Plan for PURE Math 2012 Seminar

Week 1

Monday: Polynomials, affine space, affine varieties, parametrizations (Chapter 1, §§1,2,3)
Tuesday: Ideals (Chapter 1, §4)
Wednesday: Polynomials in one variable, division and Euclidean algorithms (Chapter 1, §5 – motivate by determination of $\mathbf{I}(C)$ for twisted cubic from §4)
Thursday: Monomial orders in $k[x_1, \ldots, x_n]$ (Chapter 2, §2)

PURE Math 2012 – Seminar
Week 1 Discussions – Polynomials, Varieties, and Algorithms

Note: Solutions for each day's problems will be due on the next scheduled "class day". Only one write-up per group is required.

Day 1: Getting started with varieties

Goals

Today, we want to start off the discussion part of the seminar by thinking about the definition of a variety presented earlier in the morning.

Since this is also the first of the discussion meetings of our seminar, a few words about this way of working are probably in order. In these discussion meetings, we will be aiming for *collaborative learning* – that is, for an integrated group effort in analyzing and attacking the discussion questions. The ideal is for everyone in each of the groups to be fully involved in the process. The idea is that, by actively participating through talking about the ideas yourself in your own words, you can come to a better first understanding of what is going on than if you simply listen to someone else talk about it. These meetings will also help prepare you for your work in a research group.

However, it must be said that to get the most out of this kind of work, you may have to adjust some of your preconceptions. In particular:

- This is *not a competition* in any sense. You and your fellow group members are working as a team, and the goal is to have everyone understand what the group does fully.
- At different times, it is inevitable that different people within the group will have a more complete grasp of what you are working on and others will have a less complete grasp. Dealing with this a group setting is excellent preparation for real work in a team; it also offers opportunities for significant educational experiences:
  a) If you feel totally "clueless" at some point, you need to feel free to ask questions and even pester your fellow group members until the point has been worked out to your full satisfaction. (Don't forget, the others may be jumping to unwarranted conclusions, and your questions may save the group from pursuing an erroneous train of thought!)
  b) On the other hand, when you think you do see something, you may need to explain it carefully to others. (Don't forget, the *absolutely best* way to make sure you really understand something is to try to explain it to someone else(!) If you are skipping over an important point in your thinking, it can become very apparent when you set out to explain your ideas to a team member.)

  In short, everyone has important things to contribute, and everyone will contribute in different ways at different times.

Background

Recall that given a collection of polynomials

$$f_1(x_1, \ldots, x_n), \ldots, f_s(x_1, \ldots, x_n)$$

the *variety* $\mathbf{V}(f_1, \ldots, f_s)$ is just the set of all points in k^n where *all* of the polynomials f_i are zero *simultaneously*. In symbols:

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = \text{ for all } 1 \leq i \leq s\}.$$

Discussion Questions

A) Sketch (or describe in words if necessary!) the following varieties:

1) $\mathbf{V}(y - x^3 + 3x + 1) \subset \mathbf{R}^2$, and also in $\mathbf{R}^3$, with coordinates x, y, z.
2) $\mathbf{V}(y^2 - x^6) \subset \mathbf{R}^2$ (what does it mean when the defining equation factors as this one does: $y^2 - x^6 = (y - x^3)(y + x^3)$?)
3) $\mathbf{V}(x^2/4 + y^2/9 - 1, xy) \subset \mathbf{R}^2$
4) $\mathbf{V}(x^2 + y^2 - z^2 - 4, z - 3) \subset \mathbf{R}^3$
5) $\mathbf{V}(x^2 + y^2 + z^2 - 9, x^2 + y^2 - 4, y - z) \subset \mathbf{R}^3$
6) Consider the variety
$$C = \mathbf{V}(y^2 - x(x-1)(x-2)) \subset \mathbf{R}^2$$
(C is a curve in $\mathbf{R}^2$ called an *elliptic curve* – it is not an ellipse itself, but related curves are involved in questions like computing arc lengths of parts of ellipses.) For which x is it possible to solve the equation of the variety for $y \in \mathbf{R}$? How many y-values are there for each of these x's? This curve is *symmetric* under reflection across a line – which line? Generate an accurate sketch of this curve.

B) The geometry of varieties has many interesting "real-world" applications. Here is a first taste of one of them. A robot arm in $\mathbf{R}^2$ consists of three rigid, straight segments of lengths $3, 2$, and 1. One end of the segment of length 3 is anchored at the origin, and the other is attached to the segment of length 2, which is attached at its other end to the segment of length 1. The "hand" is at the far end of the segment of length 1. The attachment of the arm at the origin and the joints between the three segments allow rotations through any angles.

1) Draw a picture of the robot arm in a "typical position".
2) How many variables do you need to specify the "state" of the arm, and what are the equations of the variety of possible states?
3) Describe the set of possible positions of the hand. For each of these positions, is there just one configuration of the arm that places the hand there or more than one?

C) We can also ask whether a set $S \subset k^n$ *is a variety*. That is, we can ask whether $S = \mathbf{V}(f_1, \ldots, f_s)$ for polynomials $f_i \in k[x_1, \ldots, x_n]$ as above.

1) Consider $S = \{(x, y) \in \mathbf{R}^2 : y = \cos(x)\}$ (the graph of the cosine function). Suppose that $f(x, y)$ is a polynomial in $\mathbf{R}[x, y]$ that is zero at every point of S. If you substitute a constant value y_0 in the range $-1 \leq y_0 \leq 1$ for y, how many roots does the resulting equation $f(x, y_0) = 0$ have? What does this say about f? (Be careful! Think about writing f as a polynomial in x whose coefficients are polynomials in y:

$$f(x, y) = a_n(y)x^n + \cdots + a_1(y)x + a_0(y)$$

Is S a variety?

2) Let M be a positive integer and let $S \subset \mathbf{Z}^2$ be the set of points with integer coordinates such that $1 \leq x, y \leq M$. Is S a variety? Why or why not?
3) Generalizing part 2, show that *every finite set S in $\mathbf{R}^2$ is a variety.* (Hint: one method begins by showing that there is always a rotated (x', y') coordinate system such that the x'-coordinates of the points in S are *distinct*.)

D) Problem 13 of "IVA", Chapter 1, §3. (Note: Try to work out the implicit equation both ways from the Hint in the problem to check your work. If you don't recall the vector cross product and the way it can be used to get a normal vector for a plane, we will show that to you.)

Day 2: Ideals

Background

As we saw in lecture earlier, the "defining equations" $f_i = 0$ of a variety given as $V = \mathbf{V}(f_1, \ldots, f_s)$ are never *the only* polynomial equations that are satisfied at all points of the variety. We can always look at other polynomials of the form

$$f = g_1 f_1 + \cdots + g_s f_s \tag{3}$$

(where the g_i are any polynomials at all in the same set of variables), and we get other polynomials that vanish at all points of V. The polynomials f in (3) are the elements of the *ideal*

$$I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n].$$

An ideals is a non-empty collection I of polynomials that is

- closed under sums, and
- closed under multiplication by arbitrary polynomials $g \in k[x_1, \ldots, x_n]$.

Given a variety V, we can also produce an ideal by considering the collection of *all polynomials that vanish at every point of V*:

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0, \text{ all } (a_1, \ldots, a_n) \in V\}.$$

Discussion Questions

A) In this problem, we will develop a way to tell whether two ideals are equal.

1) Let's start with an example. We ask: Are $I = \langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3\rangle$ and $J = \langle x^2 - 4, y^2 - 1\rangle$ equal or not? Show that both $2x^2 + 3y^2 - 11$ and $x^2 - y^2 - 3$ are in J by finding polynomials A_1, B_1 and A_2, B_2 such that

$$\begin{aligned} 2x^2 + 3y^2 - 11 &= A_1(x^2 - 4) + B_1(y^2 - 1) \\ x^2 - y^2 - 3 &= A_2(x^2 - 4) + B_2(y^2 - 1) \end{aligned}$$

Explain why this shows $I \subseteq J$. Similarly, decide whether both $x^2 - 4$ and $y^2 - 1$ are in I by seeing whether there exist polynomials C_1, D_1 and C_2, D_2 such that

$$\begin{aligned} x^2 - 4 &= C_1(2x^2 + 3y^2 - 11) + D_1(x^2 - y^2 - 3) \\ y^2 - 1 &= C_2(2x^2 + 3y^2 - 11) + D_2(x^2 - y^2 - 3) \end{aligned}$$

Are I and J equal? Why or why not?

2) Now, consider this question in general. Let I be an ideal, and $g_1, \ldots, g_t$ be a collection of polynomials. Show that $\langle g_1, \ldots, g_t\rangle \subseteq I$ if and only if $g_i \in I$ for all $i = 1, \ldots, t$.
3) Use part 1 to develop a general "test" to perform to determine whether two ideals $I = \langle f_1, \ldots, f_s\rangle$ and $J = \langle g_1, \ldots, g_t\rangle$ are equal.

B) Let C be the curve in $\mathbf{R}^3$ parametrized by

$$\alpha(t) = (t, t^3, t^5)$$

1) Show that $f_1 = y - x^3$ and $f_2 = z - x^5$ are elements of $\mathbf{I}(C)$.
2) Prove that C is a variety.
3) Following what the text does for the twisted cubic, determine $\mathbf{I}(C)$.

C) Let I be an ideal in $k[x_1, \ldots, x_n]$. Let $\sqrt{I}$ be the collection of all polynomials f such that some power of f is in I (the smallest power that "works" can be different for different f). $\sqrt{I}$ is called the *radical* of I, since it consists of all polynomials that are "ℓ-th roots" of elements of I, for all $\ell \geq 1$. In symbols,

$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] : f^\ell \in I, \text{ for some } \ell \geq 1\}$$

1) For example, explain why $f = x + y$ is in $\sqrt{I}$ for $I = \langle x^4 + y^4, xy\rangle$.
2) Show that $\sqrt{I}$ is closed under products by all $g \in k[x_1, \ldots, x_n]$.
3) Show that $\sqrt{I}$ is closed under sums. (That is, if $f \in \sqrt{I}$ and $g \in \sqrt{I}$ so $f^\ell \in I$, and $g^m \in I$ for integers $\ell, m \geq 1$ (not necessarily the same), you need to show there is some $p \geq 1$ such that $(f + g)^p \in I$. What p work?)
4) What do parts 2 and 3 say about $\sqrt{I}$?

D)

1) Show that $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$ for all ideals I.
2) An ideal I is said to be a *radical ideal* if $\sqrt{I} = I$. Show that if V is variety, then $\mathbf{I}(V)$ is a radical ideal.

Day 3: Algorithms

Background

In class today, we studied our first examples of *algorithms*, or step-by-step procedures for performing a particular computation. The two examples we looked at were:

- the *division algorithm* in $k[x]$,
- the *Euclidean algorithm* for gcd's in $k[x]$.

Today, we want to work through a few examples, following the "pseudo-code" description of the algorithm (as if you were a computer, yourself, following a program!) Then we will want to develop an extension of the Euclidean algorithm that, together with the gcd, also produces polynomials A and B satisfying

$$gcd(f, g) = Af + Bg.$$

Discussion Questions

A) Work through the division algorithm in $\mathbf{Q}[x]$ step by step (see page 38 in "IVA"), dividing $g(x) = 2x^3 + 3x - 5$ into $f(x) = x^5 - x^4 + x^2 - 2x + 1$. At the start of each pass through the main loop, what are the values of q, r? Show that the equation $f = qg + r$ is always true. (This is an example of a "loop invariant" – using these is often important in developing an algorithm or proving that an algorithm is correct.)

B) Work through the Euclidean algorithm step by step (see page 41) to compute the gcd of f and g from part A. What are the values of h,s at the start of each pass through the loop?

C) Do Problem 10 in Chapter 1, §5 of "IVA". (Hint: Read the given Hint carefully and think about the idea of "loop invariants" from above.) "Run" your algorithm on the example from questions A and B, and check your results.

Comment: Although this "extended Euclidean algorithm" is also available as a "built-in" command in Sage and other computer algebra systems, you will also see how to code it as a Sage procedure in a lab meeting.

Day 4: Monomial Orders

In class today, we introduced the definition of a *monomial order* in the polyomial ring $k[x_1, \ldots, x_n]$. This was an ordering $>$ on the monomials x^α (or equivalently on the exponent vectors α) such that:

1) $>$ is a total (linear) order on vectors with nonnegative integer components. (This means that for every pair of monomials x^α and x^β, exactly one of the following is true: either $x^\alpha > x^\beta$, or $x^\alpha = x^\beta$, or $x^\beta > x^\alpha$.)
2) For all α, β, γ, we have
$$\alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma$$
3) $>$ is a well-ordering. (In other words, every non-empty subset of monomials or exponent vectors has a smallest element under $>$).

Today, we want to think about some of the implications of this definition.

Discussion Questions

A) To practice with monomial orders, do Problems 1,2 from Chapter 2, §2 of "IVA".

B) Show that in $k[x, y]$, the graded lexicographic and graded reverse lexicographic orders are the same. Is this true for $n > 2$?

C) Suppose we try to define an order $>$ by omitting the first part of the definition of the graded lexicographic order, so that $\alpha > \beta$ if the rightmost entry in $\alpha - \beta$ is negative. Do we get a monomial order? Why or why not?

D) We could also try to define an order $>_w$ by comparing the "total weights" of two monomials with respect to a given weight vector w on the variables. That is, for a monomial x^α, we think of the variable x_i as having weight w_i (from the vector w). We compute $\alpha \cdot w = \alpha_1 w_1 + \cdots + \alpha_n w_n$ and say $x^\alpha >_w x^\beta$ if $\alpha \cdot w > \beta \cdot w$.

1) Let $n = 2$ and $w = (3, 5)$. Is $>_w$ a monomial order? Why or why not?
2) Let $n = 2$ again and $w = (1, \sqrt{2})$. Same question.
3) What property of the components of the vector $w \in \mathbf{R}^n$ would imply that $>_w$ *does* define a monomial order on $k[x_1, \ldots, x_n]$? (The fact that $\sqrt{2}$ is not a rational number in part 2 is an important clue, but it is not the whole story!)