

Assignment 3

Evan Curry Wilbur

March 5, 2023

2.2.2

Each of the following polynomials is written with its monomials ordered according to (exactly) one of lex, grlex, or grevlex order. Determine which monomial order was used in each case.

a. $f(x, y, z) = 7x^2y^4z - 2xy^6 + x^2y^2$

b. $f(x, y, z) = xy^3z + xy^2z^2 + x^2z^3$

c. $f(x, y, z) = x^4y^5z + 2x^3y^2z - 4xy^2z^4$

Solution.

a. grlex

b. grevlex

c. lex

□

2.2.3

Rewrite each of the following polynomials, ordering the terms using the lex order, the grlex order, and the grevlex order, giving $\text{LM}(f)$, $\text{LT}(f)$, and $\text{multideg}(f)$ in each case when the variables are ordered $z > y > x$

a. $f(x, y, z) = 2x + 3y + z + x^2 - z^2 + x^3$

b. $f(x, y, z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$

Solution.

a.

	Lex	Grlex	Grevlex
Polynomial	$x^3 + x^2 + 2x + 3y - z^2 + z$	$x^3 + x^2 - z^2 + 2x + 3y + z$	$x^3 + x^2 - z^2 + 2x + 3y + z$
$\text{LM}(f)$	x^3	x^3	x^3
$\text{LT}(f)$	x^3	x^3	x^3
$\text{multideg}(f)$	$(3, 0, 0)$	$(3, 0, 0)$	x^3

b.

	Lex	Grlex	Grevlex
Polynomial			
LM(f)			
LT(f)			
multideg(f)			

□

2.2.5

Show that grevlex is a monomial order according to Definition 1.

Solution.

□

2.2.6

Another monomial order is the **inverse lexicographic** or **invlex** order defined by the following: for $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$, $\alpha >_{\text{invlex}} \beta$ if and only if the rightmost nonzero entry of $\alpha - \beta$ is positive. Show that invlex is equivalent to the lex order with the variables permuted in a certain way. (Which permutation?)

Solution.

Lemma 1. Let (S, \leq) and (T, \preceq) be two partial orders and $f : S \rightarrow T$ be an order embedding such that for all $\alpha, \beta \in S$, $f(\alpha + \beta) = f(\alpha) + f(\beta)$. Then if T is a monomial ordering, so is S .

Proof. Let the above be given and suppose T is a monomial ordering. First, we show that (S, \leq) is a total ordering. Indeed, given some $\alpha, \beta \in S$, since (T, \preceq) is total, one and only one of the following must be true

1. $f(\alpha) < f(\beta)$
2. $f(\alpha) > f(\beta)$
3. $f(\alpha) = f(\beta)$.

In any of these three cases, by definition of an order embedding, the corresponding relation must be true. That is to say, if $f(\alpha) < f(\beta)$ then it must be the case that $\alpha < \beta$, and correspondingly for the remaining two possibilities. Thus S is totally ordered.

Next, we show that S is well-ordered. Let $A \subseteq S$ be some non-empty subset. Since $f(A) \subseteq T$ and T is well ordered, there must exist a smallest element $t \in f(A)$. Necessarily, since every order embedding is injective, there must exist

a unique element $a \in A$ such that $f(a) = t$. It will be shown that a is the smallest element of A . Indeed if there were to exist some $a' \in A$ such that $a' < a$ then $f(a') < f(a) = t$, contradicting the fact that t is the smallest element of $f(A)$. Hence (S, \leq) is well-ordered.

Finally, we show that if $\alpha, \beta, \gamma \in A$ with $\alpha > \beta$ then $\alpha + \gamma > \beta + \gamma$. Again by definition of an order embedding, we must have $f(\alpha) > f(\beta)$. Additionally, $f(\gamma) \in T$ and since T is a monomial ordering it follows that

$$\begin{aligned} f(\alpha) + f(\gamma) &> f(\beta) + f(\gamma) && \implies \\ f(\alpha + \gamma) &> f(\beta + \gamma) && \implies \\ \alpha + \gamma &> \beta + \gamma. \end{aligned}$$

Thus (S, \leq) is a monomial ordering. □

□

2.3.5

We will study the division of $f = x^3 - x^2y - x^2z + x$ by $f_1 = x^2y - z$ and $f_2 = xy - 1$.

- a. Compute using grlex order:

$$r_1 = \text{remainder of } f \text{ on division by } (f_1, f_2).$$

$$r_2 = \text{remainder of } f \text{ on division by } (f_2, f_1).$$

Your results should be *different*. Where in the division algorithm did the difference occur?

- b. Is $r = r_1 - r_2$ in the ideal $\langle f_1, f_2 \rangle$? If so, find an explicit expression $r = Af_1 + Bf_2$. If not, say why not.
- c. Compute the remainder of r on division by (f_1, f_2) . Why could you have predicted your answer before doing the division?
- d. Find another polynomial $g \in \langle f_1, f_2 \rangle$ such that the remainder on division of g by (f_1, f_2) is nonzero. Hint: $(xy + 1) \cdot f_2 = x^2y^2 - 1$, whereas $y \cdot f_1 = x^2y^2 - yz$
- e. Does the division algorithm give us a solution for the ideal membership problem for the ideal $\langle f_1, f_2 \rangle$? Explain your answer

Solution.

- a. On a separate sheet of paper, I computed the remainder to be

$$r_1 = x^3 - x^2z + x - z$$

$$r_2 = x^3 - x^2z$$

b. Yes

$$r = -(x^2y - z) - x(xy - 1)$$

- c. There is no need to compute the remainder since it must be $r = x - z$. This can be readily seen since neither $\text{LT}(f_1)$ or $\text{LT}(f_2)$ divide any of the terms in r .
- d. The polynomial $g = yz - 1 \in \langle f_1, f_2 \rangle$, but the remainder on division of g by (f_1, f_2) is -1 .
- e. No, even if a polynomial $g \in \langle f_1, f_2 \rangle$, it need not be the case that the remainder of g by (f_1, f_2) is zero.

□

2.3.9

The discussion around equation (2) of Chapter 1, §4 shows that every polynomial $f \in \mathbb{R}[x, y, z]$ can be written as

$$f = h_1(y - x^2) + h_2(z - x^3) + r,$$

where r is a polynomial in x alone and $\mathbf{V}(y - x^2, z - x^3)$ is the twisted cubic curve in \mathbb{R}^3 .

- Give a proof of this fact using the division algorithm. Hint: You need to specify carefully the monomial ordering to be used.
- Use the parametrization of the twisted cubic to show that $z^2 - x^4y$ vanishes at every point of the twisted cubic.
- Find an explicit representation

$$z^2 - x^4y = h_1(y - x^2) + h_2(z - x^3)$$

using the division algorithm.

Solution.

- Proof.* Fix the monomial ordering to be $>_{\text{invlex}}$ which is defined in **2.2.6**. Observe that, under this ordering, $\text{LT}(y - x^2) = y$ and $\text{LT}(z - x^3) = z$. Given some $f \in \mathbb{R}[x, y, z]$, the division algorithm yields q_1, q_2 , and $r \in \mathbb{R}[x, y, z]$ such that

$$f = q_1(y - x^2) + q_2(z - x^3) + r.$$

We need to show that r is a polynomial in x alone. By the division algorithm, there are two possibilities for r . Either $r = 0$ or r is a linear

combination, with coefficients in k , of monomials, none of which is divisible by any $\text{LT}(y - x^2), \text{LT}(z - x^3)$. In the first case, we may obviously express r as a polynomial in x alone as

$$r(x) = 0.$$

In the latter case, let's assume for contradiction (and without loss of generality!) that r is a polynomial of y as well. Well then at least one monomial of r has the variable y with exponent greater than 0. But this would imply that y divides that monomial. But this is a contradiction since the division algorithm guarantees that no monomial of r can be divisible by $\text{LT}(y - x^2) = y$. So it must be that r is a polynomial in x alone. \square

b. The parametrization of the twisted cubic is

$$\begin{aligned}x(t) &= t \\y(t) &= t^2 \\z(t) &= t^3.\end{aligned}$$

Substituting these for the expression gives

$$\begin{aligned}z^2 - x^4y &= (t^3)^2 - (t)^4(t^2) \\&= t^6 - t^4t^2 \\&= t^6 - t^6 \\&= 0\end{aligned}$$

and so it vanishes at every point of the twisted cubic.

c.

$$z^2 - x^4y = -x^4(y - x^2) + (z + x^3)(z - x^3)$$

\square

2.3.10

Let $V \subseteq \mathbb{R}^3$ be the curve parametrized by $(t, t^m, t^n), n, m \geq 2$.

- Show that V is an affine variety.
- Adapt the ideas in Exercise 9 to determine $\mathbf{I}(V)$.

Solution.

- a. We show that V is the affine variety $V(x^m - y, x^n - z)$. Given some $(x_0, y_0, z_0) \in V$ we have

$$\begin{aligned}x_0 &= t \\y_0 &= t^m \\z_0 &= t^n\end{aligned}$$

for some $t \in \mathbb{R}$ by the definition of V . Substituting these into the expressions for the affine variety give

$$\begin{aligned}x_0^m - y_0 &= t^m - t^m \\&= 0\end{aligned}$$

and

$$\begin{aligned}x_0^n - z_0 &= t^n - t^n \\&= 0.\end{aligned}$$

So the point is in the affine variety and therefore $V \subseteq V(x^m - y, x^n - z)$. For the other direction, pick some $(x_0, y_0, z_0) \in V(x^m - y, x^n - z)$. By definition

$$\begin{aligned}x_0^m &= y & \text{and} \\x_0^n &= z.\end{aligned}$$

If we let $t = x_0$ then substituting t for x_0 in the expressions above give

$$\begin{aligned}y_0 &= t^m \\z_0 &= t^n.\end{aligned}$$

But this is exactly the definition of the parametrization V . So $V(x^m - y, x^n - z) \subseteq V$. Hence $V = V(x^m - y, x^n - z)$ is an affine variety.

- b. We will show that $\langle x^m - y, x^n - z \rangle = \mathbf{I}(V(x^m - y, x^n - z))$. **Lemma 7** on page 34 of the textbook says that

$$\langle x^m - y, x^n - z \rangle \subseteq \mathbf{I}(V(x^m - y, x^n - z)),$$

so we only need to show the other inclusion. Fix the monomial ordering to be $>_{\text{invlex}}$ and take some $f \in \mathbf{I}(V(x^m - y, x^n - z))$. With the division algorithm we can write

$$f = q_1(x^m - y) + q_2(x^n - z) + r$$

for $q_1, q_2, r \in \mathbb{R}[x, y, z]$. We show that r is a polynomial in x alone. Indeed, if this weren't the case, just like in the previous exercise, one of the monomials of r would be divisible by y or z . But this contradicts the division

algorithm theorem since the leading terms of $x^m - y$ and $x^n - z$ are y and z respectively. So it must be that $r \in \mathbb{R}[x]$. But then $f \in \langle x^m - y, x^n - z \rangle$

$$0 = f(t, t^m, t^n) = 0 + 0 + r(t)$$

for every t . But this implies that r is the zero polynomial. Therefore $f \in \langle x^m - y, x^n - z \rangle$ and $\langle x^m - y, x^n - z \rangle \supseteq \mathbf{I}(\mathbf{V}(x^m - y, x^n - z))$. Therefore,

$$\langle x^m - y, x^n - z \rangle = \mathbf{I}(\mathbf{V}(x^m - y, x^n - z)).$$

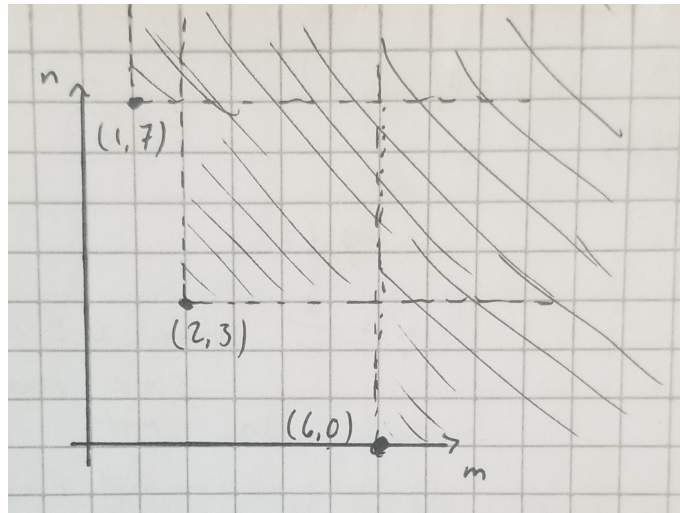
□

2.4.3

Let $I = \langle x^6, x^2y^3, xy^7 \rangle \subseteq k[x, y]$.

- In the (m, n) -plane, plot the set of exponent vectors (m, n) of monomials $x^m y^n$ appearing in elements of I .
- If we apply the division algorithm to an element $f \in k[x, y]$, using the generators of I as divisors, what terms can appear in the remainder?

Solution.



For part (b), the only terms that can appear in the remainder are linear combinations of monomials that are not in the ideal. Using **Lemma 2** on page 70 of the textbook, we can list every monomial not in the ideal:

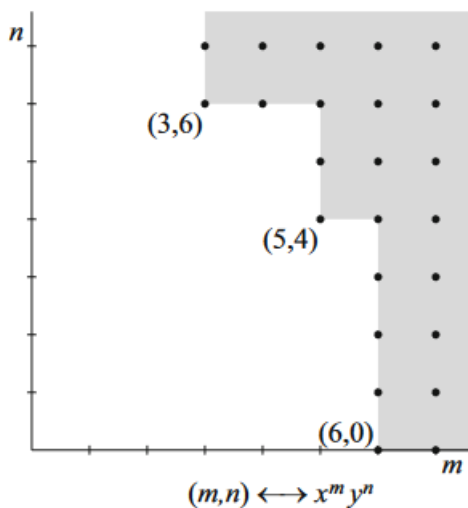
$$A = \{x^m y^n \mid (m < 6 \wedge n < 3) \vee (m < 2 \wedge n < 7) \vee (m < 1)\}.$$

So any linear combination with coefficients in k of the elements in A will give a possible remainder. □

2.4.4

Let $I \subseteq k[x, y]$ be the monomial ideal spanned over k by the monomials x^β corresponding to β in the shaded region shown at the top of the next page.

- Use the method given in the proof of Theorem 5 to find an ideal basis for I .
- Find a minimal basis for I in the sense of Proposition 7.



Solution.

- First, we find the projection to be $J = \langle x^3 \rangle$. Since we have $x^3 y^6 \in I$, then $m = 6$. So we get the following “slices”

$$\begin{aligned} J_0 = J_1 = J_2 = J_3 &= \langle x^6 \rangle \\ J_4 = J_5 &= \langle x^5 \rangle. \end{aligned}$$

So

$$I = \langle x^6, x^6 y, x^6 y^2, x^6 y^3, x^5 y^4, x^5 y^5, x^3 y^6 \rangle.$$

- Since the number of generators of I is relatively small, we can do this by hand (or just look at the picture provided!)

$$I = \langle x^6, x^5 y^4, x^3 y^6 \rangle.$$

□

2.4.9

Suppose we have the polynomial ring $k[x_1, \dots, x_n, y_1, \dots, y_m]$. Let us define a monomial order $>_{\text{mixed}}$ on this ring that mixes lex order for x_1, \dots, x_n , with grlex order for y_1, \dots, y_m . If we write monomials in the $n+m$ variables as $x^\alpha y^\beta$, where $\alpha \in \mathbb{Z}_{\geq 0}^n$ and $\beta \in \mathbb{Z}_{\geq 0}^m$, then we define

$$x^\alpha y^\beta >_{\text{mixed}} x^\gamma y^\delta \iff x^\alpha >_{\text{lex}} x^\gamma \text{ or } x^\alpha = x^\gamma \text{ and } y^\beta >_{\text{grlex}} y^\delta.$$

Use Corollary 6 to prove that $>_{\text{mixed}}$ is a monomial order. This is an example of what is called a *product order*. It is clear that many other monomial orders can be created by this method.

2.5.1

Let $I = \langle g_1, g_2, g_3 \rangle \subseteq \mathbb{R}[x, y, z]$, where $g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$ and $g_3 = x - yz^4$. Using the lex order, give an example of $g \in I$ such that $\text{LT}(g) \notin \langle \text{LT}(g_1), \text{LT}(g_2), \text{LT}(g_3) \rangle$.

2.5.7

If we use grlex order with $x > y > z$, is $\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$ a Gröbner basis for the ideal generated by these polynomials? Why or why not?

2.5.8

Repeat Exercise 7 for $I = \langle x - z^2, y - z^3 \rangle$ using the lex order. Hint: The difficult part of this exercise is to determine exactly which polynomials are in $\langle \text{LT}(I) \rangle$.

2.5.9

Let $A = (a_{ij})$ be an $m \times n$ matrix with real entries in row echelon form and let $J \subseteq \mathbb{R}[x_1, \dots, x_n]$ be an ideal generated by the linear polynomials $\sum_{j=1}^n a_{ij}x_j$ for $1 \leq i \leq m$. Show that the given generators form a Gröbner basis for J with respect to a suitable lexicographic order. Hint: Order the variables corresponding to the leading 1's before the other variables.