5. MONOMIAL ORDERS

Definition 5.1

A monomial order $>$ on $K[x_1, \dots, x_n]$ is a relation $>$ on $\mathbb{N}^n$ satisfying

(i) $>$ is a total order:

$>$ is transitive, and

For all $\alpha, \beta \in \mathbb{N}^n$, exactly one of $\alpha > \beta$, $\alpha = \beta$, $\alpha < \beta$ holds

(ii) for any $\alpha, \beta, \gamma \in \mathbb{N}^n$,

$$\alpha > \beta \implies \alpha + \gamma > \beta + \gamma$$

(iii) $>$ is a well order:

every non-empty subset $A \subset \mathbb{N}^n$ has a minimal element $\alpha \in A$ ($\beta > \alpha$ for all $\beta \in A \setminus \{\alpha\}$)

We will use $\alpha > \beta$ and $x^\alpha > x^\beta$ interchangeably.

We also denote $\alpha \geq \beta$ for ($\alpha > \beta$ or $\alpha = \beta$)

Example 5.2

In $K[t]$, there is a canonical monomial order: the standard order $>$ on $\mathbb{N}$, so

$$t^5 > t^4 > t > 1 \quad \text{etc.}$$

Lemma 5.3

A total order $>$ on $\mathbb{N}^n$ is a well order if and only if there is no infinite strictly decreasing sequence

$$\alpha_1 > \alpha_2 > \alpha_3 > \dots$$

Proof

"$\Rightarrow$" Let $\alpha_1 \geq \alpha_2 \geq \alpha_3 \geq \dots$ and consider $A = \{\alpha_1, \alpha_2, \alpha_3, \dots\}$

Well order $\Rightarrow \exists n \in \mathbb{N}$ s.t. $\alpha_n = \min A$

$\Rightarrow \alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n = \alpha_{n+1} = \alpha_{n+2} = \dots$

So no infinite strictly decreasing sequence exists.

"$\Leftarrow$" Suppose $>$ is not a well order, so $\exists A \subset \mathbb{N}^n$ without a minimal element.

Pick any $\alpha_1 \in A$. It is not minimal, so $\exists \alpha_2 \in A$, $\alpha_2 < \alpha_1$.

α_2 is not minimal, so $\exists \alpha_3$, $\alpha_3 < \alpha_2 < \alpha_1$.

By induction we obtain an infinite sequence

$$\alpha_1 > \alpha_2 > \alpha_3 > \dots \qquad \square$$

Definition 5.4

Let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$ multi-indices.

1) lexicographic order (lex) a.k.a. dictionary order

$\alpha >_{lex} \beta$ if the left-most nonzero entry of $\alpha - \beta$ is positive.

$$(0,3,0) < (1,1,3) < (2,0,1)$$

2) degree lexicographic order (deglex)

$\alpha >_{deglex} \beta$ if
- $|\alpha| > |\beta|$ or
- $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$

$$(0,3,0) < (2,0,1) < (1,1,3)$$

3) degree reverse lexicographic order (degrevlex)

$\alpha >_{degrevlex} \beta$ if
- $|\alpha| > |\beta|$ or
- $|\alpha| = |\beta|$ and the right-most nonzero entry of $\alpha - \beta$ is negative

$$(2,0,1) < (0,3,0) < (1,1,3)$$

4) weighted degree reverse lexicographic order (wdegrevlex)

Fix weights $w = (w_1, \dots, w_n) \in \mathbb{Z}_+^n = \{1, 2, 3, \dots\}^n$

$\alpha >_{wdegrevlex} \beta$ if
- $|\alpha|_w > |\beta|_w$, where $|\alpha|_w = \sum_{i=1}^{n} w_i \alpha_i$, or
- $|\alpha|_w = |\beta|_w$ and the right-most nonzero entry of $\alpha - \beta$ is negative

$$w = (10, 7, 1) \Rightarrow (1,1,3) < (2,0,1) < (0,3,0)$$

Proposition 5.5

lex, deglex, degrevlex, wdegrevlex are monomial orders.

Proof

(i) total order: All of the above consider $\alpha - \beta \in \mathbb{Z}^n$ to break ties. If $\alpha \neq \beta$, then $\alpha - \beta$ has either a first/last positive/negative term, so $\alpha > \beta$ or $\alpha < \beta$.

For transitivity, suppose $\alpha > \beta$ and $\beta > \gamma$.

Then $\alpha > \gamma$ follows from $\alpha - \gamma = (\alpha - \beta) + (\beta - \gamma)$

(ii) additivity: Let $\alpha > \beta$ and $\gamma \in \mathbb{N}^n$.

Since $|\alpha + \gamma| = |\alpha| + |\gamma|$ and $|\alpha + \gamma|_w = |\alpha|_w + |\gamma|_w$, and $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, it follows that

$$\alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma.$$

(iii) well order:

For deglex, degrevlex, wdegrevlex, if $\beta < \alpha$, then

$$\beta_i \leq |\beta| \leq |\alpha|, \quad i = 1, \dots, n$$

$$\Rightarrow \beta \in \{0, 1, \dots, |\alpha|\}^n.$$

That is, for $\alpha \in \mathbb{N}^n$, there are only finitely many $\beta < \alpha$

$\Rightarrow$ every $A \subset \mathbb{N}^n$ has a minimum.

For lex, let $A \subset \mathbb{N}^n$ and define $A = A_0 \supset A_1 \supset \dots \supset A_n$

$$A_{i+1} = \{\alpha \in A_i : \alpha_i = \min\{\beta_i : \beta \in A_i\}\}$$

Then $\alpha \in A_n$ is the minimal element of A:

by induction $A_i \ni \alpha \leq \beta \in A \setminus A_i$ $\square$

Definition 5.6

Let $>$ be a monomial order on $K[x_1,\dots,x_n]$ and $p = \sum_\alpha a_\alpha x^\alpha \in K[x_1,\dots,x_n]$.

- The multidegree of p is
$$\text{multideg}(p) = \max_> \{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$$
- The leading coefficient of p is
$$LC(p) = a_{\text{multideg}(p)}$$
- The leading monomial of p is
$$LM(p) = x^{\text{multideg}(p)}$$
- The leading term of p is
$$LT(p) = LC(p) \cdot LM(p)$$

Convention: if a monomial order $>$ is fixed we write polynomials with terms in decreasing order

Example 5.7

Using lex order in $\mathbb{Q}[x,y,z]$
$$p = \frac{1}{2}x^2z - 3xyz^3 + \frac{2}{7}y^3$$
$$(2,0,1) > (1,1,3) > (0,3,0)$$

$\text{multideg}\, p = (2,0,1)$,

$LC(p) = \frac{1}{2}$,

$LM(p) = x^2z$,

$LT(p) = \frac{1}{2}x^2z$

Lemma 5.8

Let $p, q \in k[x_1, \dots, x_n]$ and $>$ monomial order.

(i) $\operatorname{multideg}(pq) = \operatorname{multideg}(p) + \operatorname{multideg}(q)$

(ii) $\operatorname{multideg}(p+q) \leq \max\left(\operatorname{multideg}(p), \operatorname{multideg}(q)\right)$

Proof

Let $p = \sum a_\alpha x^\alpha$ and $q = \sum b_\beta x^\beta$

(i) Since $pq = \sum_{\alpha,\beta} a_\alpha b_\beta x^{\alpha+\beta}$, we have

$\operatorname{multideg}(pq) = \max\{\alpha+\beta : a_\alpha \neq 0, b_\beta \neq 0\}$

Let $\bar{\alpha} = \operatorname{multideg}(p)$ and $\bar{\beta} = \operatorname{multideg}(q)$ so that

$a_\alpha \neq 0 \Rightarrow \alpha \leq \bar{\alpha}$ and $b_\beta \neq 0 \Rightarrow \beta \leq \bar{\beta}$

Then by additivity of a monomial order

$a_\alpha b_\beta \neq 0 \implies \alpha+\beta \leq \alpha + \bar{\beta} \leq \bar{\alpha} + \bar{\beta}$

so $\operatorname{multideg}(pq) = \bar{\alpha} + \bar{\beta}$.

(ii) $p+q = \sum (a_\alpha + b_\alpha) x^\alpha$, so

$\operatorname{multideg}(p+q) = \max\{\alpha : a_\alpha + b_\alpha \neq 0\} =: \gamma$

Since $a_\gamma + b_\gamma \neq 0$ either $a_\gamma \neq 0$ or $b_\gamma \neq 0$ (or both).

If $a_\gamma \neq 0$, then $\gamma \leq \operatorname{multideg} p$

if $b_\gamma \neq 0$, then $\gamma \leq \operatorname{multideg} q$

$\Rightarrow \gamma \leq \max(\operatorname{multideg} p, \operatorname{multideg} q)$ $\square$

Theorem 5.9 (multivariate polynomial division)

Let $>$ be a monomial order on $K[x_1, \dots, x_n]$ and $P = (p_1, \dots, p_s)$ an ordered tuple, $p_i \in K[x_1, \dots, x_n]$.
Then $\forall f \in K[x_1, \dots, x_n]$ $\exists q_1, \dots, q_s, r \in K[x_1, \dots, x_n]$ s.th

$$f = q_1 p_1 + \dots + q_s p_s + r$$

where $\text{multideg}\, f \geq \text{multideg}\,(q_i p_i)$ for $i = 1, \dots, s$ and either $r = 0$, or none of the monomials of r are divisible by $LT(p_1), \dots, LT(p_s)$.

Example 5.10

Consider lex order on $\mathbb{R}[x, y, t]$

Let $f = x^2 - 2x - y$ $p_1 = x - t - 1$ $p_2 = y - t^2 + 1$

be the polynomials from Example 4.5.

$LT(f) = x^2$ is divisible by $LT(p_1) = x$

If $q_1 = x$ then $q_1 p_1 = x^2 - xt - x$

$$\Rightarrow f = q_1 p_1 + xt - x - y$$

$LT(xt - x - y) = xt$ is still divisible by $LT(p_1) = x$

If $q_1 = x + t$ then $q_1 p_1 = x^2 - x - t^2 - t$

$$\Rightarrow f = q_1 p_1 - x - y + t^2 + t$$

$LT(-x - y + t^2 + t) = -x$ still divisible by $LT(p_1) = x$

If $q_1 = x + t - 1$ then $f = q_1 p_1 - y + t^2 - 1 = q_1 p_1 - p_2$

so for $q_1 = x + t - 1$, $q_2 = -1$ we have $r = 0$.

In the computation we had

q_1	q_2	r	$LT(r)$	multdeg r
0	0	x^2-2x-y	x^2	$(2,0,0)$
x	0	$xt-x-y$	xt	$(1,0,1)$
$x+t$	0	$-x-y+t^2+t$	$-x$	$(1,0,0)$
$x+t-1$	0	$-y+t^2+1$	$-y$	$(0,1,0)$
$x+t-1$	-1	0		

Key feature: $LT(r)$ is decreasing

Proof of Theorem 5.9

Consider the following algorithm modifying $g, q_1, \dots, q_s, r$:

Start with $q_1 = \dots = q_s = 0$, $r = 0$, and $g = f$.

While $g \neq 0$:

(remainder step) If $LT(p_i) \nmid LT(g)$, replace
$$r := r + LT(g)$$
$$g := g - LT(g)$$

(division step) Otherwise, let i be the first index such that $LT(p_i) \mid LT(g)$. Replace
$$q_i := q_i + LT(g)/LT(p_i)$$
$$g := g - p_i \cdot LT(g)/LT(p_i)$$

We claim that this algorithm stops after finitely many steps and the resulting $q_1, \dots, q_s, r$ satisfy the claim

First, we claim that

$$f = q_1 p_1 + \dots + q_s p_s + g + r$$

holds throughout the algorithm:

- in a remainder step $g+r$ is unchanged:

$$(g - LT(g)) + (r + LT(g)) = g + r$$

- in a division step $q_i p_i + g$ is unchanged:

$$\left(q_i + \frac{LT(g)}{LT(p_i)}\right) p_i + \left(g - p_i \frac{LT(g)}{LT(p_i)}\right) = q_i p_i + g$$

Second, we claim that multideg(g) is decreasing:

- in a remainder step, either $g - LT(g) = 0$ or multideg$(g - LT(g))$ < multideg g
- in a division step, observe that (see Lemma 5.8)

$$LT(p_i \cdot LT(g)/LT(p_i)) = LT(g),$$

so again multideg$(g - p_i LT(g)/LT(p_i))$ < multideg(g)

By Lemma 5.3, after finitely many steps we must reach $g = 0$ and the algorithm stops. Then

$$f = q_1 p_1 + \dots + q_s p_s + r$$

By construction none of the terms added to r are divisible by any $LT(p_i)$.

Finally, every term of q_i is of the form $LT(g)/LT(p_i)$.

Using Lemma 5.8 we obtain

$$\text{multideg}(q_i p_i) \leq \text{multideg}(g) \leq \text{multideg}(f) \quad \square$$