LECTURE APRIL 27: A CRASH COURSE IN ALGEBRAIC GEOMETRY

1. Pythagorean triplets

How do you solve the Diophantine equation:

$$a^2 + b^2 = c^2?$$

For instance, $(3,4,5)$. Divide both sides by c^2, and let $x = a/c$, $y = b/c$ to get

$$x^2 + y^2 = 1.$$

The first observation is, that it is enough to find all solutions (x, y) of this last equation, where $x, y \in \mathbf{Q}$. So we are trying to find the set of points on the unit circle centered at $(0,0)$ with *rational coordinates*.

Stereographic projection gives a way from going from points on the line to points on the circle, and vice versa. So if I have a point $P' = (t, 0)$ on the x-axis, I should find the line joining P' to $N = (0,1)$, and find the point $P = (x, y)$ on the intersection of the circle and the line.

The line joining P' to N is $y - 1 = -x/t$, or $x = -ty + t$. We want to intersect this with $x^2 + y^2 = 1$. Substituting the first equation into the second gives

$$(1 + t^2)y^2 - 2ty + (t^2 - 1) = 0.$$

We already know that $y = 1$ is a solution. The sum of the two roots has to be $2t/(1 + t^2)$, and so the other root is

$$y = -(1 - t)^2/(1 + t^2).$$

So we get that the point P is

$$(x, y) = \left(\frac{2t}{1 + t^2}, -\frac{(1 - t)^2}{1 + t^2}\right)$$

This process puts into bijection the points on the circle, and the points of *real projective line* $\mathbf{R} \cup \{\infty\}$. In fact it also gives a bijection between rational points of the circle, and the points of the *rational projective line* $\mathbf{Q} \cup \{\infty\}$. ‘ How far can this procedure go? Like, how could we solve

$$x^3 + y^3 = 1$$

in rational numbers (x, y)? Is there again a *rational parametrization* of this curve? In other words, are there rational functions $p(t), q(t) \in \mathbf{Q}(t)$ such that $p(t)^3 + q(t)^3 = 1$, without p and q being constants?

2. Affine algebraic sets

Algebraic geometry is the study of solution sets to polynomial equations.

Let K be an algebraically closed field (for instance, it is common to assume that $K = \mathbf{C}$).

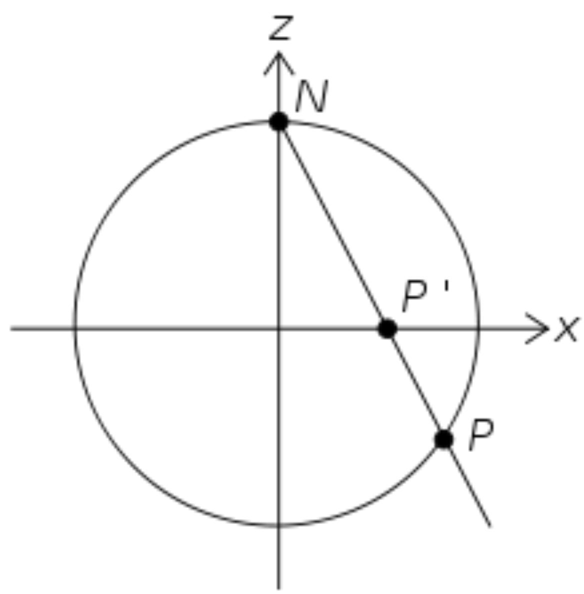
Definition 2.1. *Affine space of dimension n is*

$$\mathbf{A}^n = \left\{ (a_1, \ldots, a_n) \;\middle|\; a_i \in K \right\}$$

Definition 2.2. *Let $S \subset K[x_1, \ldots, x_n]$ be a set of polynomials. I define*

$$Z(S) = \left\{ (a_1, \ldots, a_n) \in \mathbf{A}^n \;\middle|\; f(a_1, \ldots, a_n) = 0, \ \text{all } f \in S \right\}$$

Such a subset of $\mathbf{A}^n$ is called an affine algebraic set.


z
N
P '
x
P

For instance, in $\mathbf{A}^2$, we have $Z(\{x^2+y^2-1\})$ is the circle. Well, sort of: it's the set of complex solutions to $x^2+y^2=1$.

Example 2.3. *$Z(\varnothing)=\mathbf{A}^n$, and $Z(\{0\})=\mathbf{A}^n$. Also, $Z(\{1\})=\varnothing$. Finally,*

$$Z(\{x(x-3)\})=\{0,3\}\,.$$

Example 2.4. *When $n=1$, what are the affine algebraic subsets of $\mathbf{A}^1=\mathbf{C}$? A polynomial in one variable can only have finitely many roots, unless that polynomial is the zero polynomial, in which case it has all of $\mathbf{C}$ as its roots.*

Thus a subset $S\subset\mathbf{A}^1$ is algebraic if and only if it is either finite or everything.

Example 2.5. *What are the algebraic subsets of $\mathbf{C}^2$? Is $\{(3,4)\}$ algebraic? Yes, because*

$$Z(\{x-3,y-4\})=\{(3,4)\}\,.$$

Also

$$Z(\{x,y\})=\{(0,0)\}\,.$$

What about $\{(3,4),(0,0)\}$? This too is algebraic, because

$$Z(\{x(x-3),x(y-4),y(x-3),y(y-4)\})=\{(0,0),(3,4)\}\,.$$

In fact, any finite subset of $\mathbf{A}^n$ is algebraic. There are infinite algebraic subsets of $\mathbf{A}^2$, given by $Z(f)$, where f a nonconstant polynomial.

Observe that if $S\subset K[x_1,\ldots,x_n]$, then

$$Z(S)=Z(I),$$

where I is the ideal generated by S. If $f(x)=0$ and $g(x)=0$, and if $h=af+bg$, then $h(x)=0$. So it's sufficient to only consider $Z(I)$, where I is an ideal.

Remember that if I is an ideal in a ring, then the radical of I is

$$\sqrt{I}=\left\{f\in K[x_1,\ldots,x_n]\;\middle|\; f^n\in I \text{ for some } n\right\}$$

Then $\sqrt{I}$ is also an ideal, and in fact

$$Z(I)=Z(\sqrt{I}).$$

A *radical ideal* is an ideal I for which $\sqrt{I}=I$. Note that $\sqrt{\sqrt{I}}=\sqrt{I}$. So we might as well just consider $Z(I)$ where I is a radical ideal.

So what we have is a function Z from radical ideals of $K[x_1,\ldots,x_n]$ to affine algebraic subsets of $\mathbf{A}^n$. There is a function going the other way:

Definition 2.6. *Let $V\subset\mathbf{A}^n$ be any subset of affine space. Then*

$$I(V)=\left\{f\in K[x_1,\ldots,x_n]\;\middle|\; f(a_1,\ldots,a_n)=0 \text{ for all } (a_1,\ldots,a_n)\in V\right\}$$

is a radical ideal (check this!).

Theorem 2.7 (Hilbert's Nullstellensatz)**.** *The functions $I\mapsto Z(I)$ and $S\mapsto I(S)$ are bijections between the set of radical ideals of $K[x_1,\ldots,x_n]$ and the set of algebraic subsets of $\mathbf{A}^n$. It is inclusion-reversing.*

The last sentence says that if $I\subset J$, then $Z(J)\subset Z(I)$.

As a corollary, we find that the only maximal ideals of $K[x_1,\ldots,x_n]$ are of the form

$$(x_1-a_1,\ldots,x_n-a_n)$$

for some $(a_1,\ldots,a_n)\in\mathbf{A}^n$.

3. Properties of $Z(I)$

Given an ideal $I \subset K[x_1, \ldots, x_n]$, we have an affine algebraic set $Z(I)$.

(1) $Z(0) = \mathbf{A}^n$.
(2) $Z(1) = \varnothing$
(3) If $I \subset J$, then $Z(J) \subset Z(I)$.
(4) $Z(I + J) = Z(I) \cap Z(J)$.
(5) $Z(IJ) = Z(I) \cup Z(J)$.

Let's discuss the last two properties. If I, J are ideals, and $x \in Z(I + J)$, it means that $(f + g)(x) = 0$ for all $f \in I$ and $g \in J$. In particular this is true if $g = 0$, so that $f(x) = 0$ for all $f \in I$, and so $x \in Z(I)$. Similarly, $x \in Z(J)$, so $x \in Z(I) \cap Z(J)$. I'll leave the converse to you.

Similarly, if x belongs to $Z(IJ)$, it means that $(fg)(x) = 0$ for all $f \in I$ and $g \in J$. Assume that $x \notin Z(I)$. This means there exists $f \in I$ such that $f(x) \neq 0$. Thus whenever $g \in J$, we have $f(x)g(x) = 0$, which implies $g(x) = 0$. Thus $x \in Z(J)$.

It's possible to take the sum of arbitrarily many ideals. The sum of a collection of ideals is simply the smallest ideal containing all of them. Property 4 continues to hold:

$$Z\left(\sum_i I_i\right) = \bigcap_i Z(I_i)$$

An affine algebraic set is a subset of $\mathbf{A}^n$ of the form $Z(I)$ for some ideal I. We have seen that the collection of affine algebraic sets is closed under finite unions and arbitrary intersections, and contains both $\varnothing$ and $\mathbf{A}^n$.

This property led some mathematicians in the mid-20th century (Grothendieck) to define a *topology* on $\mathbf{A}^n$, called the Zariski topology, in which closed subsets are the affine algebraic sets.

4. Primes and irreducibles

Recall that a prime ideal P is a non-unit ideal having the property: If $fg \in P$, then $f \in P$ or $g \in P$ (or both).

Lemma 4.1. *If P is a prime ideal, and I, J are ideals such that $IJ \subset P$, then either $I \subset P$ or $J \subset P$.*

Proof. Assume $IJ \subset P$. Also assume that I is not contained in P: $I \not\subset P$. This means there exists $f \in I$ such that $f \notin P$. Let $g \in J$. We have $fg \in IJ \subset P$, so that $fg \in P$. Since P is prime, we have $g \in P$. Therefore $J \subset P$. □

What are the prime ideals in $K[x, y]$? (Assume K is an algebraically closed field.)

- $P = (x - a, y - b)$ (where $a, b \in K$) is prime, and in fact it is maximal. We have that $Z(P) = \{(a, b)\}$ is a single point.
- $P = (y - x^2)$ is prime but not maximal (it is contained in (x, y) for instance). In fact any non-maximal prime ideal P is of the form $(f(x, y))$, where $f(x, y)$ is an irreducible polynomial. Then $Z(P)$ is the solution set $\{(x, y) | f(x, y) = 0\}$. This solution set is a curve.
- $P = (0)$ is prime. $Z(0) = \mathbf{A}^2$.

These are in fact the only prime ideals.

Definition 4.2. *An affine algebraic set V is* reducible *if it can be represented as a union $V = V_1 \cup V_2$, where V_1, V_2 are other affine algebraic sets, but neither is equal to V. Otherwise, V is irreducible.*

Example 4.3. *The affine algebraic set $V = Z(xy) \subset \mathbf{A}^2$ is reducible: it is $Z(x) \cup Z(y)$. But $Z(y - x^2)$ is irreducible.*

Theorem 4.4. *The only irreducible affine algebraic sets are $Z(P)$, where P is a prime ideal.*

Proof. (One direction) Let P be a prime ideal in $K[x_1, \dots, x_n]$. Assume that $Z(P) = Z(I) \cup Z(J)$ for ideals I and J. Then $Z(P) = Z(IJ)$. We get $I(Z(P)) = I(Z(IJ))$, so that $P = \sqrt{IJ} \supset IJ$. This means that $I \subset P$ or $J \subset P$, which means that either $Z(I)$ or $Z(J)$ was equal to $Z(P)$. Thus $Z(P)$ is irreducible. □

5. Dimension

Let R be any commutative ring with unit. It might happen that we have chain of ideals

$$P_0 \subset P_1 \subset \cdots \subset P_n$$

all of which are prime. For instance if $R = K[x_1, \dots, x_n]$ we can look at

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \dots, x_n).$$

Definition 5.1. *The* Krull dimension *of the ring R is the maximum n for which there exists a chain of prime ideals of length n.*

For instance, the polynomial ring in n variables has Krull dimension n.

If $V \subset \mathbf{A}^n$ is an irreducible affine algebraic set, then $V = Z(I)$ for some ideal I, and then we can define the dimension of V to be the Krull dimension of $K[x_1, \dots, x_n]/I$.

For instance, $Z(y - x^2) \subset \mathbf{A}^2$ has dimension 1: it is a curve.

6. Projective space

I define projective space $\mathbf{P}^n$ to be the set of all nonzero points $(x_0, x_1, \dots, x_n)$, modulo multiplication by a nonzero scalar.

The projective version of the circle is the projective curve

$$x^2 + y^2 = z^2.$$

The formula we found last time is an isomorphism between the projective circle and $\mathbf{P}^1$. In fact any projective curve inside of $\mathbf{P}^2$ with degree 2 is isomorphic to $\mathbf{P}^1$.

But if I let X be the projective plane curve

$$x^3 + y^3 = z^3,$$

then this not isomorphic to $\mathbf{P}^1$. The set of complex solutions to this equation is a real manifold of dimension 2 (a surface). It is also closed (compact). In fact this is a torus, whereas $\mathbf{P}^1$ is a sphere. Therefore they are not isomorphic.

In fact there is a way of defining the *genus* (= number of holes) of a projective curve without reference to topology at all; the notion is well-defined for curves over finite fields, for instance. It turns out there are no non-constant algebraic maps from a curve of genus g to a curve of genus g', if $g < g'$.