1 Preliminary

We denote by K a field and by $K[X]$ the polynomial ring over K in n variables $X_1, \ldots, X_n$. For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$ we abbreviate $X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n}$ by X^α, and we call X^α a power product.

Definition 1.1. A term order (or a term ordering or even a monomial ordering) on $K[X]$ is any relation $<$ on $\mathbf{N}^n$ satisfying :

(1) $<$ is a total (or linear) ordering on $\mathbf{N}^n$.

(2) If $\alpha < \beta$ and $\gamma \in \mathbf{N}^n$, then $\alpha + \gamma < \beta + \gamma$.

(3) $<$ is a well-ordering on $\mathbf{N}^n$. This means that every nonempty subset of $\mathbf{N}^n$ has a smallest element under $<$.

For a simple example of a term order, note that the usual numerical order

$$0 < 1 < 2 < 3 < \cdots < m < m+1 < \cdots$$

on the elements of $\mathbf{N}$ satisfies the three conditions of Definition 1.1. Hence, the degree ordering

$$1 < x < x^2 < \cdots < x^m < x^{m+1} < \cdots$$

on the monomials in $K[X]$ is a term order.

Definition 1.2. (Lexicographic Order) For $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbf{N}^n$ we define

$$\alpha <_{lex} \beta \iff \text{there is a } j \in \{1, 2, \ldots, n\} \text{ such that } \alpha_k = \beta_k \text{ if } k < j \text{ and } \alpha_j < \beta_j.$$

Example 1 : $(0, 2, 0) <_{lex} (1, 0, 0) <_{lex} (1, 0, 1)$.

With $\sum_\alpha c_\alpha X^\alpha$ or $\sum_{\alpha \in N^n} c_\alpha X^\alpha$ we always tacitly mean that only finitely many of the coefficients c_α are different from zero. If $f = \sum_\alpha c_\alpha X^\alpha$ is a polynomial in $K[X]$ and we have selected a term order $<$, then we can order the monomials of f in an unambiguous way with respect to $<$. For example, let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$. Then with respect to the lex order, we would reorder the terms of f in decreasing order as

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2.$$

We will use the following terminology.

Definition 1.3. Let $f = \sum_\alpha c_\alpha X^\alpha$ be a nonzero polynomial in $K[X]$ and let $<$ be a term order.

(1) The degree of f is

$$deg(f) := max\{\ \alpha \in N^n \mid c_\alpha \neq 0\ \}.$$

(2) The leading coefficient of f is

$$lc(f) := c_{deg(f)}\ .$$

(3) The leading monomial of f is

$$lm(f) := X^{deg(f)}\ .$$

(4) The leading term of f is

$$lt(f) := lc(f) \cdot lm(f)\ .$$

Example 2 : Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ and let $<$ denote the lex order. Then

$$deg(f) = (3,0,0),\quad lc(f) = -5,\quad lm(f) = x^3,\quad lt(f) = -5x^3.$$

For a subset $F \subseteq K[X]$ we define

$$deg(F) := \{\ deg(f) \mid f \in F - \{0\}\ \},\quad D(F) := deg(F) + \mathbf{N}^n \quad \text{and}$$

$$LT(F) := \{\ lt(f) \mid f \in F - \{0\}\ \}.$$

Let us firstly look at the special case of the division of f by g, where $f, g \in K[X]$. We fix a term order on $K[X]$.

Definition 1.4. Given f, g, h in $K[X]$, with $g \neq 0$, we say that f reduces to h modulo g in one step, written

$$f \xrightarrow{g} h,$$

if and only if $lm(g)$ divides $lt(f)$ and

$$h = f - \frac{lt(f)}{lt(g)}\ g\ .$$

Example 3 : Let $f = 6x^2y - x + 4y^3 - 1$ and $g = 2xy + y^3$ be polynomials in $Q[x, y]$. If the term order is lex order with $y < x$, then $f \xrightarrow{g} h$, where $h = -3xy^3 - x + 4y^3 - 1$, since, in this case $lt(f) = 6x^2y$ is the term of f we have canceled using $lt(g) = 2xy$.

In the multivariable case we may have to divide by more than one polynomial at a time, and so we extend the process of reduction defined above to include this more general setting.

Definition 1.5. Let f, h, and $f_1, \ldots, f_s$ be polynomials in $K[X]$, with $f_i \neq 0$ $(1 \leq i \leq s)$, and let $F = \{f_1, \ldots, f_s\}$. We say that f reduces to h modulo F, denoted

$$f \xrightarrow{F}_+ h,$$

if and only if there exist a sequence of indices $i_1, i_2, \ldots, i_t \in \{1, 2, \ldots, s\}$ and a sequence of polynomials $h_1, \ldots, h_{t-1} \in K[X]$ such that

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h \ .$$

Definition 1.6. A polynomial r is called reduced with respect to a set of non-zero polynomials $F = \{f_1, \ldots, f_s\}$ if $r = 0$ or no power product that appears in r is divisible by any one of the $lm(f_i)$, $i = 1, 2, \ldots, s$. In other words, r cannot be reduced modulo F.

Definition 1.7. Fix a term order and let I be an ideal in $K[X]$, $I \neq \{0\}$. A finite subset G of $I - \{0\}$ is a Gröbner basis of $I \iff LT(G)$ generates the ideal $< LT(I) >$.

Definition 1.8. Let $0 \neq f, g \in K[X]$, and let $L = lcm\big(lm(f), lm(g)\big)$. The polynomial

$$S(f, g) = \frac{L}{lt(f)}\ f - \frac{L}{lt(g)}\ g$$

is called the S-polynomial of f and g .

Example 4 : Let $f = 2yx - y$, $g = 3y^2 - x \in \mathbf{Q}[x, y]$. If the term order is lex order with $x < y$, then $L = y^2x$, and $S(f, g) = \frac{y^2x}{2yx}\ f - \frac{y^2x}{3y^2}\ g = \frac{1}{2}yf - \frac{1}{3}xg = -\frac{1}{2}y^2 + \frac{1}{3}x^2$.

Algorithm 1.9. (Buchberger's Algorithm for Computing Gröbner Bases)

INPUT : $F = \{f_1, \ldots, f_s\} \subseteq K[X]$ with $f_i \neq 0$ $(1 \leq i \leq s)$

OUTPUT : $G = \{g_1, \ldots, g_t\}$, a Gröbner basis for $< f_1, \ldots, f_s >$

INITIALIZATION : $G := F$, $\mathcal{G} := \big\{\{f_i, f_j\} \mid f_i \neq f_j \in G\big\}$

WHILE $\mathcal{G} \neq \emptyset$ DO

Choose any $\{f, g\} \in G$

$\mathcal{G} := \mathcal{G} - \big\{\{f, g\}\big\}$

$S(f, g) \xrightarrow{G}_{+} h$, where h is reduced with respect to G

IF $h \neq 0$ THEN

$\mathcal{G} := \mathcal{G} \cup \big\{\{u, h\} \mid \text{for all } u \in G\big\}$

$G := G \cup \{h\}$

Example 5 : Let $f_1 = xy - x$, $f_2 = -y + x^2 \in \mathbf{Q}[x, y]$ ordered by the lex term ordering with $x < y$.

INITIALIZATION : $G := \{f_1, f_2\}$, $\mathcal{G} := \big\{\{f_1, f_2\}\big\}$

First pass through the WHILE loop

$\mathcal{G} := \emptyset$

$S(f_1, f_2) \xrightarrow{G}_{+} x^3 - x = h$ (reduced with respect to G)

Since $h \neq 0$, let $f_3 := x^3 - x$

$\mathcal{G} := \big\{\{f_1, f_3\}, \{f_2, f_3\}\big\}$

$G := \big\{f_1, f_2, f_3\big\}$

Second pass through the WHILE loop

$\mathcal{G} := \big\{\{f_2, f_3\}\big\}$

$S(f_1, f_3) \xrightarrow{G}_{+} 0 = h$

Third pass through the WHILE loop

$\mathcal{G} := \emptyset$

$S(f_2, f_3) \xrightarrow{G}_{+} 0 = h$

The WHILE loop stops, since $\mathcal{G} := \emptyset$.

Thus, $\{f_1, f_2, f_3\}$ is a Gröbner basis for the ideal $< f_1, f_2 >$.

Definition 1.10. Let I be an ideal of $K[X]$. The initial ideal of I for the term order $<$ is the ideal

$$in_<(I) = \big\langle X^\alpha \mid \text{for all } \alpha \in D(I)\big\rangle \ .$$

The ideal $in_<(I)$ is highly dependent on the chosen ordering ; once $<$ is fixed, the ideal is denoted simply by $in(I)$.

Let us fix, for our discussion, a term order which we denote simply by $<$. Let $S = \{X^\alpha + I \mid \alpha \notin D(I)\}$, where I is a non-zero ideal in $K[X]$. We are going to show that S is a basis for the K-vector space $K[X] / I$.

We first show that every element $f + I$ in $K[X] / I$ is a linear combination of S. Let $f = \sum_{i=0}^{r} c_{\beta_i} X^{\beta_i} \in K[X]$, and we may assume that $\beta_0 < \beta_1 < \beta_2 < \cdots < \beta_r := deg(f)$.

Let $l_1 = max\{\ i \ \mid \ \beta_i \in D(I),\ 0 \leq i \leq r\ \}$.

If $l_1 = 0$, then obviously, $f + I$ is a linear combination of S.

Suppose $l_1 > 0$. Since $\beta_{l_1} \in D(I)$, there exists a non-zero polynomial $g_1 \in I$ such that $\beta_{l_1} = deg(g_1)$ and $lt(g_1) = c_{\beta_{l_1}} X^{\beta_{l_1}}$.

Let $h_1 = f - g_1$. Then $f + I = h_1 + I$.

Write $h_1 = \sum_{i=0}^{s} d_{\gamma_i} X^{\gamma_i} \in K[X]$.

Again, let $l_2 = max\{\ i \ \mid \ \gamma_i \in D(I),\ 0 \leq i \leq s\ \}$.

If $l_2 = 0$, then $h_1 + I$ is a linear combination of S, so is $f + I$.

Suppose $l_2 > 0$. Since $\gamma_{l_2} \in D(I)$, there exists a non-zero polynomial $g_2 \in I$ such that $\gamma_{l_2} = deg(g_2)$ and $lt(g_2) = d_{\gamma_{l_2}} X^{\gamma_{l_2}}$.

Let $h_2 = h_1 - g_2$. Then $f + I = h_1 + I = h_2 + I$.

Doing the same thing on h_2 and keeping going, we will get that $f + I$ is a linear combination of S.

Next, we show that S is a linearly independent subset of $K[X] / I$. Let $\sum_{i=0}^{m} a_{\alpha_i}(X^{\alpha_i} + I) = I$, where $X^{\alpha_i} + I \in S$ and $\alpha_0 < \alpha_1 < \cdots < \alpha_m$. Then $\sum_{i=0}^{m} a_{\alpha_i} X^{\alpha_i} \in I$.

If $a_{\alpha_m} \neq 0$, then $\alpha_m \in D(I)$, a contradiction. So, $a_{\alpha_m} = 0$ and $\sum_{i=0}^{m-1} a_{\alpha_i} X^{\alpha_i} \in I$.

If $a_{\alpha_{m-1}} \neq 0$, then $\alpha_{m-1} \in D(I)$, a contradiction. So, $a_{\alpha_{m-1}} = 0$ and $\sum_{i=0}^{m-2} a_{\alpha_i} X^{\alpha_i} \in I$.

Continuing in the same way, we get that $a_{\alpha_m} = a_{\alpha_{m-1}} = \cdots = a_{\alpha_0} = 0$.

Therefore, S is a basis for the K-vector space $K[X] / I$.

Definition 1.11. For a given $f \in K[X]$, the unique polynomial

$$NormalForm(f) = \sum c_\alpha X^\alpha,$$

where each $\alpha \notin D(I)$, such that

$$f - NormalForm(f) \in I,$$

is called the normal form of f with respect to the chosen ordering.

Lemma 1.1. *Let I be an ideal of $K[X]$. Then the mapping*

$$NormalForm \ : \ K[X] \,/\, I \quad \longrightarrow \quad K[X] \,/\, in(I)$$

is an isomorphism of K-vector spaces.

Proof : Define

$$\begin{aligned} NormalForm \ : \ K[X] \,/\, I \quad &\longrightarrow \quad K[X] \,/\, in(I) \\ f + I \quad &\longrightarrow \quad NormalForm(f) + in(I) \end{aligned}$$

Since $\{X^\alpha + I \mid \alpha \notin D(I)\}$ is a basis of the K-vector space $K[X] \,/\, I$, clearly, *NormalForm* is well-defined, epimorphism, and $ker(NormalForm) = \{ \ I \ \}$.
Therefore, $K[X] \,/\, I \ \simeq \ K[X] \,/\, in(I)$. □