Lecture notes for PM 464/764 – Week One

David McKinnon
Department of Pure Mathematics
University of Waterloo

Spring 2021

1 What's the point of algebraic geometry?

L'algèbre n'est qu'une géométrie écrite, la géométrie n'est qu'une algèbre figurée. – Sophie Germain

("Algebra is nothing but written geometry; geometry is nothing but algebra in pictures.")

The Soph – as they no doubt called her in the 'hood – was right on with that remark, and it describes the central theme of this course. With your indulgence, I'll elaborate.

The great thing about geometry is that it's full of pictures. There's a physicality to it that makes it easier to guess what's going on – to guide one's intuition, if you will.

Trouble is, it's often fiendishly difficult to actually *prove* that intuition. The pictures that so eloquently inspire you to understand the truth also conspire to conceal nuances and special cases. It is, frankly, a pain in the neck.

Algebra, unlike geometry, is quite amenable to computation. I mean, that's kind of the whole point of it. But ... algebra and intuition are not good friends. Look at an algebraic statement, and it's often really hard to understand what it's all about.

Enter the genius of Professor Germain. If you can somehow marry the two subjects of algebra and geometry, then you can get the best of both worlds: the intuition of the geometry, and the calculational power of the algebra. Not that she was the only (or even the first) person to figure this out, but her realization certainly predated the modern idea of algebraic geometry, and helped usher it in.

(Incidentally, you should check out Sophie Germain's life story. She kicked bum.)

So how do we arrange the wedding? Do these two really love each other?

Sure they do. That's why there's a whole course about them, so we can 'ship them.

The key is functions. Functions are things that we can be all algebra-like about. If you have a Geometry Thing, then the corresponding Algebra Thing is the set of functions from the Geometry Thing to some nice algebra place, like the complex numbers.

But more on that later. The first step is to describe the kind of Things we're going to play with in this course.

2 Algebraic sets

In this course, we will be working over the complex numbers. And we'll be doing algebra. And we're lazy.

So what's the easiest, smallest collection of things that you can do algebra with, given that you've already got the complex numbers? Well, you'll need coordinates, because we're doing geometry. And you'll need to add, subtract, and multiply, because come on. And that means ... polynomials. All the algebra we'll do in this course will be with polynomials (and closely related beasts).

And the Geometry Things we'll talk about are also defined by polynomials.

Definition 2.1. *Let n be a positive integer.* **Affine space** $\mathbb{A}^n$ *is the set* $\mathbb{C}^n$*.*

(You might ask why we bother with $\mathbb{A}^n$ specially, when we've already got the perfectly serviceable $\mathbb{C}^n$. Well ... for this course, I don't have a good answer for you. But when you're older, you may want to do algebraic geometry over other places than the complex numbers, in which case the extra notation can come in handy.)

Definition 2.2. *Let S be a subset of the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$. The* **algebraic set** *corresponding to S is the set:*

$$V(S) = \{x \in \mathbb{A}^n \mid f(x) = 0 \text{ for all } f \in S\}$$

In other words, $V(S)$ is the set of points where all *the functions in S vanish.*

There are lots of algebraic sets out there. The xy-plane, for example. (Defined as the algebraic subset of $\mathbb{A}^2$ corresponding to the empty set S. Isn't math great?)

The x-axis is the set defined by $y = 0$, so it's $V(S)$ for $S = \{y\}$.

The unit sphere in $\mathbb{C}^3$ is defined by $x^2+y^2+z^2-1$. Of course, this isn't a sphere, really, but we call it that anyway, because of nostalgia for the good old real numbers.

The **twisted cubic** is an algebraic subset of $\mathbb{A}^3$ defined by the set $\{y - x^2, z - x^3\}$. (It's a curve! Defined by two equations in a 3-dimensional space. This, um, doesn't always work out so nicely: the dimension isn't always reduced by one for every additional defining polynomial. Think about it for a sec, and you'll realize that this is true ... and then I'll tell you that it's worse than you think. More on that later.)

The origin in $\mathbb{A}^2$ is an algebraic set, defined by the set $\{x, y\}$.

And on it goes. I mean, there are lots of those suckers.

This all means that we can make a Geometric Thing (an algebraic set) out of an Algebra Thing (a bunch of polynomials). Next step is to go the other way.

Definition 2.3. *Let $X \subset \mathbb{A}^n$ be a subset of affine space. The* **ideal of** X *is the set*

$$I(X) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(P) = 0 \text{ for all } P \in X\}$$

In other words, $I(X)$ is the set of polynomials that vanish on all of X.

Plenty of examples here too, of course. The ideal of the xy-

plane, for example, is the set of polynomials in x and y that vanish on all the points of the xy-plane. That's, um ... $\{0\}$.

The ideal of the x-axis is the set of all polynomials in x and y that vanish when $y = 0$. That is to say, it's the set of all the polynomials that you can factor a y out of:

$$I(x\text{-axis}) = \{yp(x, y) \mid p(x, y) \in \mathbb{C}[x, y]\} = (y)$$

The ideal of the "unit sphere" and the twisted cubic are, respectively, the ideals generated by $\{x^2 + y^2 + z^2 - 1\}$ and $\{y - x^2, z - x^3\}$. This is not obvious (although part of it is), and we'll have to wait to prove it.

The ideal of the origin in $\mathbb{A}^2$ is the set of polynomials with no constant term:

$$\{xp(x, y) + yq(x, y) \mid p(x, y), q(x, y) \in \mathbb{C}[x, y]\} = (x, y)$$

But hang on a minute. We're calling these sets of polynomials "ideals". Are they actually *ideals*?

Of course they are, silly.

Theorem 2.4. *Let X be a subset of $\mathbb{A}^n$, and $I(X)$ the ideal of X. Then $I(X)$ is an ideal of the ring $\mathbb{C}[x_1, \ldots, x_n]$.*

Moreover, $I(X)$ is a **radical ideal***: if $f^n \in I(X)$ for some positive integer n, then $f \in I(X)$.*

Proof: To check if a set is an ideal, we need to check that it's an additive subgroup, and that it's closed under multiplication by arbitrary elements of the ring.

So. Say $f, g \in I(X)$. Then $f(x) = g(x) = 0$ for all $x \in X$. But then $(f \pm g)(x) = 0$ for all $x \in X$, so $f \pm g \in I(X)$ too.

And clearly $0 \in I(X)$, so $I(X)$ is indeed an additive subgroup of $\mathbb{C}[x_1, \ldots, x_n]$.

And if $h \in \mathbb{C}[x_1, \ldots, x_n]$ is any element, and $f \in I(X)$, then $(hf)(x) = h(x)f(x) = h(x) \cdot 0 = 0$, so $I(X)$ is an ideal, as desired.

As for the "moreover": if $f^n \in I(X)$, then $(f(x))^n = 0$ for all $x \in I(X)$, so $f(x) = 0$ for all $x \in I(X)$, so $f \in I(X)$. ♣

The "moreover" is a slightly sneaky thing. It means that not every ideal is the ideal of an algebraic set. Which is only fair, really, because not every subset of $\mathbb{A}^n$ is the algebraic set of an ideal. (That is, not every subset of $\mathbb{A}^n$ is defined by polynomials.)

This revelation, that every algebraic set is the algebraic set corresponding to an ideal, allows us to make the observation that every algebraic set is defined by a *finite* set of polynomials. This is because of the Hilbert Basis Theorem, which says that every ideal of $\mathbb{C}[x_1, \ldots, x_n]$ is finitely generated. (If you don't know that theorem, check it out online. It's rockin'.) So if $I(X) = (f_1, \ldots, f_r)$, then $X = V(f_1, \ldots, f_r)$.

Definition 2.5. *An ideal I of a ring R is called* **radical** *if every $r \in R$ with $r^n \in I$ for some positive integer n satisfies $r \in I$. In other words, I is closed under "radicals".*

For an arbitrary ideal I of a ring R, define the **radical of I** *to be*

$$rad(I) = \{r \in R \mid r^n \in I \text{ for some integer } n > 0\}$$

Theorem 2.6. *Let I be an ideal of a ring R. Then $rad(I)$ is a radical ideal of R containing I.*

Proof: The "containing I" part is pretty obvious (take $n = 1$ in the definition), so we'll just show that $\text{rad}(I)$ is a radical ideal.

Well, $\text{rad}(I)$ contains 0. That's pretty clear.

If $j \in \text{rad}(I)$ and $r \in R$, then $j^n \in I$, so $(rj)^n = r^n j^n \in I$, so $rj \in \text{rad}(I)$.

And if $j^n \in \text{rad}(I)$, then $(j^n)^m \in I$, so $j^{nm} \in I$ and so $j \in \text{rad}(I)$. So $\text{rad}(I)$ is radical.

All that's left is closure under addition and subtraction. So let's say j_1 and j_2 are elements of $\text{rad}(I)$. We want to show that $j_1 \pm j_2 \in \text{rad}(I)$.

Well, $j_1^{n_1} \in I$ and $j_2^{n_2} \in I$. Consider $(j_1 \pm j_2)^{n_1+n_2}$. When you expand that out, every term in the expanded product will either have a factor of $j_1^{n_1}$ (which puts that term in I), or a factor of $j_2^{n_2}$ (which puts that term in I). So all the terms lie in I, meaning that $(j_1 \pm j_2)^{n_1+n_2} \in I$, and so $j_1 \pm j_2 \in \text{rad}(I)$. ♣

Now for the big correspondence. Given a set S of polynomials, we can make an algebraic set X. And given a subset $X \subset \mathbb{A}^n$, we can make an ideal $I(X)$. And the two relations are actually inverse to one another ... provided that you only allow algebraic sets, and radical ideals.

Theorem 2.7 (Hilbert's Nullstellensatz)**.** *Let n be a positive integer. There is a bijection*

$$\{\textit{algebraic subsets of } \mathbb{A}^n\} \longleftrightarrow \{\textit{radical ideals of } \mathbb{C}[x_1, \ldots, x_n]\}$$

The bijection is given by $X \mapsto I(X)$ and $I \mapsto V(I)$.

Note that for any subset $X \subset \mathbb{A}^n$, we know that $I(X)$ is a radical ideal, so that makes our restriction to radical ideals

reasonable. And $V(I)$ is always an algebraic set by definition, so that explains the left side of the correspondence. It's also not too hard to check that $V(I(X)) = X$ for every algebraic set X.

The hard part is, unsurprisingly, proving that $I(V(I)) = I$ if I is a radical ideal. We won't do that here, because it takes us a bit too far afield, but you can find proofs aplenty online.

But this correspondence is more awesome than it appears! For example, it's pretty easy to see that if you enlarge your algebraic set, then you shrink the ideal, and *vice versa*:

$$X \subset Y \text{ if and only if } I(Y) \subset I(X)$$

In other words, bigger ideals correspond to smaller algebraic sets.

Also, unions of algebraic sets correspond to intersection of ideals:

$$I(X \cup Y) = I(X) \cap I(Y)$$

To see this, notice that if f vanishes on X and Y, then it's simultaneously in $I(X)$ and $I(Y)$, so it's in their intersection. And conversely, if $f \in I(X) \cap I(Y)$, then f vanishes on X and on Y, so it vanishes on their union.

[Notice that this also means that finite unions of algebraic sets are algebraic sets.]

We also know about special kinds of ideals. What kind of algebraic sets do they correspond to?

For example. Let's say $I(X)$ is a maximal ideal. What kind of algebraic set does it correspond to? [Hint: it corresponds to a single point. But don't tell anyone, because it's still a secret.]

Well, it can't correspond to the empty set $X = \emptyset$, because the ideal corresponding to the empty set is $\mathbb{C}[x_1, \ldots, x_n]$, which is, oddly, too big to be maximal.

So X has to have at least one point in it. Pick one, and call it P.

Every element of $I(X)$ vanishes at P, by definition. Let Q be any other point of $\mathbb{A}^n$. Then we can find a polynomial f that vanishes at P, but not at Q.

Now, the ideal generated by $I(X)$ and f is not all of $\mathbb{C}[x_1, \ldots, x_n]$. because everything in $I(X)$ vanishes at P, and so does f ... and not every polynomial vanishes at P. (Hello, nonzero constant functions!)

But the ideal generated by $I(X)$ and f is an ideal, and it contains the maximal ideal $I(X)$. And it's not the whole ring. So it must be $I(X)$. So f is actually in $I(X)$. Which means – think about this – that Q is not in X.

That's right! The only point of X is the single point P.

So every maximal ideal corresponds to a single point. Conversely, if P is a point, we want to show that $I(P)$ is a maximal ideal.

Best way to show an ideal is maximal? Mod out, and show that the quotient is a field.

Best way to show that R/I is a field? Find an onto homomorphism from R to a field, such that the kernel is I.

Here's my homomorphism, for the ideal $I(P)$: define

$$\phi\colon \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C} \text{ by } \phi(f) = f(P)$$

It's clearly a homomorphism – we're just plugging in numbers to a polynomial – and it's clearly onto. (Hello again, constant functions!) And the kernel is exactly the functions that vanish at P. Which is $I(P)$.

So $I(X)$ is a maximal ideal if and only if X is a single point. Cool!

What about prime ideals?

It turns out to be slightly easier to figure out what *non*-prime ideals correspond to. So let's say that $I(X)$ is *not* prime (but is still radical). What does X look like then? [Hint: X is going to be in pieces.]

Before we go any further, I'd like to remind you that the unit ideal – that's the ideal (1), which is the entire ring – is not a prime ideal. This is basically for the same reason that 1 is not a prime number. But (1) is irritatingly similar to a prime ideal – if $ab \in (1)$ then either $a \in (1)$ or $b \in (1)$, for example – so it's convenient to rule it out right now.

In summary: in what follows, we will assume that $I(X)$ is a *proper* ideal of $\mathbb{C}[x_1, \ldots, x_n]$. Which, by the Nullstellensatz, is equivalent to assuming that X is nonempty.

Well, if $I(X)$ is not prime, then there are polynomials f_1 and f_2, with $f_1, f_2 \notin I(X)$, but $f_1 f_2 \in I(X)$. So $f_1 f_2$ vanishes at all points of X, but f_1 and f_2 don't – they only vanish on part of X.

Let J_1 be the ideal generated by $I(X)$ and f_1, and let J_2 be the ideal generated by $I(X)$ and f_2. Both J_i are ideals that are strictly bigger than $I(X)$, so their radicals $\mathrm{rad}(J_1)$ and $\mathrm{rad}(J_2)$

are also strictly bigger than $I(X)$. By the Nullstellensatz, this means that each $\mathrm{rad}(J_i)$ corresponds to a proper algebraic subset $Y_i = V(\mathrm{rad}(J_i)) \subset X$.

We'll show that $Y_1 \cup Y_2 = X$ – namely, that X can be split into two algebraic pieces.

Now,

$$Y_1 \cup Y_2 = V(\mathrm{rad}(J_1)) \cup V(\mathrm{rad}(J_2)) = V(\mathrm{rad}(J_1) \cap \mathrm{rad}(J_2))$$

And $\mathrm{rad}(J_1) \cap \mathrm{rad}(J_2)$ contains $I(X)$ (because both of the intersecting ideals contain $I(X)$), so $Y_1 \cup Y_2$ is contained in X.

To show the reverse inclusion, let's say that $P \in X$. Then $f_1(P)f_2(P) = 0$, because $f_1 f_2 \in I(X)$. But then either $f_1(P) = 0$ or $f_2(P) = 0$, so either $P \in Y_1$ or $P \in Y_2$. So $P \in Y_1 \cup Y_2$, and we conclude that $X \subset Y_1 \cup Y_2$.

Thus, if $I(X)$ is not prime, then X can be written as the union of two proper algebraic subsets.

Conversely, if $X = Y_1 \cup Y_2$ is the union of two proper algebraic subsets, then there are polynomials f_1 and f_2 that vanish on Y_1 and Y_2, respectively, but not on all of X. Then $f_1 f_2 \in I(X)$, but f_1 and f_2 are not in $I(X)$, so $I(X)$ is not prime.

In other words, $I(X)$ is not prime if and only if X is the union of two proper algebraic subsets.

That's too many words.

Definition 2.8. *Let X be a nonempty algebraic set. We say that X is* **reducible** *if and only if it is the union $X = Y_1 \cup Y_2$ of two proper algebraic subsets.*

We say that X is **irreducible** *if and only if it is not reducible.*

If X is empty, then it is neither irreducible nor reducible.

So $I(X)$ is a prime ideal if and only if X is an irreducible algebraic set.