Lecture 8

Algebraic sets

8.1 Goals

1. Understand that polynomial functions are functions with special properties.

2. (Terminology.) Know what vanishing loci are.

3. (Notational.) Know what $V(I)$ stands for—so you know what both I and $V(I)$ are.

4. (Definitional.) Know the definition of an algebraic set.

5. Begin to explore what it means for a subset of $\mathbb{R}^n$ to be an algebraic set.

6. Begin to explore the connections between the algebra of functions and the geometry of vanishing loci. (For example, multiplication of functions becomes union of shapes.)

8.2 Polynomials are functions

You are probably already used to thinking of polynomials as functions. Let's be explicit what we mean. If you have a polynomial

$$p(x) = 3 - \pi x + \frac{1}{2}x^7$$

you know that p is a function from $\mathbb{R}$ to $\mathbb{R}$. For example, if you plug in the number -1 for x, you obtain

$$p(-1) = \frac{7}{2} + \pi.$$

On the other hand, last class, we were only treating polynomials as things that we could add and multiply (i.e., as elements of some ring). The power of interesting mathematical objects is that there is more than one way to think about them. So today, we will focus a little more on the idea that polynomials define functions.

8.2.1 Polynomials as special kinds of functions

Even when we are only considering one variable x (as opposed x, y and z) polynomials inhabit a special place in the world of functions.

You know from calculus the derivative of a polynomial is another polynomial, and that in fact, you can take as many derivatives as you want of a polynomial. This is contrast to a function like $f(x) = |x|$, which does not have a derivative at the origin.

Another special thing about polynomials is: so long as you know how to add and multiply, you can evaluate polynomials very efficiently. For example, regardless of the degree of a polynomial p, I bet you can plug in $x = 2$ and tell me what $p(2)$ is to a precision only limited by the precision of the coefficients of p. This is contrast to functions like $\sin(x)$, where it would take you a long time (or a calculator/computer) to tell me $\sin(2)$ up to ten decimal places.

Polynomials are special for many other reasons, which we will not see in this course. But when we fixate on the operations of addition and multiplication, we saw in the last lecture that an invariant called *degree* is available for polynomials, and degrees allow us to prove all kinds of wonderful facts about the ring of polynomials (see the exercises from last lecture).

8.2.2 Polynomials in many variables are also (special) functions

In case you haven't seen it before, let me emphasize that elements of $\mathbb{R}[x, y]$ can also be thought of as functions. For example, if you have a polynomial $p \in \mathbb{R}[x, y]$ like

$$p(x, y) = 3 - x + y + \frac{1}{2}x^2y + y^3$$

then p defines a function from $\mathbb{R}^2$ to $\mathbb{R}$.

Example 8.2.1. At $(x, y) = (1, 4)$, we can compute that

$$p(1,4) = 3 - 1 + 4 + \frac{1}{2}(1)^2 \cdot 4 + (4)^3 = 72.$$

Likewise, an element of $\mathbb{R}[x, y, z]$ defines a function from $\mathbb{R}^3$ to $\mathbb{R}$.

8.2.3 Digression: How do you know when a function is polynomial?

It probably doesn't surprise you to know that none of the following are polynomial functions on $\mathbb{R} = \mathbb{R}^1$:

$$f(x) = |x|, \qquad g(x) = \sin(x), \qquad h(x) = e^x, \qquad f(x) = \begin{cases} 1 & x \text{ is rational} \\ 0 & x \text{ is irrational} \end{cases}.$$

Likewise, none of the following are algebraic functions on $\mathbb{R}^2$:

$$f(x,y) = |x|, \qquad g(x,y) = \sin(x)y, \qquad h(x,y) = e^x + y^2, \qquad f(x,y) = \begin{cases} 1 & x \text{ is rational} \\ 0 & x \text{ is irrational} \end{cases}.$$

However, it can often be quite subtle to prove whether or not a given function is polynomial! For example, consider the functions

$$D(x,y) = \text{The distance of } (x,y) \text{ from the circle } x^2 + y^2 = 3$$

or the function

$$E(x,y) = \text{The smallest perimeter among all triangles of area } xy.$$

or the variant

$$F(x,y) = \text{The smallest perimeter among all rectangles of area } x^2y^2.$$

The point is that some functions are not presented to us in an obviously polynomial form. It can be incredibly difficult to know whether a random function can, or cannot, be presented as a polynomial function. For example, it turns out that D and F above are polynomial functions, but E is not.

Oftentimes, to prove whether a function is polynomial involves using (i) knowledge of the field of math that gave rise to the function, and (ii) knowledge of how polynomials fit into that field of math.

Example 8.2.2. As an example, if you want to prove that e^x is not a polynomial function, you'll want to use tools of calculus or analysis. (Though you might know it yet, in fact, any function of the form $blah^x$ requires some analysis to define for all real numbers.)

Here is one proof: e^x has the property that it is its own derivative. However, taking the derivative of a polynomial always reduces the degree of the polynomial (and hence no polynomial is equal to its derivative)—with the exception of the zero polynomial $p(x) = 0$. Clearly e^x is not equal to the zero function, so e^x is not equal to any polynomial.

The reason I bring this up is because you might feel like you're *supposed* to be able to tell whether a given function is polynomial. But you're not, because whether you can tell depends heavily on how the function is presented to you. Thankfully, most of this course will *not* require you to be able to tell when some crazily-presented function is polynomial or not. But who knows what the rest of your mathematical life holds in store.

8.3 Algebraic sets

We talked about how polynomials are special kinds of functions. Here is one illustration:

Proposition 8.3.1. Let $f : \mathbb{R} \to \mathbb{R}$ be a non-zero polynomial. Then there are only finitely many[1] values of x for which $f(x) = 0$. (In fact, the number of such x is less than or equal to the degree of f.)

We haven't talked about something called the Euclidean algorithm so we can't prove the proposition yet, but you might find the proposition intuitive. For example, if you've ever graphed polynomial functions in one variable, you've probably noticed that the graph only crosses the x-axis finitely many times.

Remark 8.3.2. The assumption that f is polynomial is necessary. For example, $f(x) = \sin(x)$ has infinitely many zeroes.

On the other hand, there may of course be many non-polynomial functions with finitely many zeroes. For example, $g(x) = \sin(x) + x^2$. So the converse of the proposition is false.

[1] By the way, there may be no such values of x. Because zero is a finite number, "finitely many values of x" also includes the case of "no value of x."

So aside from all the special properties of polynomial functions we've talked about before, another interesting property is that the set of zeroes of a polynomial are special. (When f is a polynomial in one variable, the above proposition tells us that the set of zeroes is always *finite*.) Let's give these sets of zeros a name:

Definition 8.3.3. Let $f : X \to \mathbb{R}$ be a function. Then the *zero locus*, or the *vanishing locus* of f is the set

$$V(f) = \{x \in X \mid f(x) = 0\}.$$

In words, $V(f)$ is the set of all elements on which f vanishes.

More generally, given a collection I of functions, the zero/vanishing locus of I is the set of points on which every function in that collection vanishes. We write

$$V(I)$$

for this vanishing locus.

Example 8.3.4. Make sure to work through the following examples:

(a) Consider the function from $\mathbb{R}$ to $\mathbb{R}$ given by $f(x) = x^2 - 1$. Then the zero locus of f is the set $\{1, -1\}$ consisting of two points.

(b) Consider the function from $\mathbb{R}^2 \to \mathbb{R}$ given by $f(x, y) = x^2 + y^2 - 1$. Then the zero locus of f is the unit circle.

(c) Consider the functions $f(x, y) = x^2 + y^2 - 18$ and $g(x, y) = y - x$. These are functions $\mathbb{R}^2 \to \mathbb{R}$. Let $I = \{f, g\}$. Then $V(I)$ consists of two elements: $(3, 3)$ and $(-3, -3)$.

Remark 8.3.5. Suppose that $S = V(I)$ and $T = V(J)$. Then $S \cap T = V(I \cup J)$. Here is one proof:

$$\begin{aligned} x \in V(I) \cap V(J) &\iff (\forall f \in I,\ f(x) = 0) \& (\forall g \in J,\ g(x) = 0) \\ &\iff \forall f \in I \cup J,\ f(x) = 0 \\ &\iff x \in V(I \cup J). \end{aligned}$$

Note that as we go from line to line, we do not just see logical implications, but logical equivalences: Those $\iff$ are "if and only if" symbols. So make sure you know not only how to logically justify moving down in the string of statements, but also how to move up in the string of statements.

Remark 8.3.6. In general, suppose you have a polynomial $f \in R[x_1, \ldots, x_n]$ where R is now an arbitrary commutative ring. Then again, f is a function from R^n to R. And one can still speak of the vanishing locus $V(f)$ as a subset of R^n.

A lot of modern algebraic geometry is more concerned with $R = \mathbb{C}$ then with $R = \mathbb{R}$, but we'll still with mostly $R = \mathbb{R}$ so that we can visualize things more easily. However, I would strongly encourage you to take a few afternoons trying to figure out ways you can visualize subsets of $\mathbb{C}^2 \cong \mathbb{R}^4$. It is a worthwhile task for any mathematical mind!

Remark 8.3.7. Let $R = \mathbb{Z}$, fix $k \geq 2$, and consider the polynomial $f(x, y, z) = x^k + y^k - z^k$. What is $V(f)$? (It is some subset of $\mathbb{Z}^3$, but which one?)

When $k = 2$, there are many elements in $V(f)$. You can find Pythagorean triples like $(3, 4, 5)$ for example.

But for $k \geq 3$, the only immediate answers are answers involving 0s. For example, $(x, y, z) = (a, 0, a)$ is in $V(f)$ for all k and for all $a \in \mathbb{Z}$. But are there other non-trivial elements on $V(f)$ that don't involve 0?

Fermat's Last Theorem states that in fact, when $k \geq 3$, every element of $V(f)$ must have some coordinate equal to 0. This was claimed by Fermat in a notebook without proof in 1637, and finally proven hundreds of years later by Andrew Wiles in 1994.

What this is meant to show is that, actually, understanding $V(f)$ for arbitrary f can be very hard! Indeed, in the scope of all mathematics, our civilization can only solve a tiny fraction of the problems one could state. So it's okay if some $V(f)$ and some $V(I)$ feel a little inaccessible. What's important is that you explore and have some success in some examples, so that you can feel like there are some concrete instances that you *can* work out.

8.3.1 Algebraic sets defined

If the vanishing loci of polynomial functions are special sets, then we can choose to study only such special sets. Let's give these special sets a name:

Definition 8.3.8. Let S be a subset of $\mathbb{R}^n$. We say that S is an *algebraic set* (with respect to the base ring $\mathbb{R}$) if there is some collection I of polynomial functions for which $S = V(I)$.

More generally, if one fixes a base ring R, then we say that a subset $S \subset R^n$ is algebraic (with respect to R) if there is some collection of polynomials $I \subset R[x_1, \ldots, x_n]$ for which $S = V(I)$.

Remark 8.3.9. By elaborating on Remark 8.3.5, one sees that S is an algebraic set if it is the common zero set of a collection of polynomials. That is, if there is some collection I of polynomials so that S is the intersection of all the $V(f)$ for $f \in I$.

Remark 8.3.10. Given an algebraic set S, there may be *many* different choices of I. For example, let $S = \{0\} \subset \mathbb{R}$ be the set consisting only of the origin in $\mathbb{R}$. Then all of the following are choices of I for which $S = V(I)$:

(a) $I = \{x\}$.

(b) $I = \{x, x^2, x^3\}$.

(c) $I = \{x, x^2, x^3, x^4, \ldots\}$. (Note in particular that I need not be finite.)

(Despite the last example, we will often deal with examples where we know that I can be chosen to be finite.)

8.3.2 Examples of algebraic sets

Example 8.3.11. (a) Let $S = \{x_1, \ldots, x_n\}$ be a finite collection of points in $\mathbb{R}$. Then S is an algebraic set! For example, consider the polynomial

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n).$$

Then $S = V(f)$.

(b) Let S be some subset of $\mathbb{R}$ with infinitely many elements, and for which $S \neq \mathbb{R}$. By Proposition 8.3.1, we see that S is not algebraic.

(c) Let S be the unit circle in $\mathbb{R}^2$. Then S is algebraic. For example, consider the polynomial $f(x, y) = x^2 + y^2 - 1$. Then $S = V(I)$.

(d) Let $S \subset \mathbb{R}^2$ consist of one point, say $(1, 2)$ in $\mathbb{R}^2$. Then S is an algebraic set. To see this, consider the two functions $f(x, y) = x - 1$ and $g(x, y) = y - 2$, and let $I = \{f, g\}$. Then $V(I) = S$.

(e) Let $S \subset \mathbb{R}^2$ be the two-element set $\{(1,1),(-1,1)\}$. Then S is algebraic. To see this, consider the functions $f(x,y) = x^2 - y$ and $g(x,y) = y - 1$ and set $I = \{f, g\}$. Then $V(I) = S$.

(f) Let $S \subset \mathbb{R}^2$ be the set of all points $(x,y) \in \mathbb{R}^2$ for which $y = e^x$. (This is the graph of the function e^x.) It turns out S is not an algebraic set.

(g) Let $S \subset \mathbb{R}^2$ be the union of the x-axis and the y-axis. Then S is an algebraic set. In fact, let $f(x,y) = xy$. Then $V(f) = S$.

Remark 8.3.12. Let S be an algebraic set. Then S may also be the zero locus of some finite collection of non-polynomial functions—for example, the set $S = \{0\} \subset \mathbb{R}$ is also the zero locus of the (non-polynomial) function $f(x) = 1 - e^x$.

Remark 8.3.13. We have seen that the only algebraic subsets of $\mathbb{R}$ are either finite subsets, or are equal to $\mathbb{R}$. However, let me emphasize that the choice of base ring matters very much when contemplating what is and is not algebraic.

As an example, let $R = \mathbb{Q}$. Then the zero polynomial $0 \in \mathbb{Q}[x]$ has zero locus given by $\mathbb{Q}$ itself. So $\mathbb{Q}$ is an algebraic subset. On the other hand, $\mathbb{Q} \subset \mathbb{R}$ is an infinite set, so it couldn't be algebraic. Right?

Wrong, because we need to always keep in mind what our base ring is. $\mathbb{Q}$ *is* algebraic over the base ring $\mathbb{Q}$, but is not algebraic over the base ring $\mathbb{R}$.

8.3.3 Algebraic sets as geometric objects

Many beautiful shapes are examples of algebraic sets. Figure 8.1 is a modest example depicting the zero locus of the function $f(x,y,z) = z - x^3 + xy^2$. This shape is sometimes called the "monkey saddle," as it looks like a saddle with a three grooves (for two legs and one tail).

In general, you could think of (x_1, x_2) as a complex number $w = x_1 + ix_2$, and graph (in three dimensions) the function z = imaginary part of p(w) where p is any polynomial. (Figure 8.1 is the simple example where $p = iw^3$.) This graph is the zero locus of the polynomial function $z-$imaginary part of $p(w)$.

If you have access to a graphing device that can graph functions in $\mathbb{R}^3$ (for example, Grapher on any Apple computer), I would highly recommend exploring these shapes with whatever polynomial p you like.

And, for fun, Figure 8.2 is another algebraic set in $\mathbb{R}^3$.

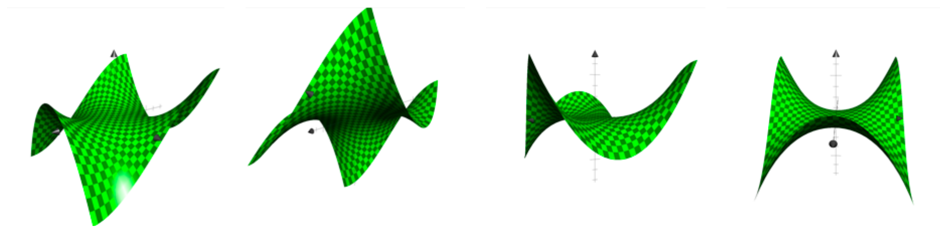

Figure 8.1: The monkey saddle.

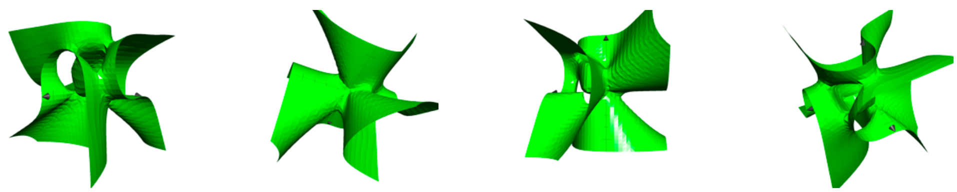

Figure 8.2: The zero locus of the polynomial $(z - x^2 - zy)(x - y^2 - zx)(y - z^2 - yx) - (z - x^3)(y - z^3)(x - y^3)$.

8.4 Union and multiplication (example of a proof using vanishing loci)

The impetus of this course is to see connections between geometry and algebra. So far, we have seen the following passage:

$$\text{Subsets of the ring } \mathbb{R}[x_1, \ldots, x_n] \to \text{(Algebraic) subsets of the space } \mathbb{R}^n.$$

where we take a subset I and produce the algebraic set $V(I)$. While this passage is interesting already, we'd like to say more about it. For example, we haven't actually done any algebra in the sense of this course: When did we exploit the fact that we can multiply/add in our ring of polynomials? (Never.)

Well, here's a fun exercise. When we have algebraic sets S and T that can be defined as the zero locus of just one polynomial, it turns out that that the above passage sends multiplication (of polynomials) to unions (of sets). Here is a more precise statement:

Proposition 8.4.1. Let $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ be polynomials in n variables. Suppose that $S = V(f)$ and $T = V(g)$. Then

$$S \cup T = V(fg).$$

(The lefthand side is the union of S and T. The righthand side is the vanishing locus of the function "f times g.")

Example 8.4.2. Let $f(x, y) = x$; this vanishes exactly when the x-coordinate is 0 (and the y-coordinate can be arbitrary). In other words, $V(x)$ is the y-axis in $\mathbb{R}^2$.

Let $g(x, y) = y$. By similar reasoning, $V(y)$ is the x-axis.

Now let $h(x, y) = f(x, y)g(x, y)$ be the product, so $h(x, y) = xy$. Then $V(h)$ is equal to the union of the x-axis and the y-axis.

We will now prove the proposition; this also serves as an example of what kinds of tools you need to use in a proof like this. Really, this is a matter of unwinding definitions—but it's also removing the cobwebs from your knowledge of unions, removing the cobwebs from your knowledge of how to show two sets are equal, and using the fact that $\mathbb{R}$ is an integral domain (Definition 7.3.23).

Proof of Proposition 8.4.1. Suppose that $x = (x_1, \ldots, x_n)$ is a point for which $f(x) = 0$. Then

$$(fg)(x) = f(x)g(x) = 0 \cdot g(x) = 0.$$

(Note that this is a string of equalities of real numbers.) Thus, the function fg vanishes on x, meaning $x \in V(fg)$. So far, we have proven that $V(f) \subset V(fg)$.

If $x \in V(g)$, we can similarly prove that $x \in V(fg)$ just as in the previous paragraph. Combining what we've proven so far, we see that $V(f) \cup V(g) \subset V(fg)$.

So we are left to prove that $V(fg) \subset V(f) \cup V(g)$. To see this, suppose that $x \in \mathbb{R}^n$ is a point on which $(fg)(x) = 0$. By definition of product of functions, this means

$$f(x)g(x) = 0.$$

(I again emphasize that this is an equality of real numbers.) Because $\mathbb{R}$ is an integral domain, this means that at least one of $f(x)$ and $g(x)$ equals 0. In other words, x is in at least one of $V(f)$ or $V(g)$. This shows that $x \in V(fg) \implies x \in V(f) \cup V(x)$. $\square$

8.5 Exercises

Exercise 8.5.1. Let $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ be polynomials in n variables. Suppose that $S = V(f)$ and $T = V(g)$. Prove that

$$S \cap T = V(\{f, g\}).$$

(The lefthand side is the intersection of S and T. The righthand side is the vanishing locus of the collection consisting of two functions, f and g.)

Exercise 8.5.2. Let $I \subset \mathbb{R}[x_1, x_2]$ be a collection of polynomial functions.

(a) Suppose $f, g \in I$. Then prove that

$$V(I) = V(I \cup \{f + g\}).$$

In other words, if you adjoin to I a sum of any two elements already in I, you do not change the vanishing locus.

(b) Suppose that $f \in I$ and that p is any polynomial. Then prove that

$$V(I) = V(I \cup \{fp\}).$$

If you think of the operation taking f to fp as "scaling by p," then this says you can adjoin to I anything obtained by scaling an element already in I, and you won't change the zero locus.

(c) Are the results above true not only for $\mathbb{R}[x_1, x_2]$, but also for $\mathbb{R}[x_1, \ldots, x_n]$ with $n \neq 2$?

Exercise 8.5.3. Let $S = V(f)$ where $f(x) = \sin(x)\cos(x)$. Is S an algebraic set? (Here, we treat f as a function from $\mathbb{R}$ to $\mathbb{R}$, and S is a subset of $\mathbb{R}$.)

Exercise 8.5.4. Let $S = V(f)$ where $f(x) = e^x - 3$. Is S an algebraic set?

Exercise 8.5.5. Let $f \in \mathbb{R}[x, y]$ be the polynomial

$$f(x, y) = y^2 - x(x - 1)(x - 2).$$

Draw $V(f)$.

Exercise 8.5.6. Let $f \in \mathbb{R}[x, y, z]$ be the polynomial $f(x, y, z) = xyz$. Draw, or describe very precisely, what $V(f)$ is.

Exercise 8.5.7. For $i = 1, 2, 3$, let $f_i \in \mathbb{R}[x_1, x_2, x_3]$ be the polynomial

$$f_i(x_1, x_2, x_3) = x_i.$$

Let $I = \{f_1, f_2, f_3\}$. Tell me what $V(I)$ is.

Exercise 8.5.8. Let $f \in \mathbb{R}[x, y]$ be the polynomial

$$f(x, y) = x^2 + y^2 + 1.$$

What is $V(f)$?

Exercise 8.5.9. Let $X \subset \mathbb{R}^n$ be a finite subset. Prove that X is algebraic.

8.6 Extra credit

Let $S = V(f)$ where f is the function

$$f(x, y) = \cos(x)^2 + \sin(y)^2 - 1.$$

Prove or disprove: S is an algebraic set.