§**1. Monomial Orderings and Division of Polynomials.** An monomial ordering or ordering of the monomials $x^\alpha, \alpha \in \mathbb{Z}^n_\geq$ is a well ordering $>$ of the set $\mathbb{Z}^n_\geq$ which is stable under addition, i.e. $\alpha > \beta$ implies $\alpha + \gamma > \beta + \gamma$. Each such monomial order arises from a matrix $M = \left\{a_i^j\right\}$, $1 \leq j \leq n$, $1 \leq i \leq t \leq n$, with $a_i^j \in \mathbb{R}$, in the following manner: Let $\ell_i(\alpha) = a_i^1\alpha_1 + \cdots + a_i^n\alpha_n$, $1 \leq i \leq t$. Then $\alpha > \beta$ if and only if for some $1 \leq u \leq t$,

$$\begin{aligned} \ell_1(\alpha) &= \ell_1(\beta), \\ &\vdots \\ \ell_{u-1}(\alpha) &= \ell_{u-1}(\beta), \\ \ell_u(\alpha) &> \ell_u(\beta). \end{aligned}$$

Given a monomial order on $\mathbb{Z}^n_\geq$, if $f \in k[x_1, \ldots, x_n]$, the *leading term* of f, denoted by $\mathrm{LT}(f)$ or $\mathrm{LT}_>(f)$, is defined in the usual manner. It is possible to implement a division algorithm (generally in several ways) with the following properties:

- the dividend is a polynomial $f \in k[x_1, \ldots, x_n]$;
- the divisor is an m-tuple $(d_1, \ldots, d_m) \in (k[x_1, \ldots, x_n])^m$;
- the result is a relation $f = q_1d_1 + \cdots + q_md_m + r$, where
  (i) $\mathrm{multidegree}(q_id_i) \leq \mathrm{multidagree}(f)$, $1 \leq i \leq m$, and either
  (ii) $r = 0$ or
  (iii) no monomial in r is divisible by any of the leading terms $\mathrm{LT}(d_1), \ldots, \mathrm{LT}(d_m)$.
- If $\mathrm{LT}(d_i)$ divides $\mathrm{LT}(d_j)$ for some $i < j$, then $q_j = 0$ and the result $f = q_1d_1 + \cdots + q_md_m + r$ is unchanged if d_j is removed from the sequence of divisors. In particular, r is unchanged.

The polynomial $r \in k[x_1, \ldots, x_n]$ is called the *remainder* and the polynomials $q_i \in k[x_1, \ldots, x_n]$ are the quotients. In general neither the remainder nor the quotients are unique even when the order $(d_1, \ldots, d_m)$ of the divisors is prescribed.

An Implementation of Division. Given $(d_1, \ldots, d_m)$ start with $\mathit{dividend} = f$, $q_1 = 0, \ldots, q_m = 0$, and $r = 0$, and

REPEAT

CASE: There is a smallest i, $1 \leq i \leq m$, with $a_i \cdot \mathrm{LT}(d_i) = \mathrm{LT}(\mathit{dividend})$. In this case make the changes $\mathit{dividend} \longrightarrow \mathit{dividend} - a_id_i$;

$q_i \longrightarrow q_i + a_i$.

CASE: There is no i, $1 \leq i \leq m$, for which $\mathrm{LT}(d_i)$ divides $\mathrm{LT}(\mathit{dividend})$. In this case make the changes $\mathit{dividend} \longrightarrow \mathit{dividend} - \mathrm{LT}(\mathit{dividend})$;

$r \longrightarrow r + \mathrm{LT}(\mathit{dividend})$.

UNTIL: $\mathit{dividend} = 0$.

§**2. Monomial Ideals and Dickson's Lemma.** An ideal $\mathbf{I} \in k[x_1, \ldots, x_n]$ is a *monomial ideal* if it can be generated by a set $\{x^\alpha, \alpha \in A\}$ of monomials. That is, if $\mathbf{I} = \langle x^\alpha, \alpha \in A\rangle$, for some $A \subset \mathbb{Z}^n_\geq$. A polynomial g is in the monomial ideal $\mathbf{I} = \langle x^\alpha, \alpha \in A\rangle$ if and only if each monomial in g is divisible by some x^α, $\alpha \in A$. This is especially true when $g = x^\beta$ is itself a monomial. That is,
($\star$): $\boxed{x^\beta \in \langle x^\alpha, \alpha \in A\rangle \Leftrightarrow x^\beta \text{ is divisible by some } x^\alpha,\ \alpha \in A}$.

Dickson's Lemma. A monomial ideal $\langle x^\alpha, \alpha \in A\rangle$ has a finite generating set. More particularly, there is a finite subset $A_0 \subset A$ with $\langle x^\alpha, \alpha \in A_0\rangle = \langle x^\alpha, \alpha \in A\rangle$.

Proof. The proof is by induction on the number of variables n. If $n = 1$, then I is the ideal in $k[x_1]$ generated by the monomials x_1^α, where $\alpha \in A \subset \mathbf{Z}_{\geq 0}$. Let $\alpha_0 = \inf A$. Since A is a subset of nonnegative integers, it is well ordered and $\alpha_0 \in A$. $x_1^{\alpha_0} \in I$ and divides each x_1^α with $\alpha \in A$; so $I = \langle x_1^{\alpha_0} \rangle$ and Dickson's Lemma is established when $n = 1$.

Assume $n > 1$ and for notation write the variables as $x_1, \ldots, x_{n-1}, y$ and the exponents as (α, j), where $\alpha \in \mathbf{Z}_{\geq 0}^{n-1}$ and $j \in \mathbf{Z}_{\geq 0}$. The monomials in $k[x_1, \ldots, x_{n-1}, y]$ can be written in the form $x^\alpha y^j$.

Suppose $I \subset k[x_1, \ldots, x_{n-1}, y]$ is a monomial ideal. Let J be the ideal in $k[x_1, \ldots, x_{n-1}]$ generated by the monomials x^α for which $x^\alpha y^j \in I$ for some $j \in \mathbf{Z}_{\geq 0}$. J is a monomial ideal in $k[x_1, \ldots, x_{n-1}]$; so by the inductive hypothesis, $J = k[\mathbf{x}]x^{\alpha(1)} + \cdots + k[\mathbf{x}]x^{\alpha(s)}$ for some choice of these $\alpha(i)$'s, where here we let $\mathbf{x} = x_1, \ldots, x_{n-1}$. Now for each of these i's there is a non negative integer m_i with $x^{\alpha(i)}y^{m_i} \in I$. Choose such m_i's and let $m = \max_{1 \leq i \leq s} m_i$. **Remark.** For each $1 \leq i \leq m$ $\boxed{x^{\alpha(i)}y^m = y^{m-m_i} \cdot x^{\alpha(i)}y^{m_i} \in I.}$

Observation: $\boxed{\text{If } x^\beta y^b \in I \text{ for some } \beta \in \mathbf{Z}_{\geq 0}^{n-1} \text{ and } b \geq m, \text{ then } x^\beta y^b \in \langle x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m \rangle.}$

Proof. From the definition of J, $x^\beta \in J = k[\mathbf{x}]x^{\alpha(1)} + \cdots + k[\mathbf{x}]x^{\alpha(s)}$; so

$$x^\beta = \sum_{i=1}^{s} f_i(\mathbf{x})x^{\alpha(i)}, \qquad \text{for suitable } f_i(\mathbf{x}) \in k[x_1, \ldots, x_{n-1}].$$

But then

$$x^\beta y^b = \sum_{i=1}^{s} f_i(\mathbf{x})y^{b-m} \cdot x^{\alpha(i)}y^m \text{ is in } \langle x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m \rangle \subset I \qquad \square$$

Now for each q with $0 \leq q \leq m$ let J_q be the monomial ideal in $k[x_1, \ldots, x_{n-1}]$ generated by the x^β for which $x^\beta y^q \in I$. Using the inductive assumption, choose a finite generating set $x^{\alpha_q(1)}, \ldots, x^{\alpha_q(s_q)}$ for J_q; so $J_q = k[\mathbf{x}]x^{\alpha_q(1)} \cdots + k[\mathbf{x}]x^{\alpha_q(s_q)}$.

I now claim that the monomials in the sets

$$\begin{aligned}
&\{x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)}\}, && \text{from } J_0 \\
&\{x^{\alpha_1(1)}y, \ldots, x^{\alpha_1(s_1)}y\}, && \text{from } J_1 y \\
&\{x^{\alpha_2(1)}y^2, \ldots, x^{\alpha_2(s_2)}y^2\}, && \text{from } J_2 y^2 \\
&\cdots \\
&\{x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}\} && \text{from } J_{m-1}y^{m-1}, \text{ together with} \\
&\{x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m\} && \text{from } Jy^m
\end{aligned} \tag{2.4.0.8}$$

generate I. Let L be the ideal they generate. These monomials clearly belong to I; so $L \subset I$. To establish that $I \subset L$ it suffices to show that each monomial $x^\beta y^j$ of I is in L. There are two cases: $j < m$ and $j \geq m$.

Case I: Suppose $x^\beta y^j \in I$ and $j < m$. Then $x^\beta \in J_j$ and is consequently in the ideal generated by $\{x^{\alpha_j(1)}, \ldots, x^{\alpha_j(s_j)}\}$. This means that $x^\beta = \sum_{k=1}^{s_j} f_k(\mathbf{x})x^{\alpha_j(k)}$ for a suitable choice of $f_k(\mathbf{x}) \in k[x_1, \ldots, x_{n-1}]$ (here $\mathbf{x} = (x_1, \ldots, x_{n-1})$). But then $x^\beta y^j = \sum_{k=1}^{s_j} f_k(\mathbf{x})\big(x^{\alpha_j(k)}y^j\big) \in L$ is in the ideal generated by the monomials (2.4.0.8).

Case II: If $x^\beta y^j \in I$ and $j \geq m$, then the observation above shows that $x^\beta y^j$ is in the ideal generated by $\{x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m\}$ and hence in the ideal generated by the terms (2.4.0.8). Thus every monomial in I is in L and it follows that $I \subset L$ as we desired to show.

We have shown that I is finitely generated. To complete the proof it remains to show that we can choose a finite set of generators whose exponents lie in the original list A. First, switch back to calling the variables $x_1, x_2, \ldots, x_n$. We have produced a finite set $\{x^\gamma : \gamma \in W\}$, with W finite, which generates I. Now (2.4.0.1) states that every term of any $f \in I$ is divisible by some x^α with $\alpha \in A$. In particular, each x^γ is so divisible, say by $x^{\alpha(\gamma)}$. But then the set $\{\alpha(\gamma) : \gamma \in W\}$ will satisfy the role of A_0 in the statement of the lemma. ∎

§**3. Hilbert's Finite Basis Theorem and Gröbner Bases.** Let $\mathbf{I}$ be an ideal in $k[x_1,\dots,x_n]$. Let

$$\mathrm{LT}(\mathbf{I}) = \{\mathrm{LT}(h)\colon h \in \mathbf{I}\}.$$

Since $\langle \mathrm{LT}(\mathbf{I})\rangle$ is a monomial ideal, according to Dickson's Lemma we can choose a finite subset $\{g_1,\dots,g_s\} \subset \mathbf{I}$ with the property that

$$\langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)\rangle = \langle \mathrm{LT}(\mathbf{I})\rangle. \tag{3.1}$$

I claim: $\langle g_1,\dots,g_s\rangle = \mathbf{I}$. To show this, suppose $f \in \mathbf{I}$ and implement the division algorithm, dividing f by $(g_1,\dots,g_s)$, to get $f = q_1g_1 + \cdots + q_sg_s + r$ as in §1. Note that $r = f - (q_1g_1 + \cdots + q_sg_s) \in \mathbf{I}$; so

$$\mathrm{LT}(r) \in \mathrm{LT}(\mathbf{I}) \subset \langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)\rangle.$$

By $(\star)$, the fundamental property of monomial ideals, it follows that $\mathrm{LT}(r)$ is divisible by one of the generating monomials $\mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)$. But by the division algorithm no $\mathrm{LT}(g_i)$ divides any (non zero) monomial in r. Since $\mathrm{LT}(r)$ is one of these monomials it must be that $r = 0$ and $f = q_1g_1 + \cdots + q_sg_s \in \mathbf{I}$. A finite set $\{g_1,\dots,g_s\}$ which generates I as an ideal is called a Hilbert Basis for I. A subset $\{g_1,\dots,g_s\} \subset \mathbf{I}$ satisfying (3.1) is called a *Gröbner Basis for* $\mathbf{I}$. We have shown that Gröbner Bases always exist and that a Gröbner basis for I is a Hilbert basis for I.

The Ascending Chain Condition. A commutative ring with identity satisfies the ascending chain condition (ACC) if each ascending chain of ideals, $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_i \subset \mathfrak{a}_{i+1} \subset \cdots$, contains only a finite number of distinct ideals, i.e. iff there is a positive integer m such that $m \le j$ implies $\mathfrak{a}_j = \mathfrak{a}_{j+1}$.

FB and ACC are equivalent. Suppose R is a commutative ring with identity. Then FB (every ideal has a finite generating set) and the ACC are equivalent conditions for R.

Proof: *FB* $\Rightarrow$ *ACC*: Suppose $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_i \subset \mathfrak{a}_{i+1} \subset \cdots$ is an ascending chain of distinct ideals. The ideal $\mathfrak{A} = \bigcup_i \mathfrak{a}_i$ has a finite generating set $A = \{a_1,\dots,a_q\}$. If m is large enough so that $A \subset \mathfrak{a}_m$, then $\mathfrak{a}_j = \mathfrak{a}_m$ for all $j \ge m$. The converse *FB* $\Leftarrow$ *ACC* is also easy. Let $\mathfrak{B}$ be an ideal of R. If possible, construct recursively two paired sequences: (i) a sequence $a_j \in \mathfrak{B}$ and (ii) a sequence of ideals $\mathfrak{a}_i$ of R. The requirements are that $a_{j+1} \in \mathfrak{B}$, $a_{j+1} \notin \mathfrak{a}_j$ and $\mathfrak{a}_{j+1} = \langle \mathfrak{a}_j, a_{j+1}\rangle$. If this can be carried out $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_i \subset \mathfrak{a}_{i+1} \subset \cdots$ is a non finite strictly increasing sequence of ideals of R which violates the ACC. The only reason it couldn't be carried out is that at some stage $\mathfrak{a}_m = \mathfrak{B}$ which means that $\mathfrak{B}$ has the finite generating set $\{a_1,\dots,a_m\}$. ∎

§**4. Buchberger's S-Criterion and Gröbner bases.** We write $\overline{f}^F$ for the remainder when $f \in k[x_1,\dots,x_n]$ is divided by the (ordered) s-tuple $F = (f_1,\dots,f_s)$. If G and H are two different Gröbner basis $G = \{g_1,\dots,g_s\}$, $H = \{h_1,\dots,h_t\}$ for the ideal I, then

$$\begin{aligned} f &= \varphi + \overline{f}^G, \qquad \text{where } \varphi \in \mathbf{I};\\ f &= \psi + \overline{f}^H, \qquad \text{where } \psi \in \mathbf{I}; \qquad \text{so}\\ \overline{f}^G - \overline{f}^H &= \psi - \varphi \in \mathbf{I}. \end{aligned}$$

(i) No nonzero monomial of $\overline{f}^G$ is divisible by any of the $\mathrm{LT}(g_i)$'s according to the division algorithm.

(ii) No nonzero monomial x^β of $\overline{f}^G$ is divisible by any of the $\mathrm{LT}(h_j)$'s, because if it were we could use the fact that $\mathrm{LT}(h_j) \in \langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)\rangle$ and the basic property $(\star)$ of monomial ideals to infer that some $\mathrm{LT}(g_i)$ must divide $\mathrm{LT}(h_j)$. This fact together with the transitivity of division would in turn imply that this $\mathrm{LT}(g_i)$ would divide x^β in violation of (i) above.

Similarly it follows from symmetry and (ii) above that (iii) no nonzero monomial of $\overline{f}^H$ is divisible by any of the $\mathrm{LT}(g_i)$'s. But then we have both

$$\text{no nonzero monomial of } \overline{f}^G - \overline{f}^H \text{ is divisible by any } \mathrm{LT}(g_i), 1 \le i \le s;$$
$$\text{and } \overline{f}^G - \overline{f}^H \in I.$$

Since G is a Gröbner basis for I these last two lines imply that $\overline{f}^G - \overline{f}^H = 0$. We have shown that $\overline{f}^G$ depends only on the fact that G is a Gröbner basis for I. In particular it doesn't depend on the way G is ordered. We will denote this remainder by $\overline{f}^I$ and refer to it as the *normal form for* f with respect to the ideal I and the given monomial order.

Example 4.0. Here we use lex order on $k[x, y]$. Let $F = (x, xy + x + 1)$, $H = (xy + x + 1, x)$, $f = xy + x + 1$.

Division of f by F yields $xy + x + 1 = (y + 1)x + 1$ and $f^F = 1$.

Division of f by H yields $xy + x + 1 = 1 \cdot (xy + x + 1)$ and $f^H = 0$.

Of course $\langle \mathrm{LT}(x), \mathrm{LT}(xy + x + 1)\rangle = \langle x, xy\rangle = \langle x\rangle$ and $\mathrm{LT}(\langle x, xy + x + 1\rangle) = \langle 1\rangle$; so neither F nor H is a Gröbner basis.

Equivalents. Let $G = \{g_1, \ldots, g_s\} \subset k[x_1, \ldots, x_n]$. The following statements are equivalent:

(4.1) • G is a Gröbner basis for $\langle G\rangle$. Abbreviated: "G Gröbner".

(4.2) • $\mathrm{LT}(\langle G\rangle) \subset \langle \mathrm{LT}(G)\rangle$.

(4.3) • $\langle \mathrm{LT}(\langle G\rangle)\rangle \subset \langle \mathrm{LT}(G)\rangle$.

(4.4) • $\langle \mathrm{LT}(\langle G\rangle)\rangle = \langle \mathrm{LT}(G)\rangle$.

(4.5) • $f \in \langle G\rangle$ if and only if $\overline{f}^G = 0$
no matter how G is ordered to implement the division algorithm.

(4.6) • if $\{a_1, \ldots, a_s\} \subset k[x_1, \ldots, x_n]$,
then $\mathrm{LT}(g_1a_1 + \cdots + g_sa_s)$ is divisible by $\mathrm{LT}(g_i)$ for some $1 \le i \le s$.

Proof. (4.1) and (4.4) are equivalent by definition. (4.4) $\Rightarrow$ (4.2) $\Rightarrow$ (4.3), and (4.3) together with the inclusion obtained by applying $W \mapsto \langle W\rangle$ to the obvious inclusion $\mathrm{LT}(G) \subset \mathrm{LT}(\langle G\rangle)$ implies (4.4); so (4.1)...(4.4) are equivalent. Now it is always true, no matter what G is, that $\overline{f}^G = 0$ implies $f \in \langle G\rangle$. So the content of (4.5) is that $\boxed{\overline{f}^G = 0 \text{ for every } f \in \langle G\rangle \text{ implies } G \text{ is a Gröbner basis for } \langle G\rangle.}$ If G is not a Gröbner basis, there is an $f \in \langle G\rangle$ with $\mathrm{LT}(f)$ not divisible by any $\mathrm{LT}(g_i)$ and for this f, $\overline{f}^G \neq 0$. Thus G not Gröbner implies (4.5) not true. So (4.5) and "G Gröbner" are equivalent. (4.6) is another restatement of the fact that $f \in \langle G\rangle \Rightarrow \overline{f}^G = 0$. So (4.6) and (4.5) really say the same thing in different words. ∎

Definition 4.7. (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

$$S(f, g) = \frac{x^{\alpha\vee\beta}}{cx^\alpha} \cdot f - \frac{x^{\alpha\vee\beta}}{dx^\beta} \cdot g. \tag{4.8}$$

We use $\mathrm{MD}(q)$ to denote the multidegree of a polynomial $q \in k[x_1, \ldots, x_n]$ and $\mathrm{LC}(q)$ to denote its leading coefficient; so $\mathrm{LC}(q) \cdot x^{\mathrm{MD}(q)} = \mathrm{LT}(q)$.

Example 4.9.1.. Suppose $g_i, g_{i+1} \in k[x_1, \ldots, x_n]$, that $\alpha(i) \geq \alpha(i+1)$, and that $\mathbf{x}^{\alpha(i)} g_i$ and $\mathbf{x}^{\alpha(i+1)} g_{i+1}$ both have multidegree δ; so we must have $\mathrm{MD}(g_i) \leq \mathrm{MD}(g_{i+1})$. $\mathbf{x}^{\alpha(i)-\alpha(i+1)} g_i$ and g_{i+1} have the same multidegree. Then

$$\begin{aligned} S(x^{\alpha(i)} g_i, x^{\alpha(i+1)} g_{i+1}) &= \frac{x^{\alpha(i)} g_i}{\mathrm{LC}(g_i)} - \frac{x^{\alpha(i+1)} g_{i+1}}{\mathrm{LC}(g_{i+1})} \\ &= x^{\alpha(i+1)} \left(\frac{x^{\alpha(i)-\alpha(i+1)} g_i}{\mathrm{LC}(g_i)} - \frac{g_{i+1}}{\mathrm{LC}(g_{i+1})} \right) \\ &= x^{\alpha(i+1)} S(g_i, g_{i+1}). \end{aligned} \tag{4.9.2}$$

The following lemma says: Let each of the t polynomials $f_i \in k[x_1, \ldots, x_n]$, $1 \leq i \leq t$. have precise multidegree δ. Let $v = \sum_{i=1}^t c_i f_i$ be a k-linear combination of these polynomials in which the x^δ degree terms cancel. Then v can be expressed as a k-linear combination of the $t-1$ Buchberger S-polynomials $S(f_i, f_{i+1})$, $1 \leq i \leq t-1$, and each of these of these S-polynomials has multidegree $< \delta$. This is rephrased as:

Lemma 4.10. Suppose $f_i = d_i x^\delta + h_i$, $1 \leq i \leq t$, where for each i, $1 \leq i \leq t$, $d_i \in k$, $h_i \in k[x_1, \ldots, x_n]$ and $d_i x^\delta$ is the leading term of f_i. Suppose each $c_i \in k$ and

$$\mathrm{multideg} \left(\sum_{i=1}^t c_i f_i \right) < \delta. \tag{4.11}$$

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

Proof. (4.10) states that $\left(\sum_{i=1}^t c_i d_i \right) x^\delta + \left(\sum_{i=1}^t c_i h_i \right)$ has multidegree $< \delta$. It is clear that the multidegree of $\sum_{i=1}^t c_i h_i$ is less than δ; so we must have

$$\sum_{i=1}^t c_i d_i = 0. \tag{4.12}$$

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

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

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 (4.12) to conclude that

$$\sum_{i=1}^t c_i f_i = \sum_{i=1}^{t-1} \left(\sum_{j=1}^i c_j d_j \right) S(f_i, f_{i+1}). \tag{4.13}$$

The last assertion follows from the fact that $S(f_i, f_{i+1}) = p_i - p_{i+1} = \frac{1}{d_i} h_i - \frac{1}{d_{i+1}} h_{i+1}$ and both h_i and h_{i+1} have multidegree $< \delta$. ∎

What follows is the main result of this section: We divide it into two statements.

Statement 4.14. $B = \{g_1, \dots, g_s\}$ is a Gröbner basis for $\langle G\rangle \Rightarrow$ for each $i < j$, $\overline{S(g_i, g_j)}^{B} = 0$ (no matter how B is ordered).

Proof. The $S(g_i, g_j) \in I$; so if G is an (ordered) Gröbner basis the remainder on division of $S(g_i, g_j)$ by G is zero by (4.5). ∎

Statement 4.15. Suppose $B = \{g_1, \dots, g_s\} \subset k[x_1, \dots, x_n]$. Suppose for each $i < j$ there is an ordering G_{ij} of B such that $\overline{S(g_i, g_j)}^{G_{ij}} = 0$. Then B is a Gröbner basis for $\langle B\rangle$.

Proof. It suffices to show that for every non zero $f \in I = \langle B\rangle$, $\mathrm{LT}(f)$ is divisible by at least one of the terms $\{\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\}$. Since B is a basis for I there is an expression of the form

$$f = h_1 g_1 + \cdots + h_s g_s, \qquad \text{where each } h_i \in k[x_1, \dots, x_n], \tag{4.16}$$

and among such expressions for f we can assume that we have chosen one in which the multiindex $\delta = \max\{\mathrm{multideg}(h_i g_i)\colon 1 \le i \le s\}$ is a minimum. (Remember: multidegrees are well ordered.) Clearly, $\mathrm{multideg}(f) \le \delta$.

Case I: $(\mathrm{multideg}(f) = \delta)$.

Completion of proof in Case I. In this case, for at least one value of i, $\mathrm{multideg}(h_i g_i) = \delta = \mathrm{multideg}(f)$. Then for this particular i, $\mathrm{LT}(g_i)$ has a multiindex $\le \delta$ and consequently $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_i)$ and we are done.

Case II: $\mathrm{multideg}(f) < \delta$. **CAUTION:** For reasons which will become apparent we replace f by v at this point.

Completion of proof in Case II. We will show that if $\mathrm{multidegree}(v) < \delta$, then there is an expression $v = h_1 g_1 + \cdots h_s g_s$, where for each i, $\mathrm{multidegree}(h_i g_i) < \delta$. This will contradict the assumed minimality of δ and show that case II cannot arise. The proof of Statement 4.15 will then be complete.

Suppose h_i have been chosen as in (4.16) and that $\mathrm{multidegree}(v) < \delta$. ($h_i g_i$ is used to run over the summands in (4.16). At least one of these summands must have multidegree δ.)

$$\begin{aligned} v = &\sum\{\mathrm{LT}(h_i) g_i\colon \mathrm{MD}(h_i g_i) = \delta\}, && \text{In this case this sum has multidegree } < \delta,\\ &+ \sum\{(h_i - \mathrm{LT}(h_i)) g_i\colon \mathrm{MD}(h_i g_i) = \delta\}, && \text{These terms have multidegrees } < \delta,\\ &+ \sum\{h_i g_i\colon \mathrm{MD}(h_i g_i) < \delta\}, && \text{and these terms have multidegrees } < \delta. \end{aligned} \tag{A.0}$$

CAUTION: We reintroduce f to represent the sum on the first line in (A.0). Note that $\mathrm{Multidegree}(f) < \delta$. Without loss of generality we can assume by rearranging the terms if needed in the sum for f above that (i) the index i in the first line ranges over $1 \le i \le m$; (ii) $\mathrm{LT}(h_i) = c_i \mathbf{x}^{\alpha(i)}$; and (iii) $\alpha(1) \ge \alpha(2) \ge \cdots \ge \alpha(m)$. So for $1 \le i \le m$ we must have $\mathrm{MD}(g_i) \le \mathrm{MD}(g_{i+1})$. $\mathbf{x}^{\alpha(i)-\alpha(i+1)} g_i$ and g_{i+1} have the same multidegree and in accordance with example (4.9.1)

$$\begin{aligned} S(x^{\alpha(i)} g_i, x^{\alpha(i+1)} g_{i+1}) &= \frac{x^{\alpha(i)} g_i}{\mathrm{LC}(g_i)} - \frac{x^{\alpha(i+1)} g_{i+1}}{\mathrm{LC}(g_{i+1})}\\ &= x^{\alpha(i+1)} \left(\frac{x^{\alpha(i)-\alpha(i+1)} g_i}{\mathrm{LC}(g_i)} - \frac{g_{i+1}}{\mathrm{LC}(g_{i+1})} \right)\\ &= x^{\alpha(i+1)} S(g_i, g_{i+1}). \qquad 1 \le i \le m-1. \end{aligned} \tag{4.9.2}$$

With $f_i = \mathbf{x}^{\alpha(i)} g_i$ the first sum in (A.0) now reads: "each f_i has multidegree δ and yet the sum

$$f = \sum_{i=1}^{m} c_i f_i \qquad \text{has multidegree } < \delta." \tag{A.0.1}$$

This is a setup for Lemma 4.10 from which we can safely conclude that

$$f = \sum_{i=1}^{m-1} a_i S(f_i, f_{i+1}), \qquad \text{for some choice of } a_i \in k,$$

$$= \sum_{i=1}^{m-1} a_i \mathbf{x}^{\alpha(i+1)} S(g_i, g_{i+1}) \tag{A.0.2}$$

Now for each i, $1 \le i < m$ we use the division algorithm and and divide $S(g_i, g_{i+1})$ by G_{ij}. The divisor is $\{g_1, \ldots, g_s\}$ taken in the order G_{ij} and the remainder is zero. This produces a sum expressing the dividend as a sum of quotient×divisor products, no one of which has a multidegree which is greater than that of the dividend. The multidegree of this dividend $S(g_i, g_{i+1})$ is, by example 4.9.1 if you want, strictly less than $\mathrm{MD}(g_{i+1})$. That is, we get an expression of the form

$$S(g_i, g_{i+1}) = \sum_{\ell=1}^{s} B_i^\ell g_\ell, \qquad B_i^\ell \in k[x_1, \ldots, x_n], \ \text{multidegree}(B_i^\ell g_\ell) < \text{multidegree}(g_{i+1}) = \delta - \alpha(i+1). \tag{A.3}$$

Now putting these together, f can be written as

$$f = \sum_{i=1}^{m-1} \sum_{\ell=1}^{s} a_i x^{\alpha(i+1)} B_i^\ell g_\ell = \sum_{\ell=1}^{s} \left(\sum_{i=1}^{m-1} a_i x^{\alpha(i+1)} B_i^\ell \right) g_\ell$$

which has the form $H_1 g_1 + \cdots + H_s g_s$ where for each t, $1 \le t \le s$, $\text{multidegree}(H_t g_t) < \delta$. Adding to this sum the second and third sums of (A.0) we can express the v there (or the original 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. ∎

Statement 4.15 is sometimes called "Buchberger's S-pair criterion".

§**5. Buchberger's Algorithm.** We start with an example.

Example 5.1. Consider $k[x, y]$ with grlex order and let $I = \langle f_1, f_2 \rangle$ where $f_1 = x^3 - 2xy$, $f_2 = x^2 y - 2y^2 + x$.

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

Since the leading term of $S(f_1, f_2) = -x^2$ is not in $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle = x^3 k[x, y] + x^2 y k[x, y]$, 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)/(and succeed in producing) a Gröbner basis for I by adding at each stage to the prebasis the remainders of those S-polynomials which give nonzero remainders when divided by the prebasis. We continue this augmentation until every S-polynomial formed from pairs taken from the prebasis gives a zero remainder when divided by some ordering of the prebasis. (Actually we will not worry about changing the order of the prebasis, but will take it in the order it is created by making additions on the right. At worst this may lengthen the process of constructing a Gröbner basis.) When no further additions are possible, the prebasis is actually a Gröbner basis for I according to Buchberger's S-Criterion.

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

$$S(f_1, f_2) = f_3 \text{ and straighforward division yields } \overline{S(f_1, f_2)}^F = 0,$$
$$\text{since neither } \mathrm{LT}(f_1) \text{ nor } \mathrm{LT}(f_2) \text{ divides } \mathrm{LT}(f_3).$$
$$S(f_1, f_3) = (x^3 - 2xy) + x(-x^2) = -2xy; \ \text{ and } \overline{S(f_1, f_3)}^F = -2xy.$$

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 5.1. Let G be a Gröbner basis for the polynomial ideal I. Let $p \in G$ 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 5.2. A *minimal Gröbner basis* for a polynomial ideal I is a Gröbner basis G for I such that:

(i) The leading coefficient 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 5.3. 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, $1 \leq i \leq s$.

Remark. If we weaken (ii) in Definition 5.2 so that it reads: (ii') No $\mathrm{LT}(g_i)$ lies in $\langle \mathrm{LT}(G - \{g_i\})\rangle$ for any i, $1 \leq i \leq s$, the so-altered Definition 5.3 defines a minimal Gröbner basis for I; so it is true that every reduced Gröbner basis is a minimal Gröbner basis as a matter of course.

Reduced Gröbner bases are unique.

Theorem 5.4. 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 any of 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 $\mathrm{LT}(f)$. **Because G and $\tilde{G}$ are reduced** 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. ∎