7 Monomial Orderings: [CLO] §2.2

Definition 7.1. A **monomial ordering** $<$ (also called a **term ordering**) is a an ordering of $\mathbb{N}_0^n$ such that

(1) $<$ is a total ordering: for any $\alpha, \beta \in \mathbb{N}_0^n$, exactly one of the following is true: $\alpha < \beta$, or $\alpha = \beta$, or $\alpha > \beta$.

(2) $<$ respects addition: $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$.

(3) $<$ is a well ordering: any nonempty subset of $\mathbb{N}_0^n$ has a least element.

Assume that a specific term ordering is chosen. We order monomials in $k[\bar{x}]$ by applying the term ordering to the exponent vector of the monomials. For $f \in k[x_1, \ldots, x_n]$ we will write its terms in descending term order. We use $\mathrm{LT}(f)$ for the leading term, $\mathrm{LM}(f)$ for the leading monomial, $\mathrm{LC}(f)$ for the leading coefficient, and $\mathrm{LE}(f)$ for the leading exponent (the exponent of the leading term). IVA calls $\mathrm{LE}(f)$ the multidegree and uses $\mathrm{mdeg}(f)$.

The most common term orderings are lexicographic (lex), graded lexicographic (glex or grlex), and graded reverse lexicographic (grevlex). See IVA for their definitions.

Two articles by Robbiano, (*Theory of graded structures*, 1986, and *Term orderings on the polynomial ring* , 1985) classify all possible term orders. These papers broaden the context for term orders, so are useful to discuss.

Here is a summary of the main steps used to classify monomial orderings in Robbiano's papers.

(1) Any term ordering on $\mathbb{N}_0^n$ extends in a unique way to a term ordering on $\mathbb{Z}^n$.

(2) Any term ordering on $\mathbb{Z}^n$ extends in a unique way to a term ordering on $\mathbb{Q}^n$.

(3) Any term ordering on $\mathbb{Q}^n$ is such that $(\mathbb{Q}^n)^+$ (the set of elements larger than $(0, \ldots, 0)$) is convex, and $(\mathbb{Q}^n)^-$ (the set of elements smaller than $(0, \ldots, 0)$) is also convex. By convex we mean that for all $\alpha, \beta \in (\mathbb{Q}^n)^+$, and r a rational between 0 and 1, $r\alpha + (1-r)\beta \in (\mathbb{Q}^n)^+$.

(4) The convexity property for a term order on $\mathbb{Q}^n$ implies that the ordering is continuous. That means $\forall \alpha \in \mathbb{Q}^n$ if there exists a neighborhood U_α such that $U_\alpha - \{\alpha\} \subseteq (\mathbb{Q}^n)^+$ then $\alpha \in (\mathbb{Q}^n)^+$ (and similarly for $-$).

(5) Thus, every ordering on $\mathbb{Q}^n$ extends to a continuous order respecting addition on $\mathbb{R}^n$. (The extension may not be unique).

I will just explain the first step above (the second is similar, the rest are harder). Suppose that $<$ is an ordering on $\mathbb{N}_0^n$. Let $\alpha, \beta \in \mathbb{Z}^n$ (so α and β may have negative terms). There is some $\gamma \in \mathbb{N}_0^n$ such that $\alpha + \gamma$ and $\beta + \gamma$ both have positive components (Check this!). We will say that $\alpha < \beta$ if $\alpha + \gamma < \beta + \gamma$. Since there are many choices for γ, we have to check consistency: $\alpha + \gamma < \beta + \gamma$ iff $\alpha + \gamma' < \beta + \gamma'$ for all γ' large enough so that $\alpha + \gamma'$ and $\beta + \gamma'$ are in $\mathbb{N}_0^n$. (Check this!)

Once Robbiano has shown that each term order extends to an ordering on $\mathbb{R}^n$ he can make use of continuity. The result is this classfication theorem.

Theorem 7.2. *Every term ordering on $\mathbb{N}_0^n$ is determined by some sequence $u_1, u_2, \ldots, u_s \in \mathbb{R}^n$, in the following sense.*

> *$\alpha < \beta$ iff there is some $t \in \{1, 2, \ldots, s\}$ such that $\alpha \cdot u_i = \beta \cdot u_i$ for $i < t$ and $\alpha \cdot u_t < \beta \cdot u_t$.*

The $\cdot$ means the dot product. In other words, $\alpha < \beta$ if $\alpha \cdot u_1 < \beta \cdot u_1$ and $\alpha > \beta$ if $\alpha \cdot u_1 > \beta \cdot u_1$. If this test is inconclusive, that is $\alpha \cdot u_1 = \beta \cdot u_1$, then use u_2 to compare. Continue on till you get a definitive answer.

We may also use matrix notation. Taking exponent vectors α, β as column vectors, write each u_i as a row vector, with $u_i = [u_{i1}, u_{i2}, \ldots, u_{in}]$. Then compute

$$\begin{bmatrix} u_{11} & u_{12} & \ldots & u_{1n} \\ u_{21} & u_{22} & \ldots & u_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ u_{s1} & u_{s2} & \ldots & u_{sn} \end{bmatrix} \begin{bmatrix} \alpha_1 - \beta_1 \\ \alpha_2 - \beta_2 \\ \cdots \\ \alpha_n - \beta_n \end{bmatrix}$$

If the top most nonzero term is positive then $\alpha > \beta$ if it is negative then $\alpha < \beta$.

If there are n vectors $u_1, \ldots u_n$ and they are linearly independent, then any unequal α and β will be distinguished by one of these tests (Check!). It is possible for fewer than n vectors to determine a total ordering. This is because α and β have integer entries. An example for $n = 2$ is $u_1 = [1, \sqrt{2}]$. If α and β have integer entries and $\alpha \cdot u_1 = \beta \cdot u_1$ then $\alpha = \beta$.

Exercises 7.3. (HW) Monomial orderings: A menagerie (See [CLO] §2.4 #10-12). Each of these have fairly brief answers.

(a) For $n = 3$, list the monomials of total degree 2 or less in increasing order for grevlex and for grlex. Illustrate: for each, show a triangle with the monomials of degree 2 and the path of increasing order.

(b) Let $n = 3$. For each of the monomial orderings lex, grlex and grevlex, find vectors u_1, u_2, u_3 which determine that ordering.

(c) Find a total ordering on $\mathbb{N}_0^3$ which is determined by a single vector u_1. Explain why the one vector is sufficient.

(d) Find necessary and sufficient condition(s) on the u_i to ensure that a group ordering on $\mathbb{N}_0^n$ is also a well-ordering and therefore a monomial ordering.

(e) Find necessary and sufficient condition(s) on the u_i that ensure that a monomial ordering on $\mathbb{N}_0^n$ has no element α that is larger than an infinite number of other elements of $\mathbb{N}_0^n$. Justify your answer.

(f) Let $>_1$ be a monomial ordering on $\mathbb{N}_0^{m_1}$ and let $>_2$ be a monomial ordering on $\mathbb{N}_0^{m_2}$. Generalize the discussion in IVA II.4#10 to define the product order of $>_1$ and $>_2$.
Explain how to obtain vectors defining the product order from the vectors defining the individual orders.

Discussion

For those that have worked with Groebner bases previously, here is a discussion and experimentation problem in Sage. Choose a field: $\mathbb{Q}$ or some finite field that might be easier to work with. Create the polynomial ring in x, y over the field with lex $y > x$. Choose a set S of points in the plane (start with a small number then increase to larger sets). Find a Groebner basis for the set of points. Look at the Groebner basis and interpret what you see geometrically. Note that when the points have distinct x-coordinates the geometry of the GB is simpler. Experiment with examples in which there may be 2, 3 or even more points with the same x-coordinate.

8 Division in $k[\bar{x}]$: [CLO] §2.3

Given a term order $<$ on $k[\bar{x}]$, each $f \in k[\bar{x}]$ has a leading term. We use $\mathrm{LT}(f)$, for the leading term $\mathrm{LM}(f)$ for the leading monomial, $\mathrm{LE}(f)$ for the leading exponent, and $\mathrm{LC}(f)$ for the leading coefficient.

When using lex order I will write each monomial with the lowest variable on the left and the highest on the right. This is to encourage thinking of the lex order $y > x$ for $k[x, y]$ as treating the ring as a polynomial ring in y with coefficients from $k[x]$.

Example 8.1. Let $g = 7xy^2 + 5x^4y + x^4 + 3x^2$. With lex and $y > x$ the leading term is $7xy^2$ the LM is xy^2 the LC is 7 the LE is $(2, 1)$. With glex and $y > x$ the leading term is $5x^4y$ the LM is x^4y, the LC is 4 and the LE is $(4, 1)$.

With lex and $x > y$, we can write the polynomial as $5yx^4 + x^4 + 3x^2 + 7y^2x$. The LT is $5yx^4$ again. At some point it may be useful to think of the polynomial as an element of $(k[y])[x]$, in which case the leading term would be $(5y + 1)$. (But that is a diversion at this moment.)

In Section 2.3 the authors introduce a deterministic algorithm for dividing a polynomial h by a sequence of polynomials $[f_1, f_2, \ldots, f_s]$. The order of the f_i impacts the result.

Exercises 8.2. Let $h = x^2y+xy^2+y^2$, and let $f_1 = xy-1$, and $f_2 = y^2-1$.

(a) In §2.3 Examples 2,4, the authors use lex order with $x > y$ and divide h by f_1, f_2, and by f_2, f_1. These give two different pairs of quotients and different remainders. Call the two remainders r_1 and r_2. They show that $r_1 - r_2$ is in the ideal $\langle f_1, f_2\rangle$. (Note: I wish that, using lex with $x > y$, they had written h in the form $yx^2 + y^2x + y^2$ so that each term is in the form $\mathrm{LC} * \mathrm{LM}$ as an element of $k[y][x]$.)

(b) Do the same problem with lex and $y > x$. (Now write h in the form for $k[x][y]$ with descending term order and each term written $\mathrm{LC} * \mathrm{LM}$). Again show that the difference of remainders is in the ideal.

Let $F = [f_1, f_2, \ldots, f_t]$. We will write $\overline{f}^h$ for the remainder of h after division by F.

Exercises 8.3. (HW) Two division problems

(a) [CLO] §2.3#5

(b) Do the same work as the previous problem, but use $f_1 = x^2 - y$, $f_2 = xz - y$ and $g = x^3 - x^2y - x^2z$.

(c) [CLO] §2.3#9,10

Exercises 8.4. Finding an element h of $\langle F \rangle$ whose remainder upon division by F is h itself.

(a) [CLO] §2.3 #6, 7

Exercises 8.5. Term orders and division

(a) What conditions ensure the sequences of u_i and v_i define the same term order?

(b) Be able to apply the division theorem. You may get different results if you change the ordering of the polynomials, or if you change the term order.

Note that the multivariable division algorithm is not as simple as it is with one variable.

(1) It depends on the term order $<$.

(2) It depends on the ordering of the elements in F.

We would like to eliminate the dependence on the order of elements in F. As we will see this is possible for well chosen F.

9 Dickson's Lemma and the Hilbert Basis Theorem

Hilbert's Basis Theorem says that if every ideal in R is finitely generated then every ideal in $R[x]$ is also finitely generated. In [CLO], the Hilbert Basis Theorem is proven for polynomial rings over a field as a straightforward consequence of Dickson's lemma, which says that every *monomial ideal* in $k[\bar{x}]$ is finitely generated. Here I summarize the steps in the [CLO] treatment of Dickson's lemma and how it leads to the broader Hilbert Basis Theorem. I will also prove the general Hilbert Basis theorem. The proof for the general theorem may be somewhat easier to follow than Dickson's lemma because the notation is a bit simpler. The structure of the proofs is essentially the same.

Dickson's lemma

Lemma 9.1 (Dickson: [CLO] §2.4 Theorem 5)**.** *Every monomial ideal has a finite generating set. More precisely, for $A \subseteq \mathbb{N}_0^n$ there is a finite $A' \subseteq A$ such that*

$$\langle x^\alpha : \alpha \in A \rangle = \langle x^\alpha : \alpha \in A' \rangle$$

Furthermore, we may take A' so that $x^\alpha \nmid x^\beta$ for all $\alpha, \beta \in A'$.

The justification for the last sentence of the theorem should be fairly clear. If $\alpha, \beta \in A$ are such that x^α divides x^β then any monomial divisible by x^β is also divisible by x^α so we may remove β from A and still have a generating set. Removing all such unnecessary monomials gives the result.

In order to prove the Hilbert Basis Theorem, we introduce a term order, $<$. Relative to this order we get from any ideal in $k[\bar{x}]$, a monomial ideal called the ideal of leading terms (it could also be called the ideal of leading monomials).

Definition 9.2. Let $<$ be a term order on $k[\bar{x}]$. For an ideal I let $\mathrm{LT}(I) = \{\mathrm{LT}(f) : f \in I\}$. The **ideal of leading terms of** I is $\langle \mathrm{LT}(I) \rangle$.

Since leading terms are just a constant multiple of the leading monomials, we have $\langle \mathrm{LM}(I) \rangle = \langle \mathrm{LT}(I) \rangle$.

Dickson's lemma says that there is a finite subset of $\mathrm{LT}(I)$ that generates the monomial ideal $\langle \mathrm{LT}(I) \rangle$. Each of these is the leading term of some polynomial in I. Thus we have

Proposition 9.3 ([CLO] 2.5 Proposition 3)**.** *There exist $g_1, g_2, \ldots, g_s \in I$ such that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g(t)) \rangle$.*

From this we get the Hilbert Basis Theorem.

Theorem 9.4 (Hilbert Basis: [CLO] Theorem 4)**.** *Let I be an ideal in $k[\bar{x}]$. Let $g_1, \ldots, g_t$ be elements of I such that* $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ *generate* $\langle \mathrm{LT}(I) \rangle$*. Then $I = \langle g_1, \ldots, g_t \rangle$.*

Proof. Let $A = \mathrm{LE}(I) = \{\mathrm{LE}(f) : f \in I\}$. Then $\langle LT(I) \rangle = \langle x^\alpha : \alpha \in A \rangle$ and by Dickson's theorem there is some finite subset $A' = \{\alpha_1, \ldots, \alpha_t\}$ of A such that $\{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ generate $\langle \mathrm{LT}(I) \rangle$. Furthermore, the x_i^α are leading terms of elements of I, say $x^{\alpha_i} = \mathrm{LT}(g_i)$. Now let $f \in I$. Dividing f by G we get $f = a_1 g_1 + \cdots + a_t g_t + r$ and the remainder r has no terms divisible by any of the x^{α_i} (terms are only placed in the remainder when they are not divisible by any leading term of a g_i). Now $f - \sum a_i g_i = r \in I$. If $r \neq 0$ then $\mathrm{LT}(r) \in \langle \mathrm{LT}\, I) \rangle$ so $\mathrm{LT}(r)$ is divisible by some x^{α_i}. This gives a contradiction. Thus $r = 0$. □

Hilbert Basis Theorem more generally

Definition 9.5. A ring R satisfies the **ascending chain condition (ACC)** when every ascending chain of ideals stabilizes. That is, if $I_1 \subseteq I_2 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals in R indexed by $\mathbb{N}$ then there is some j such that $A_i = A_j$ for all $i > j$. A ring satisfying the ACC is called **Noetherian** after Emmy Noether.

Proposition 9.6. *Let R be a ring. R satisfies the ACC if and only if every ideal is finitely generated.*

Proof. Suppose R does not satisfy the ACC, so there is some $I_1 \subset I_2 \cdots$ with each ideal properly contained in the next. Let $K = \cup_{j=1}^{\infty} I_j$. It is straightforward to show that K is an ideal. I claim that K is not finitely generated. Let $h_1, \ldots, h_s$ be any finite set of elements in K. Each h_i is an element of one of the ideals I_j so there is some $m \in \mathbb{N}$ such that all of the h_i lie in I_m. Consequently, $\langle h_1, \ldots, h_s \rangle \subseteq I_m$ and so $\langle h_1, \ldots, h_s \rangle \neq K$.

Conversely, suppose that R contains an ideal I that is not finitely generated. We can choose $f_i \in I$ inductively so that $f_i \notin \langle f_1, \ldots, f_{i-1} \rangle$. This gives a strictly increasing sequence of ideals in R, so R does not satisfy the ACC. □

Theorem 9.7 (Hilbert Basis)**.** *Let R satisfy the ACC. Then so does the polynomial ring $R[y]$.*

Proof. Let $I \subseteq R[y]$. For $k \geq 0$ let

$$J_k = \langle \Big\{ r \in R : ry^k \text{ is the leading term of some element of } I \Big\} \rangle$$

One can verify that

(1) J_k is an ideal in R.

(2) $J_k \subseteq J_{k+1}$.

This ascending chain has a greatest element, let it be J_m. We know J_m is finitely generated so let

$$J_m = \langle s_1, s_2, \ldots, s_n \rangle$$

For each s_i let $g_i \in I$ have leading term $s_i y^m$. Let $G = \{g_1, \ldots, g_n\}$.

Each J_k is finitely generated. Let's choose p large enough so that J_k is generated by p elements for all $k < m$. (If J_k is generated by fewer elements, that is ok, we can make the extra generators 0.) Now let $J_k = \langle r_{k1}, \ldots, r_{kp} \rangle$ and choose elements $f_{k1}, \ldots, f_{kp}$ in I such that f_{ki} has leading term $r_{ki} y^k$. Let $F_k = \{f_{k1}, \ldots, f_{kp}\}$.

Now consider the ideal generated by $F_0 \cup F_1 \cup \cdots \cup F_{m-1} \cup G$. I claim it is equal to I, which shows I is finitely generated. Since I was arbitrary $R[y]$ satisfies the ACC.

To prove the claim, take an arbitrary element $h \in I$ divide it by $F_0 \cup F_1 \cup \cdots \cup F_{m-1} \cup G$. You will get 0. This proves the claim. □

Corollary 9.8. *For a field k, $k[\bar{x}]$ satisfies the ACC.*

Proof. k itself does. Apply the Hilbert Basis Theorem inductively. □

Exercises 9.9. Verify these claims from the material above.

(a) If $I_1 \subseteq I_2 \subseteq I_3 \cdots$ is an ascending chain of ideals in R prove that $\cup_{j=1}^{\infty} I_j$ is an ideal.

(b) Prove claims (1) and (2) in the proof of the Hilbert Basis Theorem.

Groebner Basis

The term "basis" is a bit improper in the following definition, since we commonly think of basis in terms of vector spaces. An element of a vector space has a unique representation as a sum of basis elements. An ideal has a generating set, and there may be more than one way to express a given element of an ideal as a combination of the generators. It would be more proper to use the term generating set instead of basis, but Groebner basis is more concise and has become the standard terminology.

Definition 9.10. Consider $k[\bar{x}]$ with a fixed term order $<$. Let I be an ideal in $k[\bar{x}]$ and let $G \subseteq I$ be such that $\langle \mathrm{LT}(g) : g \in G \rangle = \langle \mathrm{LT}(I) \rangle$. Then G is called a **Groebner basis** for I. If no $g_1, g_2 \in G$ satisfy $\mathrm{LT}(g_1) | \mathrm{LT}(g_2)$ then we say G is a **minimal Groebner basis**.

Let $\Delta_I = \mathbb{N}_0^n \setminus \mathrm{LE}(I)$. We call Δ_I (and the set of associated monomials) the **footprint** of I.

Suppose that G is a minimal Groebner basis, that each $g \in G$ is monic ($\mathrm{LC}(g)$ is 1) and that for each $g \in G$ all terms of $g - \mathrm{LM}(g)$ have exponent in Δ_I. Then G is a **reduced Groebner basis**.

The monomials $\{x^\alpha : \alpha \in \Delta_I\}$ form a (*true*) basis for $k[\bar{x}]/I$ as a vector space over k.

Proposition 9.11 ([CLO] §2.6 Proposition 1)**.** *Given $f \in I$ there is a unique $g \in I$ and unique $r = \sum_{\alpha \in \Delta(I)} r_\alpha x^\alpha$ such that $f = g + r$. Furthermore, for any Groebner basis, G (and any ordering of G), r is the remainder when f is divided by G.*

Proof. We can divide any $f \in k[x_1, \ldots, x_n]$ by a Groebner basis $G = \{g_1, \ldots, g_t\}$ and get $f = \sum a_i g_i + r$ with remainder r having terms with exponents in $\Delta(I)$. Let $g = \sum a_i g_i$. We have shown existence of g, r. We must show uniqueness. Suppose $f = g + r$ and $f = g' + r'$. Then $g + r - (g' + r') = 0$ so $g - g' = r' - r$. I claim $g = g'$ and $r = r'$. If not $g - g' \in I$, so $\mathrm{LE}(g - g') \notin \Delta(I)$. On the other hand $\mathrm{LE}(r - r') \in \Delta(I)$ since all terms of r and r' have exponents in $\Delta(I)$. This gives a contradiction, so $g = g'$ and $r = r'$.

We have also shown that r is the remainder when f is divided by G, for any Groebner basis G. □

Note: this is all based on a fixed term order!

Proposition 9.12 ([CLO] §2.7 Proposition 6)**.** *A nonzero ideal I has a unique reduced Groebner basis.*

Proof. For existence, let $G = \{g_1, \ldots, g_t\}$ be a minimal Groebner basis. Divide g_1 by $g_2, \ldots g_t$. We get $g_1 = \sum_{i-2}^t a_i g_i + r_1$. Furthermore $r_1 \in I$, and r_1 has the same leading term as g_1 because $\mathrm{LT}(g_1)$ is not divisible by $\mathrm{LT}(g_i)$ for $i > 1$ (since the Groebner basis is minimal). Replace g_1 with r_1 and we still have a minimal Groeber basis, but no term of r_1 is divisible by $\mathrm{LT}(g_i)$ for $i = 2, \ldots, t$. Proceed similarly with g_i for $i = 2, \ldots, t$.

To prove uniqueness, suppose G and G' are both reduced Groebner bases. For $g \in G$ there is a unique $g' \in G'$ (by minimality) such that $\mathrm{LT}(g) = \mathrm{LT}(g')$. Then $g - g'$ cancels the leading term so each term of $g - g'$ is in $\Delta(I)$. On the other hand $g - g' \in I$, so we must have $g - g' = 0$.

□

These important results generalize the Division Theorem. Given a fixed term order $<$ for any $f \in k[x_1, \ldots, x_n]$ and ideal I, there is a unique remainder of f

divided by I. We have also solved the ideal description problem in a satisfying way: there is a *unique* reduced Groebner basis. We have an easy test for ideal membership, divide by the Groebner basis and see if the result is 0.

The next and key question is how to compute a Groebner basis, akin to the question for $k[x]$: how do we compute the gcd of two polynomials in one variable? The answer in one indeterminate is the Euclidean algorithm. It is not so simple with several indeterminates.

Exercises 9.13. Recall that a Groebner basis is defined relative to a fixed monomial ordering $<$.

(a) IVA 2.3#9, 10 Implicitization of a twisted rational curve.

(b) IVA 2.6 #1, 4, uniqueness of remainder.

(c) IVA 2.5 #7, 8; 2.6 #9, 10 computation of GB.

(d) IVA 2.7 #2, 3.

(e) IVA 2.5 #9, 2.7 #9,10 linearpolynomials and GB.

(f) IVA 2.7#5-7, minimal GB.

(g) IVA 2.7#14

Exercises 9.14. Syzygy polynomials

(a) IVA 2.6#5, 6 compute the syzygy polynomial.

(b) IVA 2.6#8, 12 syzygy and monomial multiples.

Here is some SageMath code

```
FF = FiniteField(19)
PF.<x,y> = PolynomialRing(FF, 2, order =’deglex’)
f = PF.random_element(2, 6)
g = PF.random_element(2, 6)
I = PF.ideal([f,g])
G= I.groebner_basis()
LMs = [g.lm() for g in G]
LEs = [m.degrees() for m in LMs]

Here is a little experiment to count the number of different
footprints for two sorta randomly generated degree 2 polynomials.

A = [(0, 3), (2, 0), (1, 1)]
B = [ (2,0), (0,2)]

cntA = 0
cntB = 0
for i in range(100):
    f = PF.random_element(2, 6)
    g = PF.random_element(2, 6)
    I = PF.ideal([f,g])
    G= I.groebner_basis()
    LMs = [g.lm() for g in G]
    LEs = [m.degrees() for m in LMs]
    if LEs == A:
        cntA = cntA +1
    elif LEs == B:
        cntB = cntB +1
    else:
        print LEs

This is a function to compute the syzygy polynomial (Spoly) of f and g.

def Spoly(f,g):
    m = f.lm()
    n = g.lm()
    h = LCM(m,n)
    return PF(h/m)*f/f.lc() - PF(h/n)*g/g.lc()
```

10 Syzygy Polynomials

Definition 10.1. Let $\alpha, \beta \in \mathbb{N}_0^n$. For $i = 1, \ldots, n$, let $\gamma_i = \max(\alpha_i, \beta_i)$. We will call $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ the $\mathrm{LCM}(\alpha, \beta)$. We will also call x^γ the $\mathrm{LCM}(x^\alpha, x^\beta)$.

It should be clear that $\mathrm{LCM}(x^\alpha, x^\beta)$ is the smallest monomial that is a multiple of both x^α and x^β. Using LCM for α and β is a small abuse of terminology.

Definition 10.2. Let $f, g \in k[x_1, \ldots, x_n]$. The syzygy polynomial of f and g (also called the S-polynomial) is

$$S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} f - \frac{x^\gamma}{\mathrm{LT}(g)} g$$

where $\gamma = \mathrm{LCM}(\mathrm{LE}(f), \mathrm{LE}(g))$.

In other words, if the leading monomial of f is x^α and the leading monomial of g is x^β , then x^γ is the smallest monomial divisible by both $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ and $\dfrac{x^\gamma}{\mathrm{LT}(f)} f$ and $\dfrac{x^\gamma}{\mathrm{LT}(g)} g$ both have leading term x^γ (the leading coefficients are both 1). The S-poly results from taking the smallest multiples of f and g that will give cancellation of leading terms. Thus $\mathrm{LM}(S(f,g)) < \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$. Of course if $f, g \in I$ then $S(f,g) \in I$ since it is a polynomial combination of f and g.

Buchberger's algorithm

Let $F = \{f_1, \ldots, f_s\}$ and let $I = \langle F \rangle$ be the ideal generated by F. We would like to have

(1) a test to see if F is a Groebner basis for I, and

(2) an algorithm to compute a Groebner basis for I if F is not one.

The algorithm is essentially this: for various $f_1, f_2 \in F$ compute $S(f_1, f_2)$ then divide the result by F and get a remainder r with no terms divisible by leading terms of polynomials in F. Since $S(f_1, f_2) \in I$ and we divided by $F \subseteq I$ we must have $r \in I$. In addtion, since we divided by F, $\mathrm{LT}(r)$ is not divisible by $\mathrm{LT}(f)$ for all $f \in F$. If $r \neq 0$, we add r to our set F and repeat the process: choose two elements of $F \cup \{r\}$, compute their S-poly, divide by $F \cup \{r\}$ to get a remainder, if it is nonzero throw it into our set of polynomials and continue.

Theorem 10.3 (S-poly. [CLO] §2.6 Theorem 6.)**.** *Let $G = \{g_1, \ldots, g_t\}$ be a generating set for I. G is a Groebner basis for I iff $\overline{S(g_i, g_j)}^G = 0$ for all i, j.*

Futhermore the algorithm described above terminates with a Groebner basis for I after a finite number of steps.

Note: $\overline{h}^F$ means the remainder when h is divided by F where F is an ordered set of polynomials, $F = f_1, \ldots, f_t$. The symbol $h \to_F r$ means that $h = \sum a_i f_i + r$ and $\mathrm{LE}(f) \geq \mathrm{LE}(a_i f_i)$ for all i with $a_i \neq 0$. We'll discuss this in class.

Exercises 10.4. (HW) Consider the ideal I generated by $x - y^2$ and $xy^2 - x$ in $\mathbb{R}[x, y]$

- **(a)** Using lex $x > y$,
  - (1) Find a GB for I;
  - (2) Identify a basis for $\mathbb{R}[x, y]/I$ and show how to compute the product of two arbitrary monomials from this basis;
  - (3) Working over $\mathbb{R}$, identify all the maximal ideals containing I;
  - (4) Localize at each of these maximal ideals and simplify the ideal.
- **(b)** Redo the previoius problems using lex $y > x$.
- **(c)** Redo the previous problems using glex $x > y$ or $y > x$ (your choice).

Exercises 10.5. Buchberger and Groebner bases

- **(a)** II.8 #1, 2, 6, Groebner basis computations,
- **(b)** II.8 #7 implicitization of parametrically defined surface.
- **(c)** II.9 #1, 2 standard representation and Groebner bases.
- **(d)** II.10 #1, 2, 3 syzygy and determinental ideals.

Exercises 10.6. Groebner basis and computations. In $k[x, y, z]$ with the grlex term order with $x > y > z$, let $I = \langle g_1, g_2, g_3, g_4 \rangle$ where,

$$g_1 = x^2 - x \qquad g_2 = xy - z$$
$$g_3 = xz - z \qquad g_4 = yz - z^2$$

- **(a)** Show that $S(g_1, g_2)$ and $S(g_3, g_4)$ reduce to 0 when divided by $G = [g_1, g_2, g_3, g_4]$. If you did this for all pairs g_i, g_j you would find that this is a Groebner basis for I (trust me).
- **(b)** Identify a basis for $k[x, y, z]/I$ using this Groebner basis. It may help to graph the leading terms of G.
- **(c)** Write down a general element of $k[x, y, z]/I$.
- **(d)** Explain how to compute in $k[x, y, z]/I$. In particular, show that $y^i z^j = z^{i+j}$.
- **(e)** Show that the associated variety is the union of two lines defined by ideals I_1 and I_2. Show that I_1 contains I and similarly for I_2.

(f) Analyze the ring map

$$k[x,y,z]/I \longrightarrow k[x,y,z]/I_1 \times k[x,y,z]/I_2$$

Is it injective? Is it surjective?