_1g_1 + \cdots + c_rd_rg_r \\ &= c_1d_1(g_1 - g_2) + (c_1d_1 + c_2d_2)(g_2 - g_3) + (c_1d_1 + c_2d_2 + c_3d_3)(g_3 - g_4) \\ &\quad + \cdots + (c_1d_1 + \cdots + c_{r-1}d_{r-1})(g_{r-1} - g_r) + (c_1d_1 + \cdots + c_rd_r)g_r. \end{aligned}$$

This shows that C is a linear combination of $g_i - g_j = X^{u_i}f_i/d_i - X^{u_j}f_j/d_j$. From this we get the crucial S -polynomials. Observe that $u_i + v_i = u_j + v_j$ as vectors in \mathbb{N}^n (the initial terms of g_i and g_j cancel). Now define $w_{ij} \in \mathbb{N}^n$ by $X^{w_{ij}} = \text{lcm}(X^{v_i}, X^{v_j})$. Then

$$\begin{aligned} g_i - g_j &= \frac{X^{u_i}f_i}{d_i} - \frac{X^{u_j}f_j}{d_j} \\ &= X^\zeta \left(\frac{X^{w_{ij}}}{d_i X^{v_i}} f_i - \frac{X^{w_{ij}}}{d_j X^{v_j}} f_j \right), \end{aligned}$$

where $\zeta + w_{ij} = u_i + v_i = u_j + v_j$. Notice the cancellation of the two initial terms in

$$\frac{X^{w_{ij}}}{d_i X^{v_i}} f_i - \frac{X^{w_{ij}}}{d_j X^{v_j}} f_j.$$

This naturally leads us to the following definition.

Definition 5.6.5 The S -polynomial of two non-zero polynomials f and g with respect to a term ordering \leq is defined as

$$S(f, g) = \frac{X^w}{\text{in}_{\leq}(f)} f - \frac{X^w}{\text{in}_{\leq}(g)} g,$$

where X^w is a least common multiple of $\text{in}_{\leq}(f)$ and $\text{in}_{\leq}(g)$.

The formal definition of S -polynomials may take some time to digest. Intuitively one just multiplies the initial terms of f and g up to a least common multiple. The letter S in S -polynomial stands for “syzygy.” This is a concept from Hilbert’s theory of syzygies for polynomial rings. A syzygy is a term from astronomy. It refers to a straight-line configuration of three celestial bodies. The moon is in syzygy with the Earth and the Sun when it is new or full.

Example 5.6.6 Let \leq be the lexicographic ordering given by $X \geq Y$ in $k[X, Y]$. Then $\text{lcm}(X^2, X^2Y) = X^2Y$, and

$$\begin{aligned} S(X^2 + Y, X^2Y + 1) &= \frac{X^2Y}{X^2}(X^2 + Y) - \frac{X^2Y}{X^2Y}(X^2Y + 1) \\ &= Y(X^2 + Y) - (X^2Y + 1) \\ &= Y^2 - 1. \end{aligned}$$

We have shown that

$$\begin{aligned} C &= \text{in}_{\leq}(a_1)f_1 + \cdots + \text{in}_{\leq}(a_r)f_r \\ &= b_1X^{\zeta_1}S(f_1, f_2) + \cdots + b_{r-1}X^{\zeta_{r-1}}S(f_{r-1}, f_r) \end{aligned} \quad (5.9)$$

with $b_i \in k$ and $\text{in}_{\leq}(X^{\zeta_i}S(f_i, f_{i+1})) \leq \delta$. This calculation is crucial for the proof of the following important insight.

Lemma 5.6.7 Let $F = (f_1, \dots, f_m)$ and $I = \langle f_1, \dots, f_m \rangle$. If $S(f_i, f_j) \rightarrow_F 0$ for every $i, j = 1, \dots, m$ then $f \rightarrow_F 0$ for every $f \in I$.

Proof. Let $f = a_1f_1 + \cdots + a_mf_m \in I$, where $a_1, \dots, a_m \in R$. Since $S(f_i, f_j) \rightarrow_F 0$, we have

$$S(f_i, f_j) = e_1f_1 + \cdots + e_mf_m$$

for $e_1, \dots, e_m \in R$, where $\text{in}_{\leq}(e_l f_l) \leq \text{in}_{\leq}(S(f_i, f_j))$ for $l = 1, \dots, m$. Recall that

$$\begin{aligned} f &= C + (a_1 - \text{in}_{\leq}(a_1))f_1 + \cdots + (a_r - \text{in}_{\leq}(a_r))f_r + a_{r+1}f_{r+1} + \cdots \\ &\quad + a_mf_m, \end{aligned}$$

where $C = \text{in}_{\leq}(a_1)f_1 + \cdots + \text{in}_{\leq}(a_r)f_r$ and $\text{in}_{\leq}(a_1f_1), \dots, \text{in}_{\leq}(a_rf_r)$ are the maximal initial terms in the summands a_1f_1, \dots, a_mf_m . Now insert the expression for $S(f_i, f_j)$ into (5.9) to get

$$f = h_1f_1 + \cdots + h_mf_m$$

with $\max\{\text{in}_{\leq}(h_i f_i) \mid h_i f_i \neq 0, i = 1, \dots, n\} \leq \delta$. This means that if the maximal initial terms on the right hand side of an expression $f = a_1f_1 + \cdots + a_nf_n$ cancel and $S(f_i, f_j) \rightarrow_F 0$ then there is another expression $f = h_1f_1 + \cdots + h_nf_n$ for which the maximal initial term in the summands on the right hand side is strictly less than the maximal initial term in the first expression. By Lemma A.3.8 we will eventually end up with an expression

$$f = b_1f_1 + \cdots + b_mf_m,$$

where the maximal initial term δ in the summands on the right hand side is $\text{in}_{\leq}(f)$. This means that $f \rightarrow_F 0$. \square

5.6.2 The S -criterion

Theorem 5.6.8 (Buchberger) *A sequence $F = (f_1, \dots, f_m)$ of polynomials is a Gröbner basis if and only if $S(f_i, f_j) \rightarrow_F 0$ for $1 \leq i < j \leq m$.*

Proof. This is a consequence of Proposition 5.6.4 and Lemma 5.6.7. \square

Corollary 5.6.9 *A sequence $F = (f_1, \dots, f_m)$ of polynomials is a Gröbner basis if and only if $S(f_i, f_j)^F = 0$ for $1 \leq i < j \leq m$.*

Proof. If $S(f_i, f_j)^F = 0$ for $1 \leq i < j \leq m$ then $S(f_i, f_j) \rightarrow_F 0$ for $1 \leq i < j \leq m$ and F is a Gröbner basis by Theorem 5.6.8. Conversely, if F is a Gröbner basis then $S(f_i, f_j)^F = 0$ by Proposition 5.4.2, since $S(f_i, f_j) \in \langle f_1, \dots, f_m \rangle$. \square

5.7 Buchberger's algorithm

The Buchberger S -criterion (Corollary 5.6.9) is a systematic way of testing whether a set of polynomials $F = (f_1, \dots, f_m)$ is a Gröbner basis. Compute the remainders of the S -polynomials $S(f_i, f_j)$, where $1 \leq i < j \leq m$. On the one hand, if they are all zero then F is a Gröbner basis. On the other hand, if one $S(f_i, f_j)^F \neq 0$ then we simply add it to F to obtain a new list

$$F' = F \cup \{S(f_i, f_j)^F\} = (f_1, \dots, f_m, S(f_i, f_j)^F),$$

hoping that F' will turn out to be a Gröbner basis for $I = \langle f_1, \dots, f_m \rangle$. Notice that F' and F generate the same ideal since $S(f_i, f_j)^F \in I$.

We can continue adding remainders of S -polynomials to our list. This is a somewhat daring step. We have no guarantee that this procedure will ever stop. Let us try it out on an example.

Example 5.7.1 Suppose we have the lexicographic ordering given by $X \geq Y$ on $k[X, Y]$ and $F = (X^2 + Y, X^2Y + 1)$. Then $S(X^2 + Y, X^2Y + 1) = Y^2 - 1$. This also becomes the remainder in the division algorithm, since none of the terms Y^2 and -1 is divisible by $\text{in}_{\leq}(X^2 + Y) = X^2$ or $\text{in}_{\leq}(X^2Y + 1) = X^2Y$.

Thus

$$S(X^2 + Y, X^2Y + 1)^F = Y^2 - 1.$$

Now let

$$F' = F \cup \{Y^2 - 1\} = (X^2 + Y, X^2Y + 1, Y^2 - 1).$$

To check whether this is a Gröbner basis, we have to compute $S(X^2 + Y, Y^2 - 1)^{F'}$ and $S(X^2Y + 1, Y^2 - 1)^{F'}$ and see whether they are zero. It is not necessary to compute $S(X^2 + Y, X^2Y + 1)^{F'}$, as this is zero because $S(X^2 + Y, X^2Y + 1) = 1 \cdot (Y^2 - 1) + 0$. Now

$$S(X^2 + Y, Y^2 - 1) = Y^2(X^2 + Y) - X^2(Y^2 - 1) = Y^3 + X^2.$$

The division algorithm gives $Y^3 + X^2 = 1 \cdot (X^2 + Y) + Y \cdot (Y^2 - 1)$, so the remainder is zero. Finally

$$S(X^2Y + 1, Y^2 - 1) = Y(X^2Y + 1) - X^2(Y^2 - 1) = 1 \cdot (X^2 + Y),$$

which also has zero remainder. By Corollary 5.6.9,

$$(X^2 + Y, X^2Y + 1, Y^2 - 1)$$

is a Gröbner basis.

The process of continuously adding non-zero remainders of S -polynomials is called *Buchberger's algorithm*. There are numerous ways of implementing it. The workhorse in the algorithm is the division algorithm and one usually wants as few divisions as possible. We will not go into implementation details but simply prove that the algorithm terminates.

Theorem 5.7.2 *Buchberger's algorithm terminates and the output is a Gröbner basis.*

Proof. Let $F = (f_1, \dots, f_s)$ be the list of polynomials in a step of Buchberger's algorithm. Suppose that $1 \leq i < j \leq s$ and $S^F \neq 0$, where $S = S(f_i, f_j)$. Since S^F is a remainder coming from the division algorithm with $F = (f_1, \dots, f_s)$, no term in S^F is divisible by any of $\text{in}_{\leq}(f_1), \dots, \text{in}_{\leq}(f_s)$. So we may prove that the algorithm terminates by proving that for any sequence of terms $T = (t_1, t_2, \dots)$ there exists a number $N \in \mathbb{N}$ such that if $i \geq N$ then t_i is divisible by t_j , where $j < N$. Dickson's lemma (Lemma 5.1.5) implies that there are finitely many terms $t_{i_1}, \dots, t_{i_r} \in T$

such that every term $t \in T$ is divisible by one of t_{i_1}, \dots, t_{i_r} . Putting $N = \max(i_1, \dots, i_r)$ we get the result. \square

The following lemma sometimes simplifies the computations in Buchberger's algorithm considerably.

Lemma 5.7.3 *Let \leq be a term ordering on $R = k[X_1, \dots, X_n]$. Let $f, g \in R$ and suppose that $\text{in}_{\leq}(f)$ and $\text{in}_{\leq}(g)$ have no common divisors (except constants). Then*

$$S(f, g) \rightarrow_{(f, g)} 0.$$

Proof. Put $r = f - \text{in}_{\leq}(f)$ and $s = g - \text{in}_{\leq}(g)$. Then

$$S(f, g) = (g - s)f - (f - r)g = rg - sf.$$

If the initial terms in rg and sf cancel then

$$\text{in}_{\leq}(r) \text{in}_{\leq}(g) = \text{in}_{\leq}(s) \text{in}_{\leq}(f).$$

This implies that $\text{in}_{\leq}(f) \mid \text{in}_{\leq}(r)$, contradicting that $\text{in}_{\leq}(r) < \text{in}_{\leq}(f)$. So the initial terms of rg and sf do not cancel. This shows that $S(f, g) \rightarrow_{(f, g)} 0$. \square

Example 5.7.4 Let $F = (T_1 - X - Y, T_2 - XY) \subseteq k[X, Y, T_1, T_2]$. Then F is already a Gröbner basis with respect to the lexicographic term ordering given by $T_1 \geq T_2 \geq X \geq Y$. This is a consequence of Theorem 5.6.8 and Lemma 5.7.3. However, if the term ordering is given by $X \geq Y \geq T_1 \geq T_2$, as in Example 5.5.2, then

$$\begin{aligned} S &= S(T_1 - X - Y, T_2 - XY) = Y(T_1 - X - Y) \\ &\quad - (T_2 - XY) = YT_1 - Y^2 - T_2. \end{aligned}$$

Notice that $S^F = S$. Using Corollary 5.6.9 you should check that $F \cup \{S\}$ is a Gröbner basis.

Example 5.7.5 Looking innocent at first, Gröbner bases can be hairy beasts that are extremely time consuming to compute and very dependent on the term ordering. Take for example ([23], Example 3.9) the ideal

$$I = \langle x^5 + y^3 + z^2 - 1, x^2 + y^2 + z - 1, x^6 + y^5 + z^3 - 1 \rangle$$

in $\mathbb{Q}[x, y, z]$. A Gröbner basis of I with respect to the lexicographic ordering $z \geq y \geq x$ is the monstrous list of polynomials seen in Figure 5.2.

$$\begin{aligned}
& (225x^4 + 675x^5 + 705x^6 + 315x^7 + 100x^8 - 555x^9 - 1946x^{10} - \\
& 1983x^{11} - 10x^{12} + 1225x^{13} + 697x^{14} + 195x^{15} + 226x^{16} + \\
& 139x^{17} - x^{18} - 13x^{19} + 3x^{20} + 2x^{21} + x^{22}, 4794799513743465x^4 + \\
& 9461645755921935x^5 + 5609230341167770x^6 + 1305539383606500x^7 + \\
& 426289252230518x^8 - 12718603398056543x^9 - 28161279400718496x^{10} - \\
& 13641002940967260x^{11} + 13303041747347884x^{12} + 12841472514397999x^{13} + \\
& 1936021990228677x^{14} + 2115618449641410x^{15} + 2686197967416241x^{16} + \\
& 266417434391307x^{17} - 308399336177560x^{18} + 40028515719740x^{19} + \\
& 22083510506531x^{20} + 20898699599882x^{21} - 307985585745030x^4y + \\
& 307985585745030x^5y, 37955678888811405x^4 + 40874650161525720x^5 - \\
& 3971051857805515x^6 + 8461551779562300x^7 - 7477091544441736x^8 - \\
& 133100833227195819x^9 - 130427012317955273x^{10} + 96308769549551000x^{11} + \\
& 112430217894147542x^{12} - 28978302929820573x^{13} - 8147851966720744x^{14} + \\
& 23240432665880855x^{15} - 2547153248711687x^{16} - 6558796078633904x^{17} + \\
& 1957860431279775x^{18} - 154503618530810x^{19} + 226403721396233x^{20} - \\
& 92968302338769x^{21} + 9239567572350900x^2y - 9239567572350900x^3y - \\
& 9239567572350900x^2y^2 + 9239567572350900x^3y^2, -92395675723509000x^2 + \\
& 267932368916755545x^4 + 607600416419937750x^5 + 326949813554222075x^6 - \\
& 32115739051910620x^7 - 858543129560584x^8 - 533880675743739115x^9 - \\
& 1553067597584776499x^{10} - 1058691906621826800x^{11} + 691613184599027638x^{12} + \\
& 932606563955672291x^{13} + 151389390751950794x^{14} + 95707520810719369x^{15} + \\
& 185431646079855213x^{16} + 30397871204445410x^{17} - 24246152848015907x^{18} + \\
& 2994483268700962x^{19} + 1053727522296225x^{20} + 1579303619755253x^{21} - \\
& 92395675723509000y^2 + 92395675723509000x^2y^2 + 92395675723509000y^3, \\
& -1 + x^2 + y^2 + z).
\end{aligned}$$

Figure 5.2

Surprisingly, there is a term ordering \leq such that the Gröbner basis of I with respect to \leq is (see Exercise 5.29)

$$(x^5 + y^3 + z^2 - 1, x^2 + y^2 + z - 1, x^6 + y^5 + z^3 - 1).$$

Here Lemma 5.7.3 is very useful.

5.8 The reduced Gröbner basis

In the following, we work with a fixed term ordering \leq in $R = k[X_1, \dots, X_n]$. A Gröbner basis (f_1, \dots, f_m) for an ideal $I \subseteq R$ is not unique. You can always add another polynomial $f \in I$ to the list (f_1, \dots, f_m) and it will still be a Gröbner basis (see Exercise 5.15). We need a more well behaved object that is unique. We may begin by observing that if we have a Gröbner basis (f_1, \dots, f_m) for the ideal I and $\text{in}_{\leq}(f_1)$ is divisible by one of $\text{in}_{\leq}(f_2), \dots, \text{in}_{\leq}(f_m)$ then (f_2, \dots, f_m) is a smaller Gröbner basis for I . Assume that $\text{in}_{\leq}(f_i) \mid \text{in}_{\leq}(f_1)$; then $\text{in}_{\leq}(f_i) \mid \text{in}_{\leq}(f)$ if $\text{in}_{\leq}(f_1) \mid \text{in}_{\leq}(f)$, where $f \in I$. So (f_2, \dots, f_m) is a Gröbner basis for I and $I = \langle f_2, \dots, f_m \rangle$ by Corollary 5.4.5. This shows that an efficient strategy for cutting down on the size of a Gröbner basis is to throw away generators f whose initial term $\text{in}_{\leq}(f)$ is divisible by the initial term of one of the other generators. This leads to the definition of a minimal Gröbner basis.

Definition 5.8.1 A *minimal Gröbner basis* (f_1, \dots, f_m) is a Gröbner basis such that

- (i) $\text{in}_{\leq}(f_i)$ is not divisible by $\text{in}_{\leq}(f_j)$ for $i \neq j$,
- (ii) the coefficient of $\text{in}_{\leq}(f_i)$ is 1.

A minimal Gröbner basis is still not unique even though it has the minimal number of elements! The unique object is the reduced Gröbner basis.

Definition 5.8.2 A *reduced Gröbner basis* (f_1, \dots, f_m) is a minimal Gröbner basis such that no term (not just the initial term) in f_i is divisible by $\text{in}_{\leq}(f_j)$ for $i \neq j$.

Theorem 5.8.3 Every ideal $I \subseteq k[X_1, \dots, X_n]$ has a unique reduced Gröbner basis.

Proof. If (f_1, \dots, f_m) and $(g_1, \dots, g_{m'})$ are two reduced Gröbner bases of I , we must have $m = m'$ and

$$\begin{aligned} \text{in}_{\leq}(f_1) &= \text{in}_{\leq}(g_1), \\ &\vdots \\ \text{in}_{\leq}(f_m) &= \text{in}_{\leq}(g_m), \end{aligned}$$

rearranging g_1, \dots, g_m if necessary. Here is why. We know that some $\text{in}_{\leq}(f_j)$ divides $\text{in}_{\leq}(g_1)$. We may assume by rearranging that $j = 1$. We also know that some $\text{in}_{\leq}(g_i)$ divides $\text{in}_{\leq}(f_1)$. Here $i = 1$, because $\text{in}_{\leq}(g_1)$ is divisible by $\text{in}_{\leq}(g_i)$. This gives that $\text{in}_{\leq}(f_1) = \text{in}_{\leq}(g_1)$, since the coefficient in both is 1. The same argument applies to the other generators, and we end up with $m = m'$ identical initial terms.

Now we wish to prove that $f_1 = g_1, \dots, f_n = g_n$ in order to prove the uniqueness of the reduced Gröbner basis. Consider $f_1 - g_1$. The initial terms in f_1 and g_1 cancel. By definition of a reduced Gröbner basis none of the terms in $f_1 - g_1$ is divisible by any $\text{in}_{\leq}(f_1), \dots, \text{in}_{\leq}(f_n)$ (here we include $\text{in}_{\leq}(f_1)$ because it has been canceled already in $f_1 - g_1$). This means that $f_1 - g_1$ is the remainder after division by f_1, \dots, f_n . But since $f_1 - g_1 \in I$ we must have $f_1 - g_1 = 0$ by Proposition 5.4.2. The same procedure applies to the other generators.

Every ideal has a minimal Gröbner basis (f_1, \dots, f_m) by the reasoning at the beginning of Section 5.8. The existence of a reduced Gröbner basis is deduced as follows: replace f_1 by the remainder of f_1 divided by f_2, \dots, f_m . With this new f_1 , replace f_2 by the remainder of f_2 divided by f_1, f_3, \dots, f_n . Continue this procedure until f_m is replaced by its remainder divided by f_1, \dots, f_{m-1} . Notice that the initial terms of the original f_1, \dots, f_m will survive and that we still have a Gröbner basis. In the end no term of f_i is divisible by $\text{in}_{\leq}(f_j)$ for $i \neq j$. Thus we end up with a reduced Gröbner basis. \square

Example 5.8.4 In Example 5.7.1 we saw that $(X^2 + Y, X^2Y + 1, Y^2 - 1)$ is a Gröbner basis for the ideal $I = \langle X^2 + Y, X^2Y + 1 \rangle$ with respect to the lexicographic ordering \leq , where $Y \leq X$. It is not minimal, though! The second generator has initial term X^2Y , which is divisible by the initial term X^2 of the first generator. We can thus leave out the middle generator, ending up with

$$(X^2 + Y, Y^2 - 1)$$

which in fact is *the* reduced Gröbner basis of I for the term ordering \leq .

Example 5.8.5 The Gröbner basis

$$G = (T_1 - X - Y, T_2 - XY, YT_1 - Y^2 - T_2) \subseteq k[X, Y, T_1, T_2]$$

from Example 5.7.4 is not minimal. The reason is that $\text{in}_{\leq}(T_2 - XY) = -XY$ is divisible by $\text{in}_{\leq}(T_1 - X - Y) = -X$. Leaving out the middle generator we get the Gröbner basis

$$G' = (T_1 - X - Y, YT_1 - Y^2 - T_2).$$

This is the Gröbner basis used in Example 5.5.2. You may check that G' is the reduced Gröbner basis when multiplied by -1 .

5.9 Solving equations using Gröbner bases

Suppose we are given a set of polynomial equations in n variables over a field k :

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0, \\ f_2(x_1, \dots, x_n) &= 0, \\ &\vdots \\ f_m(x_1, \dots, x_n) &= 0. \end{aligned}$$

Just as in the old days of algebra, we want to find the solutions of these equations. If $n = 1$ we have a system of polynomial equations in just one variable x_1 . This can be solved using the Euclidean algorithm: we know that the ideal $\langle f_1, \dots, f_m \rangle \subseteq k[x_1]$ generated by $f_1, \dots, f_m \in k[x_1]$ is a principal ideal $\langle f \rangle$, generated by a greatest common divisor f of f_1, \dots, f_m . It follows that $f_1(x) = \dots = f_m(x) = 0$ if and only if $f(x) = 0$. So we have reduced to the case of just one equation. Let $V(f_1, \dots, f_m)$ denote

$$\{(a_1, \dots, a_n) \in k^n \mid f_i(a_1, \dots, a_n) = 0 \text{ for every } i = 1, \dots, m\},$$

the set of solutions of the system of equations. Then $V(f_1, \dots, f_m)$ is also given by

$$V(I) = \{(a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \text{ for every } f \in I\},$$

where I denotes the ideal generated by f_1, \dots, f_m (see Exercise 5.31). The ideal I represents all the equations we can get by “combining” f_1, \dots, f_m . In particular, if we have a Gröbner basis (g_1, \dots, g_r) of I we get

$$V(f_1, \dots, f_m) = V(g_1, \dots, g_r).$$

The point is that the equations

$$\begin{aligned} g_1(x_1, \dots, x_n) &= 0, \\ g_2(x_1, \dots, x_n) &= 0, \\ &\vdots \\ g_r(x_1, \dots, x_n) &= 0 \end{aligned}$$

are often much easier to solve.

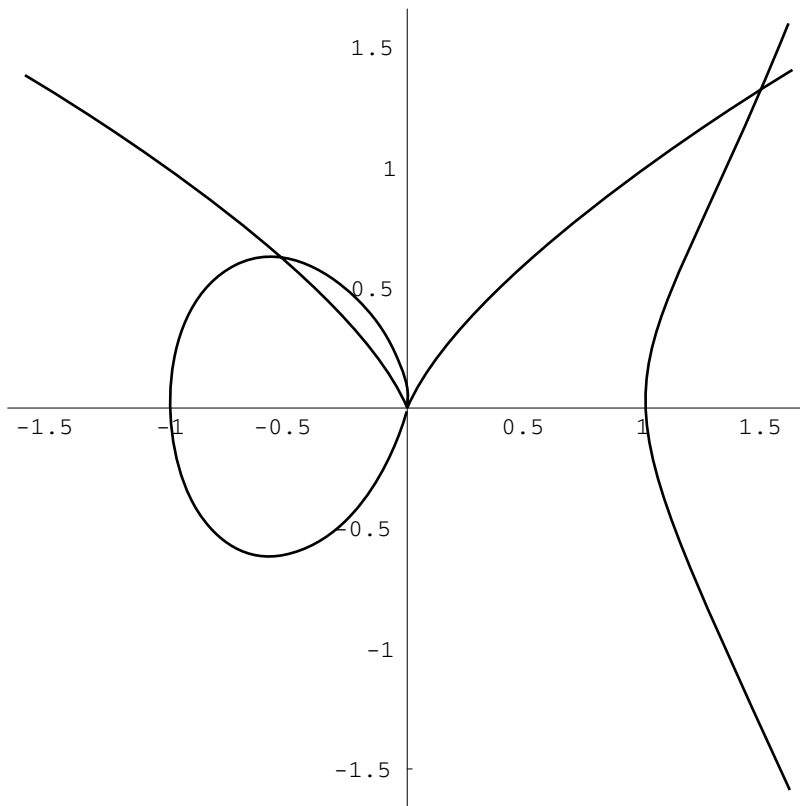
This is the basis for doing “Gaussian” elimination on our system of equations using Gröbner bases. We wish to eliminate variables by combining some equations to get equations with fewer variables. The ideal situation is if the system of equations consists of some equations containing the variables x_1, \dots, x_n , some equations containing the variables x_2, \dots, x_n and \dots and some equations containing only x_n . Then we could begin by solving the equations involving only x_n , insert our solutions into the equations involving only x_{n-1} and x_n and so forth. Thereby we only have to solve equations involving one variable. The process of eliminating variables can be formulated as that of finding polynomials in I involving only x_1 , polynomials in I involving only x_1, x_2 and so on. Viewing I as the equations that we can deduce by combining f_1, \dots, f_m we wish to find

$$\begin{aligned} I \cap k[x_1], \\ I \cap k[x_1, x_2], \\ &\vdots \\ I \cap k[x_1, \dots, x_{n-1}]. \end{aligned}$$

The following theorem is almost too good to be true.

Theorem 5.9.1 *Let G be a Gröbner basis for an ideal $I \subseteq k[X_1, \dots, X_n]$ with respect to the lexicographic ordering \leq given by $X_1 \leq X_2 \leq \dots \leq X_n$. Then $G \cap k[X_1, \dots, X_i]$ is a Gröbner basis for the ideal $I \cap k[X_1, \dots, X_i]$ in $k[X_1, \dots, X_i]$ with respect to the lexicographic ordering \leq for the polynomials in $k[X_1, \dots, X_i]$.*

Let $G' = G \cap k[X_1, \dots, X_i]$. Suppose that $f \in I \cap k[X_1, \dots, X_i]$. Then $\text{in}_{\leq}(g) \mid \text{in}_{\leq}(f)$ for some $g \in G$ using Definition 5.4.1. On the other hand

**Figure 5.3**

the terms in g are all smaller than $\text{in}_{\leq}(g)$ in our lexicographic term ordering. This tells us (why??) that $g \in G'$. Therefore G' is a Gröbner basis for $I \cap k[X_1, \dots, X_i]$ with respect to \leq for the polynomials in $k[X_1, \dots, X_i]$.

Example 5.9.2 Let us find the solutions to the system of equations

$$\begin{aligned} Y^2 - X^3 + X &= 0, \\ Y^3 - X^2 &= 0 \end{aligned} \tag{5.10}$$

in \mathbb{R}^2 . This corresponds to finding the points of intersection between the curves shown in Figure 5.3.

To solve (5.10) we need to transform it to another system of equations according to Theorem 5.9.1. We will do this by computing a Gröbner basis for $\langle Y^2 - X^3 + X, Y^3 - X^2 \rangle$ with respect to the lexicographic ordering \leq where $X \geq Y$. A straightforward application of Buchbergers algorithm (even though the algorithm needs a few steps here) gives the Gröbner basis

$$(\underline{Y^2 - X^3 + X}, \underline{Y^3 - X^2}, -X - Y^2 + \underline{XY^3}, \underline{XY^2} + Y^3 - Y^6, \\ Y^3 - Y^4 - 2Y^6 + \underline{Y^9}, -\underline{X} - Y^2 - Y^4 + Y^7),$$

where the initial terms are underlined. From this we see that the reduced Gröbner basis is

$$(Y^3 - Y^4 - 2Y^6 + Y^9, X + Y^2 + Y^4 - Y^7).$$

So finding the solutions to (5.10) is equivalent to solving

$$Y^3 - Y^4 - 2Y^6 + Y^9 = 0, \\ X + Y^2 + Y^4 - Y^7 = 0.$$

This is much more manageable than solving the original system (5.10). Now we can find the solutions to the equation

$$Y^3 - Y^4 - 2Y^6 + Y^9 = Y^3(1 - Y - 2Y^3 + Y^6) = 0 \quad (5.11)$$

and plug them into $X + Y^2 + Y^4 - Y^7$ and get the corresponding X -values. Using numerical approximations (and a computer) one finds apart from $Y = 0$ that $Y = 0.605423$ and $Y = 1.2876$ are approximate real solutions to (5.11). So the real solutions to (5.10) are $(0, 0)$, $(-0.471073, 0.605423)$ and $(1.46109, 1.2876)$.

Notice that $\mathbb{R}[Y] \cap \langle Y^2 - X^3 + X, Y^3 - X^2 \rangle = \langle Y^3 - Y^4 - 2Y^6 + Y^9 \rangle$ by Theorem 5.9.1.

It is worth pointing out that all the clever algebraic tricks one might come up with solving a system of polynomial equations have been translated into a precise method using Gröbner bases.

5.10 Exercises

1. In Section 5.1 the set $R[\mathbb{N}^n]$ was introduced along with an addition and a multiplication. Let $f, g, h \in R[\mathbb{N}^n]$.
 - (i) Prove that $f + g, fg \in R[\mathbb{N}^n]$.
 - (ii) Prove that $fg = gf$.

- (iii) Prove that $f(g + h) = fg + fh$.
- (iv) Prove that $f(gh) = (fg)h$ by reducing to the case $h = cX^v$.
- 2. Prove that the ideal $\langle X, Y \rangle \subseteq \mathbb{Q}[X, Y]$ is not a principal ideal, by assuming that there exists $f \in \mathbb{Q}[X, Y]$ such that $\langle X, Y \rangle = \langle f \rangle$. Make use of the degree function in $\mathbb{Q}[Y][X]$ with respect to X to reach a contradiction.
- 3. Give an example of a total ordering that is not a well ordering.
- 4. Why is a well order a total ordering?
- 5. Let \leq be a term ordering on \mathbb{N}^n . Show that $a + c \leq b + d$ if $a \leq b$ and $c \leq d$, where $a, b, c, d \in \mathbb{N}^n$.
- 6. Suppose that $v \in \mathbb{R}^2$. Define the relation R_v on \mathbb{N}^2 by $v_1 R v_2 \Leftrightarrow v \cdot v_1 \leq v \cdot v_2$, where \cdot refers to the usual scalar product.
 - (i) Is $R_{(1,1)}$ a partial ordering?
 - (ii) Is $R_{(1,\sqrt{2})}$ a partial ordering? Is it a term ordering?
 - (iii) Is $R_{(-1,\sqrt{2})}$ a term ordering?
- 7. Prove that \leq is reflexive, antisymmetric, transitive, total with $0 \leq v$, $v_1 \leq v_2 \Rightarrow (v_1 + v) \leq (v_2 + v)$ for every $v, v_1, v_2 \in \mathbb{N}^n$, where
 - (i) $\leq = \leq_{\text{lex}}$,
 - (ii) $\leq = \leq_{\text{grlex}}$.
- 8. Prove that \leq_v , defined in (5.1), is a term ordering.
- 9. Let $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$. Define the relation R on \mathbb{N}^n by

$$\alpha R \beta$$

if and only if $\alpha = \beta$ or $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ or $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ and the first coordinates α_i, β_i from the right that are different satisfy $\alpha_i > \beta_i$.

- (i) Show that R is a term ordering (thus R is reflexive, antisymmetric, transitive, total, with $0 R v$, $v_1 R v_2 \Rightarrow (v_1 + v) R (v_2 + v)$ for every $v, v_1, v_2 \in \mathbb{N}^n$).
 - (ii) Show without using Lemma 5.1.5 or Corollary 5.1.7 that R is a well ordering.
- The relation R is called the graded reverse lexicographic ordering. Usually it is the “fastest” term ordering in Gröbner basis computations.
- 10. Show that the graded reverse lexicographic ordering of Exercise 5.9 is the same as the graded lexicographic ordering \leq_{grlex} on \mathbb{N}^2 . Give an example showing that the graded reverse lexicographic ordering is not the same as the graded lexicographic ordering on \mathbb{N}^3 .
 - 11. Let $f, g \in R[X_1, \dots, X_n] \setminus \{0\}$ where R is a domain and let \leq be a term ordering on R . Prove that

$$\text{in}_{\leq}(fg) = \text{in}_{\leq}(f) \text{in}_{\leq}(g).$$

12. Let $f, g \in R[X_1, \dots, X_n] \setminus \{0\}$ where R is a domain and let \leq be a term ordering on R . Prove that

$$\text{in}_{\leq}(f + g) \leq \max(\text{in}_{\leq}(f), \text{in}_{\leq}(g)).$$

13. Compute the remainder $f^{(f_1, f_2)}$, where

$$f = 1 + X^5 + X + Y + X^3Y + X^4Y + Y^2 + 2X^2Y^2 + XY^3$$

and $(f_1, f_2) = (X^3 + Y^2, X^2Y + 1)$, using the division algorithm (and the lexicographic ordering $X \geq Y$).

- (i) The same as above, but with (f_2, f_1) .
 (ii) Compute the remainder $f^{(f_1, f_2)}$ assuming that $X \leq Y$.
 14. Let $F = (X^2 + Y, X^2Y + 1) \subseteq k[X, Y]$, where k is a field and let \leq be a term ordering on $k[X, Y]$. Show that F is not a Gröbner basis with respect to \leq .
 15. Let $f \in I = \langle f_1, \dots, f_m \rangle \subseteq k[X_1, \dots, X_n]$ and suppose that (f_1, \dots, f_m) is a Gröbner basis (with respect to some term ordering \leq) for I . Prove that (f_1, \dots, f_m, f) is also a Gröbner basis for I .
 16. Let $G = (g_1, \dots, g_r) \subseteq k[X_1, \dots, X_n]$ and $I = \langle g_1, \dots, g_r \rangle$. Prove that G is a Gröbner basis if and only if $(f \in I \iff f^G = 0)$ for every $f \in I$.
 17. Let R be a (commutative) ring and $a_1, \dots, a_n, b_1, \dots, b_n \in R$. Show that

$$a_1a_2 \cdots a_n - b_1b_2 \cdots b_n \in \langle a_1 - b_1, a_2 - b_2, \dots, a_n - b_n \rangle. \quad (5.12)$$

Now assume that $f, f_1, \dots, f_r \in k[X_1, \dots, X_n]$ and that $f = P(f_1, \dots, f_r)$ for a suitable polynomial $P \in k[T_1, \dots, T_r]$. Apply (5.12) to prove that

$$f(X_1, \dots, X_n) - P(T_1, \dots, T_r) \in I,$$

where I is the ideal $\langle T_1 - f_1, \dots, T_r - f_r \rangle$ in the polynomial ring

$$k[X_1, \dots, X_n, T_1, \dots, T_r].$$

18. Let $F = (X^2 + Y, X^2Y + 1) \subseteq \mathbb{Q}[X, Y]$ and $f = X^3Y + X^2Y + X + Y^2$. Consider the lexicographic ordering \leq with $X \geq Y$.
 (i) Prove that $f \rightarrow_F 0$.
 (ii) Prove that $f^F \neq 0$ and $f^{F'} \neq 0$, where $F' = (X^2Y + 1, X^2 + Y)$.
 19. Compute the reduced Gröbner basis of $(X^2 + Y, X + Y)$ using the lexicographic ordering $X \geq Y$.
 20. Is $(X^2 + Y, X + Y)$ already a Gröbner basis with respect to some term ordering?

21. Decide whether $f = X^3Y + X^3 + X^2Y^3 - X^2Y + XY + X$ lies in the ideal $I = \langle X^2 + Y, X^2Y + 1 \rangle \subseteq k[X, Y]$. If so, find $a_1, a_2 \in k[X, Y]$ such that $f = a_1f_1 + a_2f_2$.
22. Let $I \subseteq k[X, Y, Z]$ denote the ideal $\langle X^2 - Y, Z^3 + Y^2 \rangle \subseteq k[X, Y, Z]$. Let \leq denote the lexicographic ordering on $k[X, Y, Z]$ given by $X \geq Y \geq Z$.
- (i) Show that $(X^2 - Y, Z^3 + Y^2)$ is a reduced Gröbner basis with respect to \leq for I .
- (ii) Show that $X^3 - XY + Y^2 + Z^4 + ZY^2 \notin I$.
23. Let I be the ideal $(f_1, f_2) = (X^2 + Y, X + Y) \subseteq k[X, Y]$.
- (i) Show that $f = X^2 + X^4 + X^2Y + X^3Y - Y^2 + XY^2 \in I$
- (ii) Compute $a_1, a_2 \in k[X, Y]$ such that $f = a_1f_1 + a_2f_2$.
24. Let $I \subseteq \mathbb{Q}[X, Y]$ denote the ideal $\langle X^2 + Y^2, X^3 + Y^3 \rangle \subseteq \mathbb{Q}[X, Y]$. Let \leq denote the lexicographic ordering on $\mathbb{Q}[X, Y]$ given by $X \geq Y$.
- (i) Compute the S -polynomials $S_1 = S(X^2 + Y^2, X^3 + Y^3)$ and $S_2 = S(X^2 + Y^2, S_1)$ with respect to \leq and show that $S_1, S_2 \in I$. Use this to prove that $Y^4 \in I$.
- (ii) Show that the reduced Gröbner basis for I with respect to \leq is $(Y^4, XY^2 - Y^3, X^2 + Y^2)$.
- (iii) Show that $(X^2 + Y^2, X^3 + Y^3)$ cannot be a Gröbner basis for I for any term ordering.
25. Let R denote the ring $\mathbb{Q}[X, Y, S, T]$ and \leq the lexicographic term ordering on R given by

$$X \geq Y \geq S \geq T.$$

Let I denote the ideal $R(S - X^2) + R(T - XY)$.

- (i) Show that the reduced Gröbner basis for I with respect to \leq is

$$G = (X^2 - S, XY - T, XT - YS, Y^2S - T^2).$$

- (ii) Compute the remainder $Q = (X^4 + 2X^3Y)^G$. Show that $Q \in \mathbb{Q}[S, T]$ and that $X^4 + 2X^3Y = Q(X^2, XY)$.
- (iii) Let $f \in \mathbb{Q}[X, Y]$ and let Q denote the unique remainder f^G . Show that $f(X, Y) = Q(X^2, XY)$ if $Q \in \mathbb{Q}[S, T]$.
26. Let c denote the vector $(c_1, c_2) \in \mathbb{R}^2$ and let $c \cdot v = c_1a + c_2b$, where $v = (a, b) \in \mathbb{R}^2$. Define the relation R_c on \mathbb{N}^2 by

$$v_1 R_c v_2 \iff c \cdot v_1 \geq c \cdot v_2,$$

where $v_1, v_2 \in \mathbb{N}^2$.

- (i) Show that R_c is reflexive and transitive.
- (ii) Give an example showing that R_c is not necessarily antisymmetric.

- (iii) Show that R_c is antisymmetric if $c_1/c_2 \notin \mathbb{Q}$, where $c_2 \neq 0$.
- (iv) Let $c = (1, \sqrt{2})$. Show that R_c is a term ordering on \mathbb{N}^2 . Compute the reduced Gröbner basis for the ideal $\langle X^2 + Y, X^2Y + 1 \rangle$ with respect to this term ordering (the term $X^m Y^n$ is identified with the vector $(m, n) \in \mathbb{N}^2$).
- (v) Let $\leq \subseteq \mathbb{N}^2 \times \mathbb{N}^2$ denote the lexicographic term ordering on \mathbb{N}^2 given by $(1, 0) \geq (0, 1)$. Show that $\geq \neq R_c$ for every $c \in \mathbb{R}^2$.
27. Show that $X^2Z + Y \notin \langle XZ + Y^2, X + Y \rangle \subseteq \mathbb{Q}[X, Y, Z]$.
28. Let I denote the ideal generated by $X^2 + Y$ and $X^2Y + 1$ in $\mathbb{Q}[X, Y]$.
- (i) Compute a Gröbner basis for I with respect to the lexicographic term ordering \leq , where $Y \geq X$.
- (ii) Show that $Y^2 - 1, X^4 - 1 \in I$.
- (iii) Let \leq be an arbitrary term ordering. Prove that

$$(X^2 + Y, Y^2 - 1, X^4 - 1)$$

is a Gröbner basis for I with respect to \leq .

29. Show that the generators

$$I = \langle x^5 + y^3 + z^2 - 1, x^2 + y^2 + z - 1, x^6 + y^5 + z^3 - 1 \rangle$$

of Example 5.7.5 in fact form a Gröbner basis with respect to some term ordering (hint: construct a suitable weighted term ordering using (5.1)).

30. Let X be any subset of $k^n = k \times \cdots \times k$ (n times). Prove that

$$I(X) = \{f \in k[X_1, \dots, X_n] \mid f(a_1, \dots, a_n) = 0 \forall (a_1, \dots, a_n) \in X\}$$

is an ideal in $k[X_1, \dots, X_n]$. Show that $V(I(X)) \supseteq X$ and that $I(X) = I(V(I(X)))$.

31. Let $f_1, \dots, f_m \in k[x_1, \dots, x_n]$. Prove that

$$V(f_1, \dots, f_m) = V(I),$$

where $I = \langle f_1, \dots, f_m \rangle$.

32. Consider the ideal $I = \langle 5x + y + z - 17, x + y - z - 1, x + y + z - 9 \rangle \subseteq \mathbb{R}[x, y, z]$. Compute a Gröbner basis for I with respect to the lexicographic ordering \leq , where $x \geq y \geq z$. What is the relation to Gauss elimination when solving the system

$$\begin{aligned} 5x + y + z &= 17, \\ x + y - z &= 1, \\ x + y + z &= 9 \end{aligned}$$

of linear equations over \mathbb{R} ?

33. **(HOF)** The following problem shows that every ideal has a finite generating set that is a Gröbner basis with respect to all term orderings. Such a generating set is called a universal Gröbner basis. Let $I \subseteq k[X_1, \dots, X_n]$ be an ideal.

(i) Show that there are only finitely many ideals generated by initial terms of elements in I . More precisely show that

$$\{\text{in}_{\leq}(I) \mid \leq \text{ term ordering on } k[X_1, \dots, X_n]\}$$

is a finite set. Where $\text{in}_{\leq}(I) = \langle \text{in}_{\leq}(f) \mid f \in I \setminus \{0\} \rangle$.

(ii) Show that every ideal $I \subseteq k[X_1, \dots, X_n]$ has a set of generators that is a Gröbner basis for every term ordering.