MONOMIAL ORDERINGS

JOSH SWANSON

Contents

(This lecture was given in the Applied Algebraic Geometry topics course at the University of Washington on April 5th, 2017. It essentially follows [CLO15, §2.1-2.2].)

1. Motivation: Ideal Membership

Question 1.1. *Let $f \in k[x_1, \ldots, x_n]$ and let $I \subset k[x_1, \ldots, x_n]$ be an ideal. How can we check if $f \in I$?*

Remark 1.2. When $n = 1$, we have the following method. (Assume $I \neq \{0\}$.)

(1) Find $g(x)$ such that $I = \langle g(x) \rangle$.
(2) Apply division algorithm to get $f(x) = g(x)q(x) + r(x)$ with $r = 0$ or $\deg r < \deg g$.
(3) $f \in I$ if and only if $r = 0$.

For (1), the set of possible $g(x)$ is the set of minimal-degree elements of I. If we're instead given $I = \langle g_1(x), \ldots, g_m(x) \rangle$, the Euclidean algorithm provides us with $g(x)$.

Remark 1.3. When $n > 1$, things get complicated. (1) breaks down immediately; e.g. when $n = 2$, $I = \langle x, y \rangle$ can't be generated by a single element. (2) must then be modified to work with multiple $g(x)$'s simultaneously. Chapter 2 works towards a generalization of (3) to n variables. The second half of today's talk will focus on (2). The first half will lay some groundwork.

Date: April 2, 2017.

2. Monomial Orderings

2.1. Motivation.

Remark 2.1. Implicit in the 1-variable case is ordering monomials as

$$1 < x < x^2 < x^3 < \cdots .$$

This ordering shows up in the division algorithm by looking at leading monomials. Useful properties of this ordering include the following.

Property	Explanation	Usefulness
Total ordering	Any two monomials are comparable	"Leading term" makes sense
Well-ordering	Any (possible infinite) set of monomials has a unique minimum	Division algorithm terminates
Compatible with multiplication	$x^i < x^j$ implies $x^a x^i < x^a x^j$	Can predictably kill leading terms

The third property implies $\mathrm{LT}(x^a p(x)) = x^a \, \mathrm{LT}(p(x))$. This is important when we subtract off a multiple of the denominator to kill the current leading term in the division algorithm.

Remark 2.2. Sometimes it's convenient to think of the exponents of a monomial as a vector, as in

$$x_1^3 x_2^{17} x_4 \in k[x_1, \ldots, x_5] \Leftrightarrow (3, 17, 0, 1, 0) \in \mathbb{Z}^5_{\geq 0}.$$

If $\alpha := (3, 17, 0, 1, 0)$, we write

$$x^\alpha := x_1^3 x_2^{17} x_3^0 x_4^1 x_5^0.$$

2.2. Definition.

Definition 2.3. A *monomial ordering* $>$ on $k[x_1, \ldots, x_n]$ is a relation $>$ on $\mathbb{Z}^n_{\geq 0}$, or equivalently a relation $>$ on the monomials $\{x^\alpha : \alpha \in \mathbb{Z}^n_{\geq 0}\}$, satisfying:

(i) $>$ is a total (or linear) order on $\mathbb{Z}^n_{\geq 0}$.
(ii) If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.
(iii) $>$ is a well-ordering.

Remark 2.4. Property (i) means that $>$ is transitive and, for every $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, exactly one of the following is true:

$$\alpha > \beta, \qquad \alpha = \beta, \qquad \beta > \alpha.$$

Property (iii) means that for every non-empty $A \subset \mathbb{Z}^n_{\geq 0}$, there is an element $\alpha \in A$ such that for every $\beta \in A$ with $\beta \neq \alpha$, $\beta > \alpha$.

- Equivalently, any strictly decreasing sequence

$$\alpha(1) > \alpha(2) > \cdots$$

  eventually terminates. (This works for arbitrary totally ordered sets.)
- Equivalently, $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$. (This uses (ii).)

2.3. Examples.

Example 2.5. The ordering $1 < x < x^2 < x^3 < \cdots$ is the unique monomial ordering on $k[x]$.

Definition 2.6 (*Lexicographic order*)**.** For $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, we say

$$\alpha >_{\text{lex}} \beta \Leftrightarrow \text{leftmost non-zero entry of } \alpha - \beta \text{ is positive.}$$

Example 2.7. In increasing order for $n = 2$, we have

$$\begin{aligned}(0,0) <_{\text{lex}} (0,1) <_{\text{lex}} (0,2) <_{\text{lex}} \cdots <_{\text{lex}} \\ (1,0) <_{\text{lex}} (1,1) <_{\text{lex}} (1,2) <_{\text{lex}} \cdots <_{\text{lex}} \\ (2,0) <_{\text{lex}} (2,1) <_{\text{lex}} (2,2) <_{\text{lex}} \cdots .\end{aligned}$$

Definition 2.8 (*Graded lexicographic order*)**.** For $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, we say

$$\alpha >_{\text{grlex}} \beta \Leftrightarrow$$

$$|\alpha| := \sum_{i=1}^{n} \alpha_i > |\beta| := \sum_{i=1}^{n} \beta_i \qquad \text{or} \qquad |\alpha| = |\beta| \text{ and } \alpha >_{\text{lex}} \beta.$$

Example 2.9. $(1,2,3) >_{\text{grlex}} (3,2,0)$ while $(1,2,3) <_{\text{lex}} (3,2,0)$.

Definition 2.10 (*Graded reverse lex order*)**.** For $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, we say

$$\alpha >_{\text{grevlex}} \beta \Leftrightarrow$$

$$|\alpha| := \sum_{i=1}^{n} \alpha_i > |\beta| := \sum_{i=1}^{n} \beta_i \qquad \text{or} \qquad |\alpha| = |\beta| \text{ and the } \underline{\text{right}}\text{most non-zero entry of } \alpha - \beta \text{ is } \underline{\text{negative}}.$$

Example 2.11. We have:

- $(1,2,3) >_{\text{grevlex}} (3,2,0)$.
- $(1,2,3) <_{\text{grevlex}} (3,2,1)$, and $(1,2,3) <_{\text{grlex}} (3,2,1)$.
- $(1,3,1) >_{\text{grevlex}} (2,1,2)$, and $(1,3,1) <_{\text{grlex}} (2,1,2)$.

Remark 2.12. lex, grlex, and grevlex are all monomial orderings. lex is particularly simple, but it has no relationship with degrees. grlex fixes this issue. grevlex in practice tends to give nicer answers. grlex and grevlex agree for $n = 1$ or 2, and they both give $x_1 > \cdots > x_n$, though they differ for $n \geq 3$.

All three orderings depend on first choosing an ordering of $x_1, x_2, \ldots, x_n$. The descriptions above all use $x_1 > x_2 > \cdots > x_n$, though any of the other $n!$ choices could be used. Unless otherwise specified, this is the default convention. To go from grlex to grevlex, for same-degree monomials, we reverse the ordering of $x_1, \ldots, x_n$ and we reverse $>_{\text{lex}}$.

Example 2.13. Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x, y, z]$. We can write the terms of f in decreasing order with respect to any monomial ordering.

Monomial ordering	Decreasing f
lex	$-5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$
grlex	$7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$
grevlex	$4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$

3. Terminology

Definition 3.1. Let $f = \sum_\alpha c_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and let $>$ be a monomial order.

(i) The *multidegree* of f is

$$\text{multideg}(f) := \max(\alpha \in \mathbb{Z}^n_{\geq 0} : c_\alpha \neq 0) \in \mathbb{Z}^n_{\geq 0}.$$

(ii) The *leading coefficient* of f is

$$\text{LC}(f) := c_{\text{multideg}(f)} \in k^\times.$$

(iii) The *leading monomial* of f is

$$\text{LM}(f) := x^{\text{multideg}(f)}.$$

(iv) The *leading term* of f is

$$\text{LT}(f) := \text{LC}(f) \cdot \text{LM}(f).$$

Example 3.2. When $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x, y, z]$ and $>$ is $>_{\text{lex}}$, we have

$$\begin{aligned} \text{multideg}(f) &= (3, 0, 0), \\ \text{LC}(f) &= -5, \\ \text{LM}(f) &= x^3, \\ \text{LT}(f) &= -5x^3. \end{aligned}$$

Lemma 3.3. *Let $f, g \in k[x_1, \ldots, x_n]$ be non-zero polynomials. Then:*

(i) $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.
(ii) $\text{LT}(fg) = \text{LT}(f)\,\text{LT}(g)$.
(iii) *If $f + g \neq 0$, then* $\text{multideg}(f + g) \leq \max\{\text{multideg}(f), \text{multideg}(g)\}$*. If, in addition,* $\text{multideg}(f) \neq \text{multideg}(g)$*, then equality occurs.*

References

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.