Chapter 2 §6. Properties of Gröbner Bases. Remember that $\{g_1, \ldots, g_s\}$ is a Gröbner basis for the ideal $I \subset k[x_1, \ldots, x_n]$ if and only if $\{g_1, \ldots, g_s\} \subset I$ and

$$\langle cx^\alpha \colon cx^\alpha \text{ is a leading term of some } f \in I \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle. \tag{2.6.0.1}$$

(2.6.0.1) can be replaced by: Every $\mathrm{LT}(f)$ for $f \in I$ is divisible by one of the $\mathrm{LT}(g_i)$'s.

The following lists the key property of a Gröbner basis.

Proposition 2.6.0.2. (Proposition 1) Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for an ideal $I \subset k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then there is a unique $r \in k[x_1, \ldots, x_n]$ with the following properties:

(i) No term of r is divisible by any of the $\mathrm{LT}(g_i)$'s.
(ii) There is a $g \in I$ such that $f = g + r$.

In particular, r is the remainder on division of f by G no matter how the elements of G are listed in using the division algorithm.

Proof. The division algorithm gives $f = a_1 g_1 + \cdots + a_s g_s + r$ with two properties: (i) no term of r is divisible by any of the $\mathrm{LT}(g_i)$'s, $1 \leq i \leq s$, and (ii) $\mathrm{multidegree}(a_i g_i) \leq \mathrm{multidegree}(f)$, $1 \leq i \leq s$. Once G has been ordered and this division has been carried out, $g = a_1 g_1 + \cdots + a_s g_s \in I$. It remains to establish uniqueness.

Suppose $f = g_1 + r_1 = g_2 + r_2$ are two such expressions. Then $w = r_1 - r_2 = g_2 - g_1 \in I$. The leading term of w is not divisible by any of the $\mathrm{LT}(g_i)$'s. But since $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I, $\mathrm{LT}(w) \in \mathrm{LT}(I) \subset \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. This last is a monomial ideal and as such the leading term of any of its members is divisible by at least one of the monomial generators $\mathrm{LT}(g_i)$. The only possibility is that the leading term of w is zero which forces $w = 0$. The uniqueness is established. ∎

The remainder r is sometimes called the *normal form* of f. It is a fact although we won't dwell on it that Gröbner bases are the only bases for which the remainder r is unique for each $f \in I$. Although the remainder r doesn't depend on the order of the divisors, the quotients do, in general, depend on this order.

Corollary 2.6.0.3. (Corollary 2) Let G be a Gröbner basis for the ideal $I \subset k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then $f \in I \Leftrightarrow$ the remainder on dividing f by G is zero.

No proof is required as this follows trivially from Proposition 2.6.0.2.

Remark. The property detailed in corollary 2.6.0.3 is sometimes taken as the definition of a Gröbner basis. It is equivalent to the one given at the beginning of this section.

Definition 2.6.0.4. (Definition 3.) We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$. If F is a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$, we can regard F as a set (without any particular order) by the observation before the proof of Proposition 2.6.0.2.

Definition 2.6.0.5. (Definition 4) Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials.

(i) The *least common multiple* of x^α and x^β is $x^{\alpha \vee \beta}$.

(ii) If $\mathrm{LT}(f) = cx^\alpha \neq 0$ and $\mathrm{LT}(g) = dx^\beta \neq 0$, then the *S-polynomial* of f and g is the combination

$$S(f, g) = \frac{x^{\alpha \vee \beta}}{cx^\alpha} \cdot f - \frac{x^{\alpha \vee \beta}}{dx^\beta} \cdot g. \tag{2.6.0.6}$$

Key Remark (2.6.0.6a). $\mathrm{multidegree}(S(f, g)) < \max\{\mathrm{multidegree}(f), \mathrm{multidegree}(g)\}$.

Lemma 2.6.0.7. (Lemma 5) Suppose $f_i = d_i x^\delta + h_i$, $1 \leq i \leq s$, where for each i, $1 \leq i \leq s$, $d_i \in k$, $h_i \in k[x_1, \ldots, x_n]$ and $d_i x^\delta$ is the leading term of f_i. Suppose each $c_i \in k$ and

$$\mathrm{multideg}\left(\sum_{i=1}^{s} c_i f_i \right) < \delta. \tag{2.6.0.8}$$

Then $\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s-1} a_i S(f_i, f_{i+1})$ for some choice of $a_i \in k$, $1 \leq i \leq s - 1$. Furthermore, each $S(f_i, f_j)$ has multidegree $< \delta$.

Proof. □(2.6.0.8) states that $\left(\sum_{i=1}^{s} c_i d_i\right) x^\delta + \left(\sum_{i=1}^{s} c_i h_i\right)$ has multidegree $< \delta$. It is clear that the mulidegree of $\sum_{i=1}^{s} c_i h_i$ is less than δ; so we must have

$$\sum_{i=1}^{s} c_i d_i = 0. \tag{2.6.0.9}$$

Let $p_i = \frac{f_i}{d_i} = x^\delta + \frac{1}{d_i} h_i$. Then

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) \\ &+ (c_1 d_1 + c_2 d_2)(p_2 - p_3) \\ &+ (c_1 d_1 + c_2 d_2 + c_3 d_3)(p_3 - p_4) \\ &+ (c_1 d_1 + c_2 d_2 + c_3 d_3 + c_4 d_4)(p_4 - p_5) + \cdots \\ &+ (c_1 d_1 + c_2 d_2 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) \\ &+ (\sum_{i=1}^{s} c_i d_i) p_s.\end{aligned}$$

Use the fact that

$$p_i - p_{i+1} = \frac{1}{d_i} h_i - \frac{1}{d_{i+1}} h_{i+1} = \frac{x^{\delta \vee \delta}}{d_i x^\delta} h_i - \frac{x^{\delta \vee \delta}}{d_{i+1} x^\delta} h_{i+1} = S(f_i, f_{i+1})$$

and (2.6.0.9) to conclude that

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s-1} \left(\sum_{j=1}^{i} c_j d_j \right) S(f_i, f_{i+1}). \tag{2.6.0.10}$$

The last assertion of the lemma is a consequence of Key Remark (2.6.0.6a). ■

What follows is the main result of this section:

Theorem 2.6.0.11. (Theorem 6.) Let I be a polynomial ideal with basis $B = \{g_1, \ldots, g_s\}$. B is a Gröbner basis for $I \iff$ For each pair $i \neq j$, there is an ordering G_{ij} of $\{g_1, \ldots, g_s\}$ such that $\overline{S(g_i, g_j)}^{G_{ij}} = 0$.

Proof. □($\Longrightarrow$): The $S(g_i, g_j) \in I$; so if G is an (ordered) Gröbner basis the division of $S(g_i, g_j)$ by G is zero by corollary 2.6.0.3.

($\Longleftarrow$): Let $f \in I$ be nonzero. We must show that $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Since G is a basis for I there is an expression of the form

$$f = h_1 g_1 + \cdots + h_s g_s, \qquad \text{where each } h_i \in k[x_1, \ldots, x_n]. \tag{2.6.0.12}$$

Let $\delta = \max\{\text{multideg}(h_i g_i) \colon 1 \leq i \leq s\}$. Clearly, $\text{multideg}(f) \leq \delta$.

Case I: ($\text{multideg}(f) = \delta$). In this case, for at least one value of i, $\text{multideg}(h_i g_i) = \delta = \text{multideg}(f)$, and $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_i)$; so $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. When this is true for an arbitrary $f \in I$, $\{g_1, \ldots, g_s\}$ a Gröbner basis for I. The remainder of the proof rests on the following contention:

Contention. There is always an expression of the form (2.6.0.12) for which $\text{multideg}(f) = \delta$.

Proof of contention. Let the h_i's be chosen so that δ is a minimum and suppose multideg$(f) < \delta$. (The proof is by contradiction.) Assume that of all possible expressions of the form

$$f = \sum_{i=1}^{s} h_i g_i \qquad \text{with } h_i \in k[\mathbf{x}], \tag{0.1}$$

(0.1) is one of those for which $\delta = \max \text{multidegree}(h_i g_i)$, $1 \leq i \leq s$ is minimal, and that, for this δ, multidegree$(f)< \delta$. Write f as (Here and in what follows "*md*" is an abbreviation for "multidegree".)

$$\begin{aligned} f &= \sum_{md(i)=\delta} h_i g_i + \sum_{md(i)<\delta} h(i) g_i \\ &= \sum_{md(i)=\delta} LT(h_i) g_i + \sum_{md(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{md(i)<\delta} h(i) g_i. \end{aligned} \tag{0.2}$$

Without loss of generality we can assume that (a) $\{i\colon md(i) = \delta\} = \{i\colon 1 \leq i \leq m\}$ for some integer m, $1 \leq m \leq s$, and (b) that $md(g_i) \leq md(g_{i+1})$, $1 \leq i < m$. Since f and the terms of the second and third summands of (0.2) have multidegrees $< \delta$, it follows that
$\sum_{md(i)=\delta} LT(h_i) g_i$ has multidegree $< \delta$ too. To be more specific: Let $LT(h_i) = c_i \mathbf{x}^{\alpha(i)}$, for those i's with $md(h_i g_i)) = \delta$. Then the "first summand" of (0.2) is $\sum_{md(i)=\delta} c_i x^{\alpha(i)} g_i$ or $\sum_{i=1}^{m} c_i x^{\alpha(i)} g_i$, with our new numbering. This "first summand" satisfies the hypothesis of Lemma (2.6.0.7) and it follows that this sum is a linear combination of the S-polynomials $S(\mathbf{x}^{\alpha(i)} g_i, \mathbf{x}^{\alpha(i+1)} g_{i+1})$, where $1 \leq i < m$. That is,

$$\sum_{md(i)=\delta} LT(h_i) g_i = \sum_{i=1}^{m} c_i x^{\alpha(i)} g_i = \sum_{i=1}^{m-1} a_i S(\mathbf{x}^{\alpha(i)} g_i, \mathbf{x}^{\alpha(i+1)} g_{i+1}) \qquad \text{for some } a_i \in k. \tag{A.1}$$

Note that $\mathbf{x}^{\alpha(i)} g_i$ and $\mathbf{x}^{\alpha(i+1)} g_{i+1}$ both have multidegree δ; so since $md(g_i) \leq md(g_{i+1})$, $\alpha(i) \geq \alpha(i+1)$, $1 \leq i < m$, and $\mathbf{x}^{\alpha(i)-\alpha(i+1)} g_i$ and g_{i+1} have the same multidegree. This observation leads directly to

$$\begin{aligned} S(\mathbf{x}^{\alpha(i)} g_i, \mathbf{x}^{\alpha(i+1)} g_{i+1}) &= \frac{\mathbf{x}^{\alpha(i)} g_i}{\mathrm{LC}(g_i)} - \frac{\mathbf{x}^{\alpha(i+1)} g_{i+1}}{\mathrm{LC}(g_{i+1})} \\ &= \mathbf{x}^{\alpha(i+1)} \left(\frac{\mathbf{x}^{\alpha(i)-\alpha(i+1)} g_i}{\mathrm{LC}(g_i)} - \frac{g_{i+1}}{\mathrm{LC}(g_{i+1})} \right) \\ &= \mathbf{x}^{\alpha(i+1)} S(g_i, g_{i+1}). \end{aligned} \tag{A.2}$$

(A.1) then becomes

$$\sum_{md(i)=\delta} LT(h_i) g_i = \sum_{i=1}^{m-1} a_i \mathbf{x}^{\alpha(i+1)} S(g_i, g_{i+1}), \qquad a_i \in k,\ 1 \leq i < m. \tag{A.3}$$

We now use the division algorithm and the fact that the remainder is zero when we divide $S(g_i, g_{i+1})$ by G_{ij}, i.e. $\{(g_1, \ldots, g_s\}$ taken in the order G_{ij}, to find $B_i^\ell \in k[\mathbf{x}]$, satisfying

$$S(g_i, g_{i+1}) = \sum_{\ell=1}^{s} B_i^\ell g_\ell, \qquad B_i^\ell \in k[\mathbf{x}],\ \text{multidegree}(B_i^\ell g_\ell) < \text{multidegree}(g_{i+1}) = \delta - \alpha(i+1). \tag{A.4}$$

Now putting these together, the "first summand" has an expression

$$\sum_{md(i)=\delta} LT(h_i) g_i = \sum_{i=1}^{m-1} \sum_{\ell=1}^{s} a_i \mathbf{x}^{\alpha(i+1)} B_i^\ell g_\ell = \sum_{\ell=1}^{s} \left(\sum_{i=1}^{m-1} a_i \mathbf{x}^{\alpha(i+1)} B_i^\ell \right) g_\ell$$

of the form $H_1 g_1 + \cdots + H_s g_s$ where for each t, $1 \leq t \leq s$, multidegree$(H_t g_t) < \delta$. Adding to this sum the second and third sums of (0.2) we can express f as a sum $F_1 g_1 + \cdots + F_s g_s$ in which each summand has multidegree $< \delta$. This contradicts the minimality of δ and shows that Case I is really the only case that can occur. ∎

Theorem 2.6.0.11 (Theorem 6.) is sometimes called "Buchberger's S-pair criterion".

Exercises for Chapter 2 §6

$\boxed{\S\mathbf{2.6.1.}}$

Show that Proposition 1 can be strengthened slightly as follows. Fix a monomial ordering and let $I \in k[x_1, \ldots, x_n]$ be an ideal. Suppose that $f \in k[x_1, \ldots, x_n]$.

(a) Show that f can be written in the form $f = g + r$, where $g \in I$ and no term of r is divisible by any element of $\mathrm{LT}(I)$.

Solution. Choose a Gröbner basis $\{g_1, \ldots, g_s\}$ for I. Then since $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$ and these are monomial ideals, saying no term of r is divisible by any element of $\mathrm{LT}(I)$ is the same as saying no term of r is divisible by any of the $\mathrm{LT}(g_i)$'s. Now divide f by $(g_1, \ldots, g_s$ to get an expression $f = q_1g_1 + \cdots + q_sg_s + r$ where no term of r is divisible by any element of $\mathrm{LT}(I)$. Furthermore putting $g = q_1g_1 + \cdots + q_sg_s \in I$ we have $f = g + r$.

(b) Given two expressions $f = g + r = g' + r'$ as in part (a), prove that $r = r'$. Thus r and g are uniquely determined.

Solution. If $f = g + r = g' + r'$, then $r - r' = g' - g$. Now the leading term of $w = r - r'$ is either zero or it is not divisible by any $\mathrm{LT}(f)$, $f \in I$. But $r - r' = g - g' \in I$ and the leading term of any element w of I is divisible by $\mathrm{LT}(w)$ itself. The only possiblity is that $w = 0$.

This result shows once a monomial order is fixed, we can define a unique "remainder of f on division by I"

$\boxed{\S\mathbf{2.6.2.}}$

In §2.5 we showed that $G = \{x + z,\ y - z\}$ is a Gröbner basis for lex order. Let us use this basis to study the uniqueness of the division algorithm.

(a) Divide xy by $(x + z,\ y - z)$.

Solution.

$xy^2 - x$	$-y^3 + x$	$x^7y^2 + x^3y^2 - y + 1$	remainder
x^6		$x^7 + x^3y^2 - y + 1$	
		$x^3y^2 - y + 1$	x^7
x^2		$x^3 - y + 1$	
		$-y + 1$	x^3
		$+1$	$-y$
			$+1$

gives

$$x^7y^2 + x^3y^2 - y + 1 = (x^6 + x^2)(xy^2 - x) + (x^7 + x^3 - y + 1)$$

Mathematica 3.01. The command

PolynomialReduce[x^7*y^2+x^3*y^2-y+1, {x*y^2-x,y-y^3},{x,y},
MonomialOrder->DegreeLexicographic]

Produces the output

$$\mathrm{Out}[1] = \{\{x^2 + x^6,\ 0\},\ 1 + x^3 + x^7 - y\}$$

Then using lex order,

$x+z$	$y-z$	xy	remainder
y		$-yz$	
	$-z$	$-z^2$	
			$-z^2$

We get $xy = y(x+z) - z(y-z) - z^2$

(b) Now reverse the order and divide xy by $(y-z,\, x+z)$

Solution.

$y-z$	$x+z$	xy	remainder
x		xz	
	z	$-z^2$	
			$-z^2$

Here we get $xy = x(y-z) + z(x+z) - z^2$. Comparing this with $xy = y(x+z) - z(y-z) - z^2$ we see immediately that the remainders are the same, as we know they must be, but the individual quotients differ. The sums $x(y-z) + z(x+z) = y(x+z) - z(y-z) = xy + z^2$ are the same of course.

$\boxed{\S\mathbf{2.6.3.}}$

In Corollary 2, we showed that if $I = \langle g_1, \ldots, g_s \rangle$ and if $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for I, then $\overline{f}^G = 0$ for all $f \in I$. Prove the converse of this statement. Namely show that if G is a basis for I with the property that $\overline{f}^G = 0$ for all $f \in I$, then G is a Gröbner basis for I.

Solution. The fact that $\overline{f}^G = 0$, the leading term of f is divisible by one of the $\mathrm{LT}(g_i$'s or $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Since this is true for each $f \in I$ we have $\mathrm{LT}(I) \subset \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. As the g_i's themselves belong to I, $\mathrm{LT}(I) \supset \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. This gives $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$ and shows that $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I.

$\boxed{\S\mathbf{2.6.4.}}$

Let G and G' be Gröbner bases for an ideal I with respect to the same monomial order in $k[x_1, \ldots, x_n]$. Show that $\overline{f}^G = \overline{f}^{G'}$ for all $f \in k[x_1, \ldots, x_n]$. Hence the remainder on division by a Gröbner basis is even independent of which Gröbner basis we use, as long as we use one particular monomial order. Hint: Soo Exercise 2.6.1.

Solution. We have shown that for a fixed monomial order the decomposition $f = g + r$ where $g \in I$ and no term of r is divisible by any element of $\mathrm{LT}(I)$ in Exercise 2.6.1 There was no mention of a specific Gröbner basis in this decomposition; so we can safely infer that it is independent of the basis used to get the decomposition (if, in fact, a basis was used).

$\boxed{\S\mathbf{2.6.5.}}$

Compute $S(f,g)$ using the lex order.

(a) $f = 4x^2z - 7y^2$, $g = xyz^2 + 3xz^4$.

Solution.

$$S(f,g) = \frac{1}{4} \cdot yz(4x^2z - 7y^2) - \frac{1}{3} \cdot x(xyz^2 + 3xz^4) = -\frac{7}{4}y^4z - x^2z^4.$$

(b) $f = x^4y - z^2$, $g = 3xz^2 - y$.

Solution.
$$S(f,g) = z^2(x^4y - z^2) - \frac{1}{3} \cdot x^3y(3xz^2 - y) = -z^4 + \frac{1}{3}x^3y^2.$$

(c) $f = x^7y^2z + 2ixyz$, $g = 2x^7y^2z + 4$.

Solution.
$$S(f,g) = x^7y^2z + 2ixyz - \frac{1}{2}(2x^7y^2z + 4) = 2ixyz - 2.$$

(d) $f = xy + z^3$, $g = z^2 - 3z$.

Solution.
$$S(f,g) = z^2(xy + z^3) - xy(z^2 - 3z) = 3xyz + z^5.$$

$\boxed{\S\mathbf{2.6.6.}}$

Does $s(f,g)$ depend on which monomial order is used? Illustrate your assertions with examples

Solution. Let $f = x$, $g = x + y^2$. Then using lex order

$$S_{lex}(f,g) = x - (x + y^2) = -y^2.$$

Using grlex order g would more naturally be written as $g = y^2 + x$ and

$$S_{grlex}(f,g) = y^2(x) - x(y^2 + x) = -x^2.$$

So the answer to the first question is: Yes.

$\boxed{\S\mathbf{2.6.7.}}$

Prove that $\text{multideg}(S(f,g)) < \gamma$, where $x^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$. Explain why this inequality is a precise version of the claim that S-polynomials are designed to produce cancellation.

Solution. If $f = ax^\alpha + h_f$ and $g = bx^\beta + h_g$ where $\text{multideg}(h_f) < \alpha$ and $\text{multideg}(h_g) < \beta$, then $\gamma = \alpha \vee \beta$ both $\frac{x^{\alpha\vee\beta}}{x^\alpha}h_f$ and $\frac{x^{\alpha\vee\beta}}{x^\alpha}h_g$ have multidegree $< \alpha \vee \beta = \gamma$; so $S(f,g)$ which is a k-linear combination of these last two mentioned polynomials has multidegree $< \alpha \vee \beta = \gamma$.

For the moment I'll pass on the explanation called for in the last sentence of the exercise.

$\boxed{\S\mathbf{2.6.8.}}$

Show that $\{y - x^2,\, z - x^3\}$ is not a Gröbner basis for lex order with $x > y > z$.

Solution. $xy - z \in I$ but its leading term xy is not divisible by either $-x^2$ or $-x^3$, the leading terms of the basis elements in the lex order. Thus

$$xy \in \langle \text{LT}(I) \rangle \not\subset \langle \text{LT}(y - x^2),\, \text{LT}(z - x^3) \rangle = \langle -x^2,\, -x^3 \rangle.$$

$\boxed{\S\mathbf{2.6.9.}}$

Using Theorem 6, determine whether the following sets G are Gröbner bases for the ideal they generate. You may use a computer algebra system to compute the S-polynomials and remainders.

(a) $G = \{x^2 - y,\, x^3 - z\}$ grlex order.

Solution. $S(x^2 - y, x^3 - z) = -xy + z$ which is not divisible by the leading terms x^2 and x^3; so this G is not a Gröbner basis for I.

(b) $G = \{x^2 - y,\, x^3 - z\}$ invlex order (see Exercise 2.2.6).

Solution. invlex order is just lex order with the variables in the order $z > y > x$. Thus in invlex order we would write the polynomials of G as $G = \{-y + x^2,\ -z + x^3\}$. Here $S_{invlex}(-z + x^3, -y + x^2) = y(-z + x^3) - z(-y + x^2) = -zx^2 + yx^3$. Using Mathematica 3.0, the command:
PolynomialReduce[-z*x^2+y*x^3,{-y+x^2,-z+x^3},{z,y,x}, **MonomialOrder->Lexicographic**]
gives $\{\{-x^3, x^2\}, 0\}$ which is interpreted as

$$-zx^2 + yx^3 = x^2(-z + x^3) - x^3(-y + x^2) + 0.$$

This shows that indeed $G = \{x^2 - y,\ x^3 - z\}$ is a Gröbner basis in the invlex order.

(c) $G = \{xy^2 - xz + y,\ xy - z^2,\ x - yz^4\}$ lex order.

Solution.

$$\begin{aligned} S(xy^2 - xz + y, xy - z^2) &= (xy^2 - xz + y) - y(xy - z^2) = -xz + yz^2 + y; \\ S(xy^2 - xz + y, x - yz^4) &= (xy^2 - xz + y) - y^2(x - yz^4) = -xz + y^3z^4 + y; \\ S(xy - z^2, x - yz^4) &= (xy - z^2) - y(x - yz^4) = y^2z^4 - z^2. \end{aligned}$$

Dividing $S(xy^2 - xz + y, xy - z^2) = -xz + yz^2 + y$ by $G = (xy^2 - xz + y,\ xy - z^2,\ x - yz^4)$ yields

$$-xz + yz^2 + y = (-z)(x - yz^4) + y + yz^2 - yz^5;$$

so from this first division alone it follows that G is not a Gröbner basis.

$\boxed{\S\mathbf{2.6.10.}}$

Let $f, g \in k[x_1, \ldots, x_n]$ be polynomials such that $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ are *relatively prime* monomials and $\mathrm{LC}(f) = \mathrm{LC}(g) = 1$.

(a) Show that $S(f, g) = -(g - \mathrm{LT}(g))f + (f - \mathrm{LT}(f))g$.

Solution. Suppose $f = x^\alpha + (f - \mathrm{LT}(f))$ and $g = x^\beta + (g - \mathrm{LT}(g))$ and that $\alpha \wedge \beta = 0$. Then

$$\begin{aligned} S(f, g) &= x^\beta \left(x^\alpha + (f - \mathrm{LT}(f))\right) - x^\alpha \left(x^\beta + (g - \mathrm{LT}(g))\right) \\ &= x^\beta(f - \mathrm{LT}(f)) - x^\alpha(g - \mathrm{LT}(g)) \\ &= (f - \mathrm{LT}(f))\left(g - (g - \mathrm{LT}(g))\right) - (g - \mathrm{LT}(g))\left(f - (f - \mathrm{LT}(f))\right) \\ &= (f - \mathrm{LT}(f))g - (g - \mathrm{LT}(g))f \end{aligned}$$

(b) Deduce that the leading monomial of $S(f, g)$ is a multiple of either $\mathrm{LM}(f)$ or $\mathrm{LM}(g)$ in this case.

Solution. Let α' be the leading exponent of $f - \mathrm{LT}(f)$ and β' the leading exponent of $g - \mathrm{LT}(g)$. The leading exponent of $(f - \mathrm{LT}(f))g$ is $\alpha' + \beta$ and the leading exponent of $(g - \mathrm{LT}(g))f$ is $\alpha + \beta'$; so to complete the argument for (b) it suffices to show that these leading terms couldn't cancel, that is, that $\alpha + \beta' \neq \beta + \alpha'$. Phrased in another manner: The conditions $\alpha + \beta' = \beta + \alpha'$; $\alpha \wedge \beta = 0$; $\beta' < \beta$; $\alpha' < \alpha$ are contradictory. At the moment I haven't found an argument for this; so we'll leave it.

$\boxed{\S\mathbf{2.6.11.}}$

Let $f, g \in k[x_1, \ldots, x_n]$ and x^α, x^β be monomials. Verify that

$$S(x^\alpha f, x^\beta g) = x^\gamma S(f, g)$$

where

$$x^\gamma = \frac{\mathrm{LCM}\left(x^\alpha \mathrm{LM}(f),\ x^\beta \mathrm{LM}(g)\right)}{\mathrm{LCM}\left(\mathrm{LM}(f),\ \mathrm{LM}(g)\right)}.$$

Be sure to prove that x^γ is a monomial.

Solution. Suppose that $f = a_f x^{m_f} + f - \mathrm{LT}(f)$ and $g = a_g x^{m_g} + g - \mathrm{LT}(g)$. Then

$$\begin{aligned} x^\alpha f &= a_f x^{m_f+\alpha} + x^\alpha \left(f - \mathrm{LT}(f)\right); \\ x^\beta g &= a_g x^{m_g+\beta} + x^\beta \left(g - \mathrm{LT}(g)\right); \end{aligned}$$

and

$$\begin{aligned} S(x^\alpha f, x^\beta g) &= \frac{x^{(m_f+\alpha)\vee(m_g+\beta)}}{a_f x^{m_f+\alpha}} \cdot x^\alpha \left(f - \mathrm{LT}(f)\right) - \frac{x^{(m_f+\alpha)\vee(m_g+\beta)}}{a_g x^{m_g+\beta}} \cdot x^\beta \left(g - \mathrm{LT}(g)\right) \\ &= \frac{x^{(m_f+\alpha)\vee(m_g+\beta)}}{x^{m_f\vee m_g}} \cdot \left(\frac{x^{m_f\vee m_g}}{a_f x^{m_f}} \cdot \left(f - \mathrm{LT}(f)\right) - \frac{x^{m_f\vee m_g}}{a_g x^{m_g}} \left(g - \mathrm{LT}(g)\right)\right) \\ &= x^\gamma \cdot S(f,g). \end{aligned}$$

$\boxed{\S\textbf{2.6.12.}}$

Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let G be a Gröbner basis of I.

(a) Show that $\overline{f}^G = \overline{g}^G$ if and only if $f - g \in I$. Hint: See Exercise 2.6.1.

(b) Deduce that $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$. Hint: Use part (a).

(c) Deduce that $\overline{fg}^G = \overline{\overline{f}^G \cdot \overline{g}^G}^G$.

We will return to an interesting consequence of these facts in Chapter 5.

Solution. Consider the homomorphism $f \mapsto f + I$ of $k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/I$. Since $f + I = \overline{f}^G + I$, $\overline{f}^G$ is a representative of the coset $f + I$ under this homomorphism. It is the unique representative with the property that none of its terms are divisible by the leading terms $\mathrm{LT}(g_i)$ of the Gröbner basis G. Once this has been observed properties (a), (b) and (c) follow from the fact that $f \mapsto f + I$ is a homomorphism.