SIMU 1999 – Gröbner Bases Seminar
Week 1 Discussions – Polynomials, Varieties, and Algorithms

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.

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 the following varieties in $\mathbf{R}^2$:
   1) $\mathbf{V}(y - x^3 + 1)$
   2) $\mathbf{V}(y^2 - x^4)$
   3) $\mathbf{V}(x^2 + y^2/9 - 1)$
   4) $\mathbf{V}(x^2 + y^2 - 4, x - y^2 + 1)$
   5) 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 and similar problems.) 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 a lot of 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.
   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) Given a set $S \subset k^n$, what does it mean to say that S *is a variety*? Explain in your own words, but precisely.
   2) Consider $S = \{(x, y) \in \mathbf{R}^2 : y = \sin(x)\}$ (the graph of the sine 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?

3) Let M be a positive integer and let $S \subset \mathbf{Z}^2$ be the set of points with integer coordinates such that $1 \leq x, y \leq M + 1$. Is S a variety?

Challenge Problem Generalizing part 3 of C, show that every finite set in $\mathbf{R}^2$ is a variety.

Day 2: Parametrizations of Varieties

Background

A portion of our work this summer will involve the relation between the following two ways to represent geometric objects:

a) as the *sets of solutions of one or more "implicit" equations*
b) as the *images of parametrizations*.

The standard description of a variety in affine space k^n

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) : f_i(a_1, \ldots, a_n) = 0, 1 \leq i \leq s\}$$

is an example of the first kind above. For instance, the circle of radius 2 with center at $(1, 2)$ is the variety

$$V((x-1)^2 + (y-2)^2 - 4) \tag{1}$$

given by the equation $(x-1)^2 + (y-2)^2 - 4 = 0$. But there is also another way to describe the same circle – as the image of a parametrization mapping such as

$$\alpha(t) = (1 + 2\cos(t), 2 + 2\sin(t)). \tag{2}$$

We get the full circle, traced out once, for $0 \leq t \leq 2\pi$.

Each of these ways to describe objects is useful. If we want to program a computer to draw the object, for instance, then a *parametrization* is extremely good to have. With the parametrization (2) in hand, for instance, we could "plug in" lots of (closely-spaced) t values, then "connect the dots" to draw the curve. (This is exactly what programs like Maple do for parametric plotting of curves!) However, if we want to determine whether a given point is in the geometric locus (or within a given distance, etc.), then *implicit equations* are much better, since we only need to substitute the coordinates of the point in question into the right equations to determine the answer to our question.

Our discussion questions today will be two examples where we work out a way to parametrize a given variety, and two others where we "go the other way" (produce an implicit equation from a parametrization).

Discussion Questions

A) Problem 2 of "IVA", Chapter 1, §3.
B) Problem 8 of "IVA", Chapter 1, §3.
C) Problem 9 of "IVA", Chapter 1, §3 (recall the trig identities $\sin^2 t + \cos^2 t = 1$ and $\tan t = \sin t / \cos t$).
D) Problem 13 of "IVA", Chapter 1, §3. (Note: Try to work out the implicit equation both ways from the Hint to check your work. If you have not seen 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.)

Challenge Problem

Problems 14,15 from "IVA", Chapter 1, §3 (see the discussion of Bézier cubics in the text).

Day 3: Ideals

Background

As we saw in lecture earlier, the "defining equations" $f_i = 0$ of a variety $V = \mathbf{V}(f_1, \ldots, f_s)$ 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*

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

Ideals are non-empty collections I of polynomials that are

- 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 find 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 and $J = \langle g_1, \ldots, g_t \rangle$ are equal.

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

$$\alpha(t) = (t, t^3, t^4)$$

1) Show that $z - xy \in \mathbf{I}(V)$.
2) Prove that C is a variety.
3) Following what we did 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 $\sqrt{I}$?

Challege Problem

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 4: 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 a modification of the Euclidean algorithm to produce polynomials A and B such that

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

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 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". "Run" your algorithm on the example from questions A, B, and check your results. (You will also see how to code this algorithm as a Maple procedure in the lab meeting today.)