Chapter 2 §7. Buchberger's Algorithm. We start with an example.

Example 2.7.0.1. Consider $k[x,y]$ with grlex order and let $I = \langle f_1, f_2\rangle$ where $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$.

$$S(f_1, f_2) = yf_1 - xf_2 = y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2.$$

Since the leading term of $S(f_1, f_2) = -x^2$ is not in $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2)\rangle = x^3k[x,y] + x^2yk[x,y]$, because this last ideal doesn't contain any nonzero terms of total degree < 3, $\{f_1, f_2\}$ is not a Gröbner basis for I.

We will try to produce a Gröbner basis for I by adding to the trial basis the remainders of those S-polynomials which give nonzero remainders when divided by the trial basis. Continue this augmentation until every S-polynomial of the arrived at trial basis gives a zero remainder when divided by the (arrived at) trail basis. When this state has been reached the trial basis is a Gröbner basis for I according to Theorem 2.6.0.11 or (theorem 6) of §2.6.

Step 1: Put $f_3 = -x^2$. and let $F = (f_1, f_2, f_3) = (x^3 - 2xy,\ x^2y - 2y^2 + x, -x^2)$. Then

$$S(f_1, f_2) = f_3;\ \text{so } \overline{S(f_1, f_2)}^F = 0;$$
$$S(f_1, f_3) = (x^3 - 2xy) + x(-x^2) = -2xy;\ \text{ and } \overline{S(f_1, f_3)}^F = -2xy.$$

So put $f_4 = -2xy$.

Step 2: Put $F = (f_1, f_2, f_3, f_4)$. We know that $S(f_1, f_2)$, $S(f_1, f_3)$ give remainders of zero when divided by $F = (x^3 - 2xy,\ x^2y - 2y^2 + x,\ -x^2,\ -2xy)$.

$$S(f_1, f_4) = y(x^3 - 2xy) - \left(\frac{-x^2}{2}\right)(-2xy) = -2xy^2 = yf_4;\ \text{so } \overline{S(f_1, f_4)}^F = 0;$$
$$S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x;\ \text{and } \overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0$$

So put $f_5 = -2y^2 + x$.

Step 3: If we put $F = (f_1, f_2, f_3, f_4, f_5)$ we can compute that $\overline{S(f_i, f_j)}^F = 0$ for all i, j and F is then a Gröbner basis for I.

This procedure works in general and is known as "Buchberger's Algorithm". It usually leads to a somewhat larger basis than necessary.

Lemma 2.7.0.3. (Lemma 3.) Let G be a Gröbner basis for the polynomial ideal I. Let $p \in I$ be a polynomial such that $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$. Then $G - \{p\}$ is also a Gröbner basis for I.

Proof. We know $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$. Since $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$ adjoining p to $G - \{p\}$ will not increase the ideal generated by the leading terms, that is, $\langle \mathrm{LT}(G - \{p\})\rangle = \langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$. This is equivalent to the statement: " $G - \{p\}$ is a Gröbner basis for I." ∎

By adjusting constants to make all leading coefficients 1 and removing any p with $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$ we arrive at what we will call a *minimal* Gröbner basis for I. Specifically,

Definition 2.7.0.4. A *minimal Gröbner basis* for a polynomial ideal I is a Gröbner basis G for I such that:

(i) The leading term of p is 1 for all $p \in G$.
(ii) $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle$ for any $p \in G$.

We can construct a minimal Gröbner basis for an ideal I by applying Buchberger's algorithm and then proceding through the basis, deleting those members p for which $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$.

To illustrate this take the Gröbner basis for $I = \langle x^3 - 2xy,\, x^2y - 2y^2 + x\rangle$ which we constructed using Buchberger's algorithm, namely,

$$\begin{aligned}
&f_1 = x^3 - 2xy, && \mathrm{LT}(f_1) = x^3 = -x \cdot \mathrm{LT}(f_3);\\
&f_2 = x^2y - 2y^2 + x, && \mathrm{LT}(f_2) = x^2y = -\frac{1}{2}x \cdot \mathrm{LT}(f_4);\\
&f_3 = -x^2,\\
&f_4 = -2xy,\\
&f_5 = -2y^2 + x.
\end{aligned}$$

After crossing out f_1 and f_2 for the reasons indicated in the right column, we then "normalize" the leading terms to get the minimal basis

$$M = \left\{x^2,\, xy,\, y^2 - \frac{1}{2}x\right\}.$$

In general there are many minimal bases for a given ideal $I \subset k[x_1, \ldots, x_n]$ of which one type stands out:

Definition 2.7.0.5. A *reduced Gröbner basis* for a polynomial ideal I is a basis $G = \{g_1, \ldots, g_s\}$ with $\mathrm{LT}(I) \subset \langle \mathrm{LT}(G)\rangle$, where $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$; so that, in particular, it is a Gröbner basis for I, for which

(i) The leading coefficient of each g_i is 1.
(ii) No monomial of g_i lies in $\langle \mathrm{LT}(G - \{g_i\})\rangle$ for any i, $1 \leq i \leq s$.

Reduced Gröbner bases are unique.

Theorem 2.7.0.8. Let $I \neq \{0\}$ be a non empty polynomial ideal. Then, for a given polynomial ordering, I has a unique reduced Gröbner basis.

Proof. Let G be a minimal Gröbner basis for I. We say that $g \in G$ is *reduced for* G provided that no monomial of g is in $\langle \mathrm{LT}(G - \{g\})\rangle$. Our goal is to modify G until all its elements are reduced.

Note 1. Since the statement: "g is reduced for G" only involves g and the leading terms of $G - \{g\}$, it follows that if g is reduced for G, then g is also reduced for any Gröbner basis G' containing g and having $\mathrm{LT}(G - \{g\}) = \mathrm{LT}(G' - \{g\})$. That is, as long as $\mathrm{LT}(g') = \mathrm{LT}(g)$ and $g' \in I$, we can substitute g' for g in G without destroying the the fact that G is a Gröbner basis. We proceed to detail such a substitution.

Given $g \in G$, choose some ordering for $G - \{g\}$ and, using this ordering in the division, let $g' = \overline{g}^{G-\{g\}}$. Set $G' = (G - \{g\}) \cup \{g'\}$. (Note: It is not hard to show that the remainder$\overline{g}^{G-\{g\}}$ doesn't actually depend on the ordering used in the division which produced it, but we don't need this fact.) We claim that G' is a minimal Gröbner basis for I. In fact, $\mathrm{LT}(G') = \mathrm{LT}(G')$ since $\mathrm{LT}(g') = \mathrm{LT}(g)$ because the fact that G is minimal implies that $\mathrm{LT}(g) \notin \mathrm{LT}(G - \{g\})$ and hence appears in the remainder $\overline{g}^{G-\{g\}}$, where it will still be the leading term. Since whether or not a Gröbner basis is a minimal Gröbner basis only depends on the leading terms of the basis elements, it follows that G' is a minimal Gröbner basis for I.

Next note that g' is reduced for G', because no monomial of g would end up in the remainder $g' = \overline{g}^{G-\{g\}}$ if it had been divisible by any element of $\mathrm{LT}(G - \{g\})$ or (since it is the same set) $\mathrm{LT}(G' - \{g'\})$. Thus replacing G by G' doesn't change the set of leading terms $\mathrm{LT}(G)$, or the number of elements in the basis, but if g was not reduced for G the new basis G' has at least one more polynomial than G, namely the polynomial g', whose monomials are not divisible by the leading terms of the other basis elements. In this way we can replace the polynomials of a given minimal Gröbner basis one at a time to arrive at a minimal Gröbner basis for which each of its elements is reduced. This last mentioned basis is then a reduced Gröbner basis for I.

It remains to establish uniqueness. We start by establishing the following fact: If G and $\tilde{G}$ are minimal Gröbner bases for the polynomial ideal I, then $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$. **Subproof.** Suppose $f \in \mathrm{LT}(G)$. Since f is in the monomial ideal $\langle \mathrm{LT}(\tilde{G})\rangle$, there is an $\tilde{f} \in \mathrm{LT}(\tilde{G})$ with $\mathrm{LT}(f) = g \cdot \mathrm{LT}(\tilde{f})$ for some $g \in k[x_1, \ldots, x_n]$.

Similarly, there is an $\hat{f} \in \mathrm{LT}(G)$ whose leading term divides $\mathrm{LT}(\tilde{f})$; so $\mathrm{LT}(\tilde{f}) = h \cdot \mathrm{LT}(\hat{f})$ for some $h \in k[x_1, \ldots, x_n]$. Thus $\mathrm{LT}(f) = c\mathrm{LT}(\hat{f})$ for some $c \in k[x_1, \ldots, x_n]$. If $f \neq \hat{f}$ we have $\mathrm{LT}(f) = c\mathrm{LT}(\hat{f}) \in \langle \mathrm{LT}(G - \{f\}) \rangle$ which contradicts the fact that G is a minimal basis; so it must be that $f = \hat{f}$. This means that the two monomials $\mathrm{LT}(f)$ and $\mathrm{LT}(\tilde{f})$ divide each other. Since the associated leading coefficient is 1 in each case (All leading coefficients in a minimal basis are one's.), they must be identical. $\mathrm{LT}(f) = \mathrm{LT}(\tilde{f})$. The elements of G and $\tilde{G}$ are then paired and $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$. **End of subproof.** In particular, two minimal bases for I have the same number of elements.

Picking up the argument in the preceding paragraph, suppose G and $\tilde{G}$ are reduced Gröbner bases for the ideal I, and that $f \in G$ and $\tilde{f} \in \tilde{G}$ are paired by the fact that $\mathrm{LT}(f) = \mathrm{LT}(\tilde{f})$. To prove uniqueness of reduced Gröbner bases it suffices to show (for each such paired $f, \tilde{f}$) that $f = \tilde{f}$. **Subproof.** Consider $f - \tilde{f} \in I$. First, since G is a Gröbner basis for I, it follows that $\overline{f - \tilde{f}}^{G} = 0$. Second, because the leading terms of f and $\tilde{f}$ cancel in the difference, no monomial of $f - \tilde{f}$ is divisible by $\mathrm{LT}(f)$. No monomial of $f - \mathrm{LT}(f)$ is divisible by any of the leading terms $\mathrm{LT}(G - \{f\})$ and no monomial of $\tilde{f} - \mathrm{LT}(\tilde{f})$ is divisible by any of the leading terms of $\mathrm{LT}(\tilde{G} - \{\tilde{f}\}) = \mathrm{LT}(G - \{f\})$. Thus no monomial of $f - \tilde{f} = (f - \mathrm{LT}(f)) - (\tilde{f} - \mathrm{LT}(\tilde{f}))$ is divisible by any monomial of $\{\mathrm{LT}(f)\} \cup \mathrm{LT}(G - \{f\}) = \mathrm{LT}(G)$. This last sentence implies that $\overline{f - \tilde{f}}^{G} = f - \tilde{f}$. Putting this last relation together with the first relation saying $\overline{f - \tilde{f}}^{G} = 0$, shows that $f = \tilde{f}$ and completes the proof of uniqueness. ∎

Chapter 2 Exercises for §2.7.

---

§2.7.1.

Check that $\overline{S(f_i, f_j)}^{F} = 0$ for all pairs $1 \leq i < j \leq 5$ when $F = (f_1, f_2, f_3, f_4, f_5)$ and

$$\begin{aligned} f_1 &= x^3 - 2xy, \\ f_2 &= x^2 y - 2y^2 + x, \\ f_3 &= -x^2, \\ f_4 &= -2xy, \\ f_5 &= -2y^2 + x. \end{aligned}$$

We have already done this except for

$$\begin{aligned} S(f_1, f_5) &= 2y^2(x^3 - 2xy) + x^3(-2y^2 + x) = -4xy^3 + x^4 = 2y^2 f_4 - x^2 f_3. \\ S(f_2, f_4) &= 2(x^2 y - 2y^2 + x) + x(-2xy) = -4y^2 + 2x = 2f_5. \\ S(f_2, f_5) &= 2y(x^2 y - 2y^2 + x) + x^2(-2y^2 + x) = -4y^3 + 2xy = 2yf_5. \\ S(f_3, f_4) &= 2y(-x^2) - x(-2xy) = 0. \\ S(f_3, f_5) &= 2y^2(-x^2) + x^2(-2y^2 + x) = x^3 = -xf_3. \\ S(f_4, f_5) &= y(-2xy) - x(-2y^2 + x) = -x^2 = f_3. \end{aligned}$$

Since we don't know that F is a Gröbner basis yet we should actually calculate that the remainder after division by F is zero in each case.

---

§2.7.2.

Use Buchberger's algorithm to find a Gröbner basis for each of the following ideals. You may use a computer algebra system to compute the S-polynomials and remainders. Use the lex, then the glex order in each case, and then compare your results.

(a) $I = \langle x^2 y - 1,\ xy^2 - x \rangle$

(b) $I = \langle x^2 + y,\ x^4 + 2x^2 y + y^2 + 3 \rangle$ [What does your result indicate about the variety $\mathbf{V}(I)$?]

(c)$I = \langle x - z^4,\, y - z^5 \rangle$

Solution. The solutions are detailed on the Mathematica 3.0 printouts accompanying this sheet.

---

§2.7.3.

Find reduced Gröbner bases for the ideals in Exercise 2.7.2 with respect to the lex and the grlex orders.

Solution. Again the details are on the Mathematica 3.0 printouts. Here are the results

(a) $G = \{-1 + x^4,\, -x^2 + y\}$ when one uses lex order with $y > x$. In the other three cases the result is $G = \{-1 + y^2,\, x^2 - y\}$.

(b) In all four possible cases the result is $G = \{1\}$. In this case the ideal is all of $k[x, y]$.

(c) $G = \{y - z^5,\, x - z^4\}$ with

lex $x > y > z$;
lex $y > x > z$;
lex $x > z > y$.

$G = \{-x + z^4,\, y - xz\}$ with

lex $y > z > x$.

$G = \{-y + xz, -x + z^4, -x^2 + yz^3, -x^3 + y^2z^2, x^4 - y^3z\}$ with

grlex $x > y > z$;
grlex $x > z > y$.

$G = \{x^5 - y^4, -x^4 + y^3z, -y + xz, -x^3 + y^2z^2, -x^2 + yz^3, -x + z^4\}$ with

lex $z > y > x$;
lex $z > x > y$;
grlex $z > x > y$;
grlex $y > z > x$;
grlex $z > y > x$;
grlex $y > x > z$.

---

§2.7.4.

Use the result of Exercise 2.4.7 to give an alternative proof that Buchberger's algorithm will always terminate after a finite number of steps.

Proof. Let B_n denote the trial Gröbner basis which the algorithm produces at the close of the n-th step. We know that $B_1 \subset B_2 \subset B_3 \subset \cdots$, but what is more important from our point of view is that the sets of leading terms increase also. (Here we have used and will continue to use "leading terms" to mean "leading monomials".) $\mathrm{LT}(B_1) \subset \mathrm{LT}(B_2) \subset \mathrm{LT}(B_3) \subset \cdots$ and the algorithm terminates when this sequence of leading terms stabilizes. To be more precise here let $\mathrm{ELT}(B)$ denote the set of exponents of leading terms of polynomials in B. The monomials which are divisible by $\mathrm{LT}(B)$ have the form x^α where $\alpha \in \mathrm{ELT}(B) + \mathbf{Z}^n_{\geq 0}$. Now the increasing union $A = \bigcup_{t \geq 1} \left(\mathrm{ELT}(B_t) + \mathbf{Z}^n_{\geq 0}\right)$ is a subset of $\mathbf{Z}^n_{\geq 0}$ and hence by exercise 2.4.7 has the form $\bigcup_{i=1}^{s} \left(\alpha(i) + \mathbf{Z}^n_{\geq 0}\right)$ for some subset $\{\alpha(1), \ldots, \alpha(s)\} \subset \mathbf{Z}^n_{\geq 0}$. If t is large enough so that $\{\alpha(1), \ldots, \alpha(s)\} \subset \mathrm{ELT}(B_t) + \mathbf{Z}^n_{\geq 0}$, the sequence $\mathrm{ELT}(B_t) + \mathbf{Z}^n_{\geq 0} = \mathrm{ELT}(B_{t+1}) + +\mathbf{Z}^n_{\geq 0} = \cdots$ will have stabilized which means that $\mathrm{LT}(B_t) = \mathrm{LT}(B_{t+1}) = \cdots$ and Buchberger's algorithm will terminate. The reason for this is that no two polynomial remainders used to augment the growing basis in Buchberger's algorithm can have the same leading exponent; so once the $\mathrm{LT}(B_t)$'s stop growing the algorithm is not adding any more polynomials to the basis. ∎

---

§**2.7.5.**

Let G be a Gröbner basis of an ideal I with the property that $\mathrm{LT}(g) = 1$ for all $g \in G$. Prove that $\mathrm{LT}(G)$ is a minimal Gröbner basis if and only if no proper subset of G is a Gröbner basis.

Solution. In order to be a minimal Gröbner basis we must have $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle$ for each $p \in G$. So what we want to prove is:

$$\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle \text{ for each } p \in G \Leftrightarrow \text{ no proper subset of } G \text{ is a Gröbner basis for } I.$$

Proof. ($\Rightarrow$): If some $H \overset{\subset}{\neq} G$ is a Gr"obner basis for I, then for each $p \in G - H$ we have $\mathrm{LT}(p) \in \langle \mathrm{LT}(I)\rangle \subset \langle \mathrm{LT}(H)\rangle \subset \langle \mathrm{LT}(G - \{p\})\rangle$ which violates the assumption $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle$ for each $p \in G$.

($\Leftarrow$): No proper subset of G is a Gröbner basis for I. In particular, if $p \in G$, $G - \{p\}$ is not a Gröbner basis for I. This means that $\mathrm{LT}(G - \{p\})$ is not a basis for $\mathrm{LT}(I)$ but $\mathrm{LT}(G - \{p\}) \cup \{\mathrm{LT}(p)\}$ is. The only way this can happen is for $\mathrm{LT}(p) \notin \mathrm{LT}(G - \{p\})$, because if $\mathrm{LT}(p) \in \mathrm{LT}(G - \{p\})$, then $\mathrm{LT}(G) \subset \mathrm{LT}(G - \{p\})$ and $G - \{p\}$ would be a Gröbner basis for I.

---

§**2.7.6.**

Recall the notion of a *minimal* basis for a monomial ideal introduced in Exercise 2.4.8. Namely, a basis $\{x^{\alpha(1)}, \ldots, x^{\alpha(s)}\}$ for a monomial ideal J is *minimal* if no $x^{\alpha(i)}$ divides another $x^{\alpha(j)}$ for $i \neq j$. Show that a Gröbner basis G for I is minimal if and only if (i) $\mathrm{LC}(g) = 1$ for each $g \in G$ and (ii) $\mathrm{LT}(G)$ is a minimal basis of the monomial ideal $\langle \mathrm{LT}(I)\rangle$.

Proof.($\Longrightarrow$): Suppose G is a minimal Gröbner basis for I. Then (i) is satisfied by definition and (a) for each $p \in G$, $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle$. Condition (a) means that no $\mathrm{LT}(G - \{p\})$ divides $\mathrm{LT}(p)$ for $p \in G$. But this last statement is just the statement that $\mathrm{LT}(G)$ is a minimal basis for the monomial ideal $\langle \mathrm{LT}(I)\rangle$ it generates.

($\Longleftarrow$): Suppose (i) and (ii) are satisfied. If $\mathrm{LT}(G)$ is a minimal basis for the monomial ideal $\langle \mathrm{LT}(I)\rangle$, then no $\mathrm{LT}(p)$ divides any $\mathrm{LT}(q)$ for $p \neq q$ in $p, q \in G$. That is, for each $p \in G$, $\mathrm{LT}(p)$ is not divisible by any of the monomials in $\mathrm{LT}(G - \{p\})$. This means, however, that $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle$ and, accordingly, G is a minimal Gröbner basis for the ideal I that it generates. ∎

---

§**2.7.7.**

Fix a monomial order and let G and $\tilde{G}$ be minimal Gröbner bases for the ideal I.

(a) Prove that $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$.

(b) Conclude that G and $\tilde{G}$ have the same number of elements.

Proof. (This is a repetition of an argument we gave above.) Suppose $f \in \mathrm{LT}(G)$. Since f is in the monomial ideal $\langle \mathrm{LT}(\tilde{G})\rangle$, there is an $\tilde{f} \in \mathrm{LT}(\tilde{G})$ with $\mathrm{LT}(f) = g \cdot \mathrm{LT}(\tilde{f})$ for some $g \in k[x_1, \ldots, x_n]$. Similarly, there is an $\hat{f} \in \mathrm{LT}(G)$ whose leading term divides $\mathrm{LT}(\tilde{f})$; so $\mathrm{LT}(\tilde{f}) = h \cdot \mathrm{LT}(\hat{f})$ for some $h \in k[x_1, \ldots, x_n]$. Thus $\mathrm{LT}(f) = c\mathrm{LT}(\hat{f})$ for some $c \in k[x_1, \ldots, x_n]$. If $f \neq \hat{f}$ we have $\mathrm{LT}(f) = c\mathrm{LT}(\hat{f}) \in \langle \mathrm{LT}(G - \{f\})\rangle$ which contradicts the fact that G is a minimal basis; so it must be that $f = \hat{f}$. This means that the two monomials $\mathrm{LT}(f)$ and $\mathrm{LT}(\tilde{f})$ divide each other. Since the associated leading coefficient is 1 in each case (another condition for G and/or $\tilde{G}$ to be minimal), they must be identical. $\mathrm{LT}(f) = \mathrm{LT}(\tilde{f})$. The elements of G and $\tilde{G}$ are then paired and $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$. ∎ In particular, two minimal bases for I have the same number of elements.

---

§**2.7.8.**

Develop an algorithm that produces a reduced Gröbner basis for an ideal I given as input an arbitrary Gröbner basis for I. Prove that your algorithm works.

Solution. Here's the algorithm. Let G be a Gröbner basis for the polynomial ideal I.

1. Delete from G any p for which $\mathrm{LT}(p)$ is divisible by any member of $\mathrm{LT}(G-\{p\})$. Normalize the remaining polynomials so that their leading terms are 1. Call the resulting set of polynomials F. According to Exercise 2.7.6 F is a minimal Gröbner basis for I.

2. Let $F=\{f_1,\ldots,f_s\}$. Now (step 1) replace $f_1\in F$ by $f_1'=\overline{f_1}^{F-\{f_1\}}$ and set $F_1=(F-\{f_1\})\cup\{f_1'\}$. No monomial of f_1' is in $\langle \mathrm{LT}(F_1-\{f_1'\})\rangle$. (step 2) replace $f_2\in F_1$ by $f_2'=\overline{f_2}^{F_1-\{f_2\}}$ and set $F_2=(F_1-\{f_2\})\cup\{f_2'\}$. No monomial of f_i' is in $\langle \mathrm{LT}(F_2-\{f_i'\})\rangle$ for $i=1,2$. Continue in this manner ending up with (step s) replace $f_s\in F_{s-1}$ by $f_s'=\overline{f_s}^{F_{s-1}-\{f_s\}}$ and set $F_s=(F_{s-1}-\{f_s\})\cup\{f_s'\}$. No monomial of f_t' is in $\langle \mathrm{LT}(F_u-\{f_t\})\rangle$ for $t\le s$. Throughout this process the leading terms don't change– $\mathrm{LT}(F)=\mathrm{LT}(F_1)=\cdots=\mathrm{LT}(F_s)$– which means that F_s is a Gröbner basis for $\langle F\rangle$, that is, for I.

---

§2.7.9.

Consider the polynomial ideal I generated by the linear polynomials

$$3x-6y-2z,$$
$$2x-4y+4w,$$
$$x-2y-z-w$$

That is, by the rows of the matrix product

$$\begin{pmatrix}3&-6&-2&0\\2&-4&0&4\\1&-2&-1&-1\end{pmatrix}\begin{pmatrix}x\\y\\z\\w\end{pmatrix}.$$

Use lex order with $x>y>z>w$.

(a) Show that the linear polynomials determined by the row echelon matrix

$$\begin{pmatrix}1&-2&-1&-1\\0&0&1&3\\0&0&0&0\end{pmatrix}\begin{pmatrix}x\\y\\z\\w\end{pmatrix}.$$

give a minimal Gröbner basis $F=\{x-2y-z-w,\ z+3w\}$. Hint: Use Theorem 6 of §2.6.0.

Solution. Let $f_1=x-2y-z-w$, $f_2=z+3w$. Then

$$S(f_1,f_2)=zf_1-xf_2=z(x-2y-z-w)-x(z+3w)=-2zy-z^2-zw-3xw.$$

Dividing $S(f_1,f_2)$ or $-3xw-2yz-z^2-zw$ by $F=(f_1,f_2)$ gives using lex order with $x>y>z>w$,

$x-2y-z-w$	$z+3w$	$-3xw-2yz-z^2-zw$	remainder
$-3w$		$-2yz-6yw-z^2-4zw-3w^2$	
	$-2y$	$-z^2-4zw-3w^2$	
	$-z$	$-zw-3w^2$	
	$-w$	0	

gives

$$-3xw-2yz-z^2-zw=(-3w)(x-2y-z-w)+(-2y-z-w)(z+3w)+0.$$

So the remainder is zero and $F=\{f_1,f_2\}$ is a Gröbner basis. Since f_1 and f_2 are invertible linear combinations of the original basis elements, F is a minimal Gröbner basis for I.

(b) Show that the linear polynomials determined from the reduced row echelon matrix

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}.$$

give the reduced Gröbner basis $G = \{x - 2y + 2w,\ z + 3w\}$ for I.

Solution. This basis can be expressed as invertible linear combinations of the orginal basis for I; so it is clearly a basis for I. It is minimal because no two elements of $\mathrm{LT}(G) = \{x, z\}$ divide each other. It is also clearly reduced because no monomial of any basis element is divisible by a leading term of another basis element. Finally, all leading coefficients are 1.

---

§2.7.10.

Let $A = (a_{ij})$ be an $n \times m$ matrix with entries in k and let $f_i = a_{i1}x_1 + \cdots + a_{im}x_m$ be the linear polynomials in $k[x_1, \ldots, x_m]$ determined by the rows of A. Put $I = \langle f_1, \ldots, f_n \rangle$. Let $B = (b_{ij})$ be the row reduced echelon form of A and let $g_1, \ldots, g_s$ be the linear polynomials doming from the nonzero rows of B (so that $s \leq n$). We want to prove that $\{g_1, \ldots, g_s\}$ is the reduced Gröbner basis for I.

(a) Show that $I = \langle g_1, \ldots, g_s \rangle$.

Solution. If $\mathbf{x}$ is the $m \times 1$ matrix whose entries are the x_i's and $\mathbf{f}$ is the $n \times 1$ matrix whose entries are the f_j's, then $\mathbf{f} = A\mathbf{x}$. There is an invertible $n \times n$ matrix R such that $RA = B$. It follows that $\mathbf{g} = B\mathbf{x} = RA\mathbf{x} = R\mathbf{f}$, where $\mathbf{g}$ is the $n \times 1$ matrix whose entries are the g_j's filled out by setting $g_r = 0$ if $s < r \leq n$. Multiplying $\mathbf{g} = R\mathbf{f}$ on the left by R^{-1} gives $\mathbf{f} = R^{-1}\mathbf{g}$ and shows that the linear polynomial components of $\mathbf{f}$ and $\mathbf{g}$ determine the same polynomial ideal.

(b) Use Theorem 6 of §2.6.0 to show that $g_1, \ldots, g_s$ form a Gröbner basis, which by Exercise 2.7.10.a must then be a Gröbner basis for I.

Solution. We begin by illustrating what goes on here in a special case. Suppose

$$\begin{pmatrix} g_1 \\ g_2 \\ g_3 \end{pmatrix} = \begin{pmatrix} 1 & a_2 & 0 & 0 & a_5 & a_6 \\ 0 & 0 & 1 & 0 & b_5 & b_6 \\ 0 & 0 & 0 & 1 & c_5 & c_6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix},$$

so that $g_1 = x_1 + a_2x_2 + a_5x_5 + a_6x_6$, $g_2 = x_3 + b_5x_5 + b_6x_6$, and $g_3 = x_4 + c_6x_6$. We show that when $S(g_1, g_2)$ is divided by (g_1, g_2, g_3) the remainder is zero. Now

$$S(g_1, g_2) = x_3g_1 - x_1g_3 = -x_1 \cdot b_5x_5 - x_1 \cdot b_6x_6 + a_2x_2 \cdot x_3 + x_3 \cdot a_5x_5 + x_3 \cdot a_6x_6.$$

Using lex order with $x_1 > x_2 > x_3 > x_4 > x_5 > x_6$ we start the division by multiplying g_1 by $-b_5x_5$ and subtracting to get

$$\begin{aligned} &- x_1 \cdot b_5x_5 - x_1 \cdot b_6x_6 + a_2x_2 \cdot x_3 + x_3 \cdot a_5x_5 + x_3 \cdot a_6x_6 \\ &+ x_1 \cdot b_5x_5 + a_2x_2 \cdot b_5x_5 + a_5x_5 \cdot b_5x_5 + b_5x_5 \cdot a_6x_6 \\ &= -x_1 \cdot b_6x_6 + a_2x_2 \cdot x_3 + x_3 \cdot a_5x_5 + x_3 \cdot a_6x_6 + a_2x_2 \cdot b_5x_5 + a_5x_5 \cdot b_5x_5 + b_5x_5 \cdot a_6x_6. \end{aligned}$$

We then multiply g_1 by $-b_6x_6$ and subtract again to get

$$\begin{aligned} &- x_1 \cdot b_6x_6 + a_2x_2 \cdot x_3 + x_3 \cdot a_5x_5 + x_3 \cdot a_6x_6 + a_2x_2 \cdot b_5x_5 + a_5x_5 \cdot b_5x_5 + b_5x_5 \cdot a_6x_6. \\ &+ x_1 \cdot b_6x_6 + a_2x_2 \cdot b_6x_6 + a_5x_5 \cdot b_6x_6 + a_6x_6 \cdot b_6x_6 \\ &= +a_2x_2 \cdot x_3 + x_3 \cdot a_5x_5 + x_3 \cdot a_6x_6 + a_2x_2 \cdot b_5x_5 + a_5x_5 \cdot b_5x_5 + b_5x_5 \cdot a_6x_6. \\ &+ a_2x_2 \cdot b_6x_6 + a_5x_5 \cdot b_6x_6 + a_6x_6 \cdot b_6x_6. \end{aligned}$$

We are now through with the divisor g_1. Next we multiply g_2 by a_2x_2 and subtract to get

$$\begin{aligned}
&+ a_2x_2 \cdot x_3 + x_3 \cdot a_5x_5 + x_3 \cdot a_6x_6 + a_2x_2 \cdot b_5x_5 + a_5x_5 \cdot b_5x_5 + b_5x_5 \cdot a_6x_6.\\
&+ a_2x_2 \cdot b_6x_6 + a_5x_5 \cdot b_6x_6 + a_6x_6 \cdot b_6x_6.\\
&- a_2x_2 \cdot x_3 - a_2x_2 \cdot b_5x_5 - a_2x_2 \cdot b_6x_6\\
&= +x_3 \cdot a_5x_5 + x_3 \cdot a_6x_6 + a_5x_5 \cdot b_5x_5 + b_5x_5 \cdot a_6x_6. + a_5x_5 \cdot b_6x_6 + a_6x_6 \cdot b_6x_6.
\end{aligned}$$

Continuing we multiply g_2 by a_5x_5 and subtract to get

$$\begin{aligned}
&+ x_3 \cdot a_5x_5 + x_3 \cdot a_6x_6 + a_5x_5 \cdot b_5x_5 + b_5x_5 \cdot a_6x_6. + a_5x_5 \cdot b_6x_6 + a_6x_6 \cdot b_6x_6\\
&- x_3 \cdot a_5x_5 - a_5x_5 \cdot b_5x_5 - a_5x_5 \cdot b_6x_6\\
&= +x_3 \cdot a_6x_6 + b_5x_5 \cdot a_6x_6 + a_6x_6 \cdot b_6x_6
\end{aligned}$$

To finish off we multiply g_2 by a_6x_6 and subtract to get a remainder of zero. g_3 never enters the active divisor slot.

Note what happened during the division: g_1 entered the active divisor slot and picked up the terms of $-(g_2 - x_3)$ in its quotient one at a time in their proper lex order. At this stage nothing further was divisible by g_1 and it leaves the active divisor slot which is is then entered by g_2. The quotient of g_2 then picks up the terms of $g_1 - x_1$ one at a time, again in their proper lex order, ending with zero in the dividend. The division yields

$$S(g_1, g_2) = [-(g_2 - x_3)]\, g_1 + [g_1 - x_1]\, g_2 + 0.$$

To continue our illustration we calculate the remainder of $S(g_1, g_3)$ when it is divided by (g_1, g_2, g_3). Here

$$\begin{aligned}
S(g_1, g_3) &= x_5g_1 - x_1g_3 = x_4(x_1 + a_2x_2 + a_5x_5 + a_6x_6) - x_1(x_4 + c_6x_6)\\
&= -x_1 \cdot c_6x_6 + a_2x_2 \cdot x_4 + x_4 \cdot a_5x_5 + x_4 \cdot a_6x_6.
\end{aligned}$$

We begin the division by multiplying g_1 by $-c_6x_6$ and subtracting, getting

$$\begin{aligned}
&- x_1 \cdot c_6x_6 + a_2x_2 \cdot x_4 + x_4 \cdot a_5x_5 + x_4 \cdot a_6x_6.\\
&+ x_1 \cdot c_6x_6 + a_2x_2 \cdot c_6x_6 + a_5x_5 \cdot c_6x_6 + a_6x_6 \cdot c_6x_6\\
&= +a_2x_2 \cdot x_4 + x_4 \cdot a_5x_5 + x_4 \cdot a_6x_6 + a_2x_2 \cdot c_6x_6 + a_5x_5 \cdot c_6x_6 + a_6x_6 \cdot c_6x_6
\end{aligned}$$

At this stage g_1 leaves the active divisor slot. The leading term of g_2 won't divide any monomial here; so we pass on and g_3 enters the active divisor slot. Multiplying g_3 by a_2x_2 and subtracting gives

$$\begin{aligned}
&+ a_2x_2 \cdot x_4 + x_4 \cdot a_5x_5 + x_4 \cdot a_6x_6 + a_2x_2 \cdot c_6x_6 + a_5x_5 \cdot c_6x_6 + a_6x_6 \cdot c_6x_6\\
&- a_2x_2 \cdot x_4 - a_2x_2 \cdot c_6x_6\\
&= +x_4 \cdot a_5x_5 + x_4 \cdot a_6x_6 + a_5x_5 \cdot c_6x_6 + a_6x_6 \cdot c_6x_6.
\end{aligned}$$

Multiplying g_3 by a_5x_5 and subtracting then gives

$$+x_4 \cdot a_6x_6 + a_6x_6 \cdot c_6x_6.$$

Finally, multiplying g_3 by a_6x_6 and subtracting gives the remainder as zero. Note that g_2 didn't play any active role in this division.

Here again note what happened during the division: g_1 entered the active divisor slot and picked up the terms of $-(g_3 - x_4)$ in its quotient one at a time in the proper lex order. At this stage nothing further was divisible by g_1 and it leaves the active divisor slot which is is then entered by g_3. The quotient of g_3 then picks up the terms of $g_1 - x_1$ one at a time, again in the proper lex order, ending with zero in the dividend. The division yields

$$S(g_1, g_3) = [-(g_3 - x_4)]\, g_1 + [g_1 - x_1]\, g_3 + 0.$$

Without saying much more, I'd like to make an appeal that this is what always happens. The notes at the end of each division describe the pattern and the reader just has to recognize that in fact this is what happens.

If we accept this, it is clear that $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I.

(c) Explain why $\{g_1, \ldots, g_s\}$ is the reduced Gröbner basis.

Solution. We know it is a Gröbner basis. The leading coefficients are 1's. Now let $\{1, \ldots, m\} = P \cup Q$ where $\{x_j : j \in P\} = \mathrm{LT}(\{g_1, \ldots, g_s\})$ and $\{x_j : j \in Q\}$ consists of the monomials which are never leading terms of a g_i. Then each g_i has the form $g_i = x_{\ell_i} + \sum_{j \in Q} a_j x_j$, with $\mathrm{LT}(g_i) = x_{\ell_i}$ Now for each $i \leq s$ no monomial of g_i is divisible by any monomial in $\mathrm{LT}(\{g_1, \ldots, g_s\} - \{g_i\})$ so no monomial of g_i lies in $\langle \mathrm{LT}(\{g_1, \ldots, g_s\} - \{g_i\}) \rangle$. This shows $\{g_1, \ldots, g_s\}$ meets the conditions recquired to be a Gröbner basis for I.

---

§**2.7.11.**

Show that the result of applying the Euclidean Algorithm in $k[x]$ to any pair of polynomials f, g is (after normalization) a reduced Gröbner basis for $\langle , f, g \rangle$. That is, show that if q is the greatest common divisor of f and g, then $\{q\}$ is a reduced Gröbner basis for $\langle , f, g \rangle$.

Solution. First it is well known that $\{q\}$ is a basis for $\langle , f, g \rangle$. If the leading coefficient is 1, as it will be after normalization, then as a singleton basis it is always true that no monomial of q is in $\mathrm{LT}(\{q\} - \{q\}) = \emptyset$.
