Lecture notes for PM 464/764 – Week Two

David McKinnon
Department of Pure Mathematics
University of Waterloo

Spring 2021

1 But what are the morphisms?

These days, every time mathematicians start a new subject, they define the objects they're interested in. Moments after that, they define the relationships between them. They call those relationships "morphisms".

For instance. You define groups, and then you define group homomorphisms, which are functions from group to group that preserve all the group-y stuff about them.

You define topological spaces, and then you define continuous functions, which are functions that preserve the topology.

Now, the objects we're interested in are algebraic sets. The relationships between them are going to be functions between algebraic sets that preserve their algebraicky-ness.

(It actually turns out that the last sentence is the kind of old-fashioned, repressive nonsense that The Man uses to keep the good people down. Later on, we'll let freedom reign, with a more broad-minded view of relationships.)

Definition 1.1. *Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be algebraic sets. A* **polynomial map** *from X to Y is a function $\phi\colon X \to Y$ such that the coordinates of $\phi = (\phi_1, \ldots, \phi_m)$ are all polynomials in the coordinates of $\mathbb{A}^n$.*

For example, the function $\phi\colon \mathbb{A}^1 \to \mathbb{A}^3$ given by $\phi(t) = (t, t^2, t^3)$ is a polynomial map.

Let H be the hyperbola $x^2 - y^2 = 1$ in $\mathbb{A}^2$, and let C be the circle $x^2 + y^2 = 1$, also in $\mathbb{A}^2$. The function $\phi\colon H \to C$ given by $\phi(x, y) = (x, iy)$ is a polynomial map from H to C.

The function $\phi\colon \mathbb{A}^2 \to \mathbb{A}^1$ given by $\phi(x, y) = y$ is a polynomial map.

We next define an isomorphism in exactly the way you expect.

Definition 1.2. *Let X and Y be algebraic sets. A polynomial map $f\colon X \to Y$ is an isomorphism if and only if there is a polynomial map $g\colon Y \to X$ such that $f \circ g = id$ and $g \circ f = id$.*

An isomorphism therefore has to be one-to-one and onto. But it is **NOT** true that a polynomial map that's one-to-one and onto is an isomorphism. There's an example in the homework showing that. Check it out.

So. Just to repeat: an isomorphism is a polynomial map with a polynomial map inverse.

Of the three examples of polynomial maps given above, only the second one – the function $\phi(x, y) = (x, iy)$ – is an isomorphism. The first example isn't onto, and the third example isn't one-to-one. And the second one has the polynomial inverse $\psi(x, y) = (x, -iy)$.

But if one-to-one and onto isn't enough to verify that something's an isomorphism, how can we tell if it is or not?

Well, honestly, usually the best way to tell is to write down a polynomial inverse. But there are other ways. They involve understanding the algebra partner of an algebraic set a little more deeply.

In Week 1, we defined the algebraic partner of an algebraic set to be its ideal. But ... that's not the greatest thing ever.

For example, let X be the x-axis in $\mathbb{A}^2$, and let Y be the y-axis. They are clearly isomorphic as algebraic sets: $\phi(x, y) = (y, x)$ exchanges the two sets. But their ideals are different: (y) and (x), respectively.

You might say that their ideals are "isomorphic", and though I'd have some pointed questions for you about what you think "isomorphic" means for ideals, you wouldn't be totally off base.

So I'd haul out another example: the x-axis X in $\mathbb{A}^2$, and the x-axis Z in $\mathbb{A}^3$. Again, clearly isomorphic as algebraic sets – $\phi(x, y, z) = (x, y)$ is an isomorphism – but the corresponding ideals are (y) and (y, z), which aren't even nearly isomorphic. Heck, they're not even ideals of the same ring.

Ideally, we'd find an algebraic partner for an algebraic set X that is invariant under isomorphism. That is: isomorphic algebraic sets have isomorphic partners. We come up with this.

Definition 1.3. *Let $X \subset \mathbb{A}^n$ be an algebraic set, with ideal*

$I(X)$. The **coordinate ring** *of X is the ring*

$$\Gamma(X) = \mathbb{C}[x_1, \ldots, x_n]/I(X)$$

which is the ring of polynomial maps from X to $\mathbb{A}^1$.

Ok, first off: why is $\Gamma(X)$ the ring of polynomial maps from X to $\mathbb{A}^1$?

Well, a polynomial map from $\Gamma(X)$ to $\mathbb{A}^1$ is indeed a single polynomial in n variables. (Remember, $\mathbb{A}^1$ is just $\mathbb{C}$ with a fancy name.) But ... some of those take the same values on X, so they're not really different maps.

Now, f and g agree on X if and only if $f - g$ is identically zero on X. But we already built a house for all the polynomials that are identically zero on X, and we called it $I(X)$. So f and g agree on X if and only if they are congruent modulo $I(X)$.

In other words, the ring of polynomial maps from X to $\mathbb{A}^1$ is exactly $\Gamma(X) = \mathbb{C}[x_1, \ldots, x_n]/I(X)$. Just like I said.

Also, that Nullstellensatz correspondence between ideals and algebraic sets? Still works for the coordinate ring.

Theorem 1.4. *Let $X \subset \mathbb{A}^n$ be an algebraic set, with coordinate ring $\Gamma(X)$. Then there is a one-to-one correspondence between algebraic subsets of X and radical ideals of $\Gamma(X)$, given by*

$$Y \mapsto I(Y) \pmod{I(X)}$$

and

$$I \mapsto V(\overline{I})$$

where $\overline{I}$ denotes the ideal of $\mathbb{C}[x_1, \ldots, x_n]$ generated by the elements of $\mathbb{C}[x_1, \ldots, x_n]$ that lie in I modulo $I(X)$.

Moreover, under this correspondence, points correspond to maximal ideals, and irreducible subsets of X correspond to prime ideals.

Proof: The heavy lifting here is all done already. The correspondence described here is exactly the Nullstellensatz correspondence, reduced mod $I(X)$. Ideals of $\Gamma(X) = \mathbb{C}[x_1, \ldots, x_n]/I(X)$ are exactly the ideals of $\mathbb{C}[x_1, \ldots, x_n]$ that contain $I(X)$, so the correspondence is well defined: all the ideals in the statement of the theorem contain $I(X)$, and so their corresponding algebraic sets are contained in X.

For the "moreover", let $q\colon \mathbb{C}[x_1, \ldots, x_n] \to \Gamma(X)$ be the quotient homomorphism. If I is a prime (resp. maximal) ideal of $\Gamma(X)$, then $q^{-1}(I)$ is a prime (resp. maximal) ideal of $\mathbb{C}[x_1, \ldots, x_n]$, so $V(q^{-1}(I))$ is an irreducible (resp. single-point) subset of $\mathbb{A}^n$, so it's an irreducible (resp. single-point) subset of X. And if I is not a prime (resp. maximal) ideal of $\Gamma(X)$, then by the same reasoning $V(q^{-1}(I))$ is a reducible (resp. multi-point) subset of X. ♣

Awesome. Next step: prove that isomorphic algebraic sets have isomorphic coordinate rings, and *vice versa*.

To do this, let's say that $\phi\colon X \to Y$ is a polynomial map of algebraic sets X and Y. Can we somehow turn this into a homomorphism of coordinate rings $\Gamma(X) \to \Gamma(Y)$?

Alas, no. But it *is* possible to turn it into a homomorphism of coordinate rings going *backwards*, from $\Gamma(Y) \to \Gamma(X)$.

To do this, let's say someone hands us a polynomial map $f\colon Y \to \mathbb{A}^1$. We somehow need to come up with a polynomial map from X to $\mathbb{A}^1$.

But this is easy: to get from X to $\mathbb{A}^1$, just do ϕ first, to get from X to Y, and then do f, to get from Y to $\mathbb{A}^1$. Ta-da!

[Notice that the composition of polynomial maps is again a polynomial map. Y'know, because when you plug a bunch of polynomials into another polynomial, the end result is a polynomial.]

Definition 1.5. *Let X and Y be rings that contain $\mathbb{C}$. (Such rings are called* **$\mathbb{C}$-algebras***.) A* **$\mathbb{C}$-algebra homomorphism** *from X to Y is a ring homomorphism $\phi\colon X \to Y$ that satisfies*

$$\phi(z) = z$$

for all complex numbers z.

Definition 1.6. *Let $\phi\colon X \to Y$ be a polynomial map of algebraic sets. The* **pullback** *of ϕ is the $\mathbb{C}$-algebra homomorphism*

$$\phi^*\colon \Gamma(Y) \to \Gamma(X)$$

given by $\phi^*(f) = f \circ \phi$.

We can go the other way too.

Theorem 1.7. *Let X and Y be algebraic sets with coordinate rings $\Gamma(X)$ and $\Gamma(Y)$, respectively. For any $\mathbb{C}$-algebra homomorphism $\psi\colon \Gamma(Y) \to \Gamma(X)$, there is a polynomial map $\phi\colon X \to Y$ such that $\psi = \phi^*$.*

Proof: Say $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$. If we want to build a polynomial map $\phi\colon X \to Y$, then we need to find m polynomials $\phi_1, \ldots, \phi_m$ in n variables, so that $\phi = (\phi_1, \ldots, \phi_m)$.

Now, ϕ_i is just the ith coordinate of ϕ, in this hypothetical scenario. But we have a function on $\mathbb{A}^m$ that picks out the ith coordinate – it's called x_i! So let's define ϕ_i so that it corresponds to x_i via ψ.

It's tempting to define $\phi_i = \psi(x_i)$. But that doesn't quite make sense, because $\psi(x_i)$ isn't a polynomial – it's an element of $\mathbb{C}[x_1, \ldots, x_n]/I(X)$, which is an equivalence class of polynomials.

So pick one.

That is, for each i, choose a polynomial $\phi_i \in \mathbb{C}[x_1, \ldots, x_n]$ such that $\psi(x_i) \equiv \phi_i \pmod{I(X)}$. And now define $\phi\colon X \to Y$ by

$$\phi(P) = (\phi_1(P), \ldots, \phi_m(P))$$

This ϕ is certainly a polynomial map – just look at all those polynomials there. And if $f \in I(Y)$, then $\psi(f) = 0$, and we get

$$\phi^*(f(x_1, \ldots, x_m)) = f(\phi_1, \ldots, \phi_m)$$

and, modulo $I(X)$, we get:

$$0 = \psi(f(x_1, \ldots, x_m)) = f(\psi(x_1), \ldots, \psi(x_m)) = f(\phi_1, \ldots, \phi_m)$$

so we conclude that $\phi^*(I(Y)) \subset I(X)$. This means that ϕ^* is well defined from $\Gamma(Y)$ to $\Gamma(X)$, and therefore that ϕ is well defined from X to Y. (If $P \in X$, then $f(P) = 0$ for all $f \in I(X)$, so for all $g \in I(Y)$, $g(\phi(P)) = [\phi^*(g)](P) = 0$.)

Finally, it's pretty easy to see that $\phi^* = \psi$, because for any polynomial $p(x_1, \ldots, x_m)$, we have, modulo $I(X)$:

$$\phi^*(p) = p \circ \phi = p(\phi_1, \ldots, \phi_m)$$

and

$$\psi(p) = \psi(p(x_1, \ldots, x_n)) = p(\psi(x_1), \ldots, \psi(x_n)) = p(\phi_1, \ldots, \phi_m)$$

♣

Now we can present the coup de grace. (That's French for "the awesome theorem".)

Theorem 1.8. *Let X and Y be algebraic sets, with coordinate rings $\Gamma(X)$ and $\Gamma(Y)$, respectively. Then X is isomorphic to Y if and only if $\Gamma(X)$ is isomorphic to $\Gamma(Y)$ as a $\mathbb{C}$-algebra.*

Moreover, if $\phi\colon X \to Y$ is an isomorphism, then for any algebraic subset $V \subset Y$, then

$$I(\phi^{-1}(V)) = \phi^* I(V)$$

(Note that $\phi^* I(V)$ is an ideal of $\Gamma(X)$ because ϕ^* is an isomorphism.)

Proof: If X is isomorphic to Y, then there are mutually inverse polynomial maps $\phi\colon X \to Y$ and $\Phi\colon Y \to X$. Their pullbacks ϕ^* and Φ^* are therefore also mutually inverse (since the pullback of the identity polynomial map is the identity homomorphism and $(f \circ g)^* = g^* \circ f^*$), so $\Gamma(X)$ and $\Gamma(Y)$ are isomorphic as $\mathbb{C}$-algebras, as desired.

Conversely, if $\Gamma(X)$ and $\Gamma(Y)$ are isomorphic, then there are mutually inverse $\mathbb{C}$-algebra homomorphisms ψ and Ψ between them. These must correspond to polynomial maps ϕ and Φ, which must be mutually inverse because $\psi = \phi^*$ and $\Psi = \Phi^*$ are mutually inverse.

Moreover, if ϕ is an isomorphism and $V \subset Y$ is any algebraic subset, then for any $f \in I(\phi^{-1}(V))$, let

$$g = f \circ \phi^{-1} = (\phi^{-1})^* f \ \leftrightarrow f = \phi^* g$$

Then

$$g(V) = (f(\phi^{-1}(V))) = 0$$

so $g \in I(V)$ and $f \in \phi^* I(V)$.

Conversely, if $f \in \phi^*(I(V))$, then write

$$f = \phi^* g = g \circ \phi \;\leftrightarrow\; g = f \circ \phi^{-1}$$

for $g \in I(V)$, giving

$$f(\phi^{-1}(V)) = g(V) = 0$$

and therefore $f \in I(\phi^{-1}(V))$. Thus, $I(\phi(V)) = \phi^* I(V)$, as desired. ♣