Division mod an Ideal

November 2, 2023 9:19 AM

CLO 2.2 Monomial Orderings

Def A monomial ordering on $\mathbb{Z}^n_{\geq 0}$ is a relation $>$ on $\mathbb{Z}^n_{\geq 0}$ s.t.

(i) $>$ is a total ordering $LM(f)$ is unique

(ii) $\forall \alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$ $\alpha > \beta \Rightarrow \gamma + \alpha > \gamma + \beta$ $LM(f \cdot g) = LM(f) \cdot LM(g)$.

(iii) Every non-empty subset $S \subset \mathbb{Z}^n_{\geq 0}$ has a least element (well ordering). ($\Rightarrow$ $\div$ algorithm terminates).

Ex. In $k[x]$ there is only one monomial ordering

$1 < x < x^2 < \cdots$

$1 > x > x^2 > x^3 > \cdots$ satisfies (i), (ii) but not (iii).

Lemma 2 A relation $>$ on $\mathbb{Z}^n_{\geq 0}$ is a well-ordering $\Leftrightarrow$ every strictly decreasing sequence

$\alpha^{(1)} > \alpha^{(2)} > \alpha^{(3)} > \cdots$ in $\mathbb{Z}^n_{\geq 0}$ is finite.

Proof. We will prove $>$ is NOT a well ordering $\Leftrightarrow$ $\exists$ an infinite strictly decreasing sequence.

($\Rightarrow$) Given $>$ is not a well ordering

$\Rightarrow \exists S \subset \mathbb{Z}^n_{\geq 0}$ with no least element.

$\Rightarrow \exists \alpha^{(1)}, \alpha^{(2)} \in S$ s.t. $\alpha^{(2)} < \alpha^{(1)}$.

$\Rightarrow \exists \alpha^{(3)} \in S$ s.t. $\alpha^{(3)} < \alpha^{(2)}$.

$\Rightarrow \alpha^{(1)} > \alpha^{(2)} > \alpha^{(3)} > \alpha^{(4)} > \cdots$

[is an infinite strictly decreasing sequence].

($\Leftarrow$) Given an infinite strictly decreasing sequence

$\alpha^{(1)} > \alpha^{(2)} > \alpha^{(3)} > \cdots$

$S = \{\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}, \ldots\}$ has no least element.

Lexicographical Order. Let $u, v \in \mathbb{Z}_{\geq 0}^n$.

$u > v$ if $\exists k$ s.t. $u_k > v_k$ and $u_i = v_i$ for $1 \leq i < k$.

Prop 4. Lex order is a monomial ordering.

Proof of (iii). TAC suppose lex order is not a well ordering. Then by Lemma 2 there is an infinite strictly decreasing sequence in $\mathbb{Z}_{\geq 0}^n$.

$$S = \alpha^{(1)} > \alpha^{(2)} > \alpha^{(3)} > \cdots$$
$$= [\alpha_1^{(1)}, \alpha_2^{(1)}, \dots, \alpha_n^{(1)}] > [\alpha_1^{(2)}, \alpha_2^{(2)}, \dots, \alpha_n^{(2)}] > [\alpha_1^{(3)}$$

In lex order

$$A = \alpha_1^{(1)} \geq \alpha_1^{(2)} \geq \alpha_1^{(3)} \geq \cdots \quad \text{in } \mathbb{Z}_{\geq 0}$$

But $\mathbb{Z}_{\geq 0}$ is a well ordering $\Rightarrow$ this sequence A in $\mathbb{Z}_{\geq 0}$ must stop decreasing (must "stabilize") i.e.

$\exists k \geq 1$ s.t. $\alpha_1^{(k)} = \alpha_1^{(k+1)} = \alpha_1^{(k+2)} = \cdots$

So consider S starting at k i.e.

$$\alpha^{(k)} > \alpha^{(k+1)} > \alpha^{(k+2)} > \cdots$$
$$[\alpha_1^{(k)}, \alpha_2^{(k)}, \dots, \alpha_n^{(k)}] > [\alpha_1^{(k+1)}, \alpha_2^{(k+1)}, \dots, \alpha_n^{(k+1)}] > [\alpha_1^{(k+2)}, \alpha_2^{(k+2)}, \dots] > \cdots$$

In lex order $B = \alpha_2^{(k)} \geq \alpha_2^{(k+1)} \geq \alpha_2^{(k+2)} \geq \cdots$ in $\mathbb{Z}_{\geq 0}$ which is a well ordering so this sequence B also must stabilize. So $\exists \ell \geq k$ s.t.

$$\alpha_2^{(\ell)} = \alpha_2^{(\ell+1)} = \alpha_2^{(\ell+2)} = \cdots$$

Repeating this argument n times the sequence S must stop decreasing.

Ex. Let $>$ be a relation on $\mathbb{Z}_{\geq 0}^n$ that satisfies props (i) and (ii) in Def1 (~~monomial order~~). Show that $>$ is a well ordering $\Leftrightarrow$ the monomial $[0,0,0,\dots,0]$ ...

that '$>$' is a well ordering $\Longleftrightarrow$ the monomial $[0,0,0,\dots,0]$ is the least monomial.

CLO 2.3 A division algorithm for ideals in $k[x_1,\dots,x_n]$.

Given $f_1,\dots,f_s \in k[x_1,\dots,x_n]\setminus\{0\}$, $f \in k[x_1,\dots,x_n]$ to divide $f \div \{f_1,\dots,f_s\}$ we want to write

$$f = a_1 f_1 + a_2 f_2 + \dots + a_s f_s + r \quad \text{in } k[x_1,\dots,x_n].$$

quotients. remainder

Example. Suppose $f_1 = xy+1$, $f_2 = 1+y$, $f = -x + xy^2$.
Suppose we choose $<_{lex}$ with $x > y$.

$$f_1 = xy+1, \quad f_2 = y+1, \quad f = xy^2 - x$$

$a_1 = y$
$a_2 = -1$

LT

$\to f_1 = xy+1$, $f_2 = y+1$

LT

$$\begin{array}{rl}
 & xy^2 - x = f = p_1 \\
- & (a_1 f_1 = xy^2 + y) \\
\hline
 & -x - y = p_2 \\
- & (-x) \\
\hline
 & -y = p_3 \\
- & (a_2 f_2 = -y - 1) \\
\hline
 & 1 = p_4 \\
- & 1 \\
\hline
 & 0
\end{array}$$

$r = -x+1$.

$LM(p_i)$: $\overset{1}{xy^2} > \overset{2}{x} > \overset{3}{y} > \overset{4}{1}$

$a_1 = 0$
$a_2 = xy - x$

$f_2 = y+1$
$f_1 = xy+1$

$$\begin{array}{rl}
 & xy^2 - x \\
- & (xy^2 + xy) \\
\hline
 & -xy - x \\
-(-xf_2) \quad - & (-xy - x) \\
\hline
 & 0
\end{array}$$

$r = 0$

So $f = 0f_1 + \underline{a_2 f_2} \Rightarrow f \in \langle f_1, f_2 \rangle = \{h_1 f_1 + h_2 f_2 : h_1, h_2 \in \mathbb{Q}[x,y]\}$

The output of the $\div$ alg. is not unique unlike $k[x]$.

The problem is not the $\div$ algorithm. It's the basis $\{f_1, f_2\}$ for $I = \langle f_1, f_2 \rangle$.