§1. **Monomial Orderings and Division of Polynomials.**

- the dividend is a polynomial $f \in k[x_1, \dots, x_n]$;
- the divisor is an $m$-tuple $(d_1, \dots, d_m) \in (k[x_1, \dots, x_n])^m$;
- the result is a relation $f = q_1 d_1 + \cdots + q_m d_m + r$, where
  (i) multidegree$(q_i d_i) \le$ multidagree$(f)$, $1 \le i \le m$, and either
  (ii) $r = 0$ or
  (iii) no monomial in $r$ is divisible by any of the leading terms $\mathrm{LT}(d_1), \dots, \mathrm{LT}(d_m)$.
- If $\mathrm{LT}(d_i)$ divides $\mathrm{LT}(d_j)$ for some $i < j$, then $q_j = 0$ and the result $f = q_1 d_1 + \cdots + q_m d_m + r$ is unchanged if $d_j$ is removed from the sequence of divisors. In particular, $r$ is unchanged.

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 $x^\alpha$, $\alpha \in A$. 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 $\langle x^\alpha, \alpha \in A_0\rangle = \langle x^\alpha, \alpha \in A\rangle$.

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

- $\boxed{\text{a Gröbner basis for } I \text{ is a Hilbert basis for } I.}$.
- $\overline{f}^I$ is the *normal form for* $f$ with respect to the ideal $I$ and the given monomial order.

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

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

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

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

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

(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 $\{a_1, \dots, a_s\} \subset k[x_1, \dots, x_n]$,
then $\mathrm{LT}\left(g_1 a_1 + \cdots + g_s a_s\right)$ is divisible by $\mathrm{LT}\left(g_i\right)$ for some $1 \le i \le s$.

(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 $q \in k[x_1, \dots, x_n]$ 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 $g_i, g_{i+1} \in k[x_1, \dots, x_n]$, that $\alpha(i) \ge \alpha(i+1)$, and that $\mathbf{x}^{\alpha(i)} g_i$ and $\mathbf{x}^{\alpha(i+1)} g_{i+1}$ both have multidegree $\delta$; so 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. 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 $f_i \in k[x_1, \dots, x_n]$, $1 \le i \le t$. have precise multidegree $\delta$. Let $v = \sum_{i=1}^t c_i f_i$ be a $k$-linear combination of these polynomials in which the $x^\delta$ degree terms cancel. Then $v$ can be expressed as a $k$-linear combination of the $t-1$ Buchberger S-polynomials $S(f_i, f_{i+1})$, $1 \le i \le t-1$, and each of these of these S-polynomials has multidegree $< \delta$. This is rephrased as:

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

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

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 $a_i \in k$, $1 \le i \le t-1$. Furthermore, each $S(f_i, f_j)$ has multidegree $< \delta$.

**Statement 4.14.** $B = \{g_1, \ldots, g_s\}$ 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).

**Statement 4.15.** Suppose $B = \{g_1, \ldots, g_s\} \subset k[x_1, \ldots, x_n]$. 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 $\langle B\rangle$.

§**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 $\langle \text{LT}(f_1), \text{LT}(f_2)\rangle = x^3 k[x, y] + x^2 y k[x, y]$, 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

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

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 $F = (x^3 - 2xy,\ x^2 y - 2y^2 + x,\ -x^2,\ -2xy)$.

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

$$S(f_2, f_3) = (x^2 y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x; \text{ and } \overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0$$

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 $\text{LT}(p) \in \langle \text{LT}(G - \{p\})\rangle$. 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 $i$, $1 \le i \le s$.

**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 $i$, $1 \le i \le s$, 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. ∎