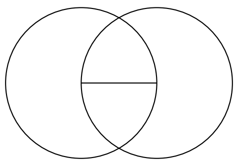
Getting to algebraic geometry's machinery ASAP but every move is motivated

Riley Levy

November 28, 2024

Classical algebraic geometry studies the *solution set* of systems of *polynomial* equations. These are geometric. For example, compass and straightedge constructions can be done through equations of lines and circles. Famously, their intersections can be found by solving a system of equations of circles and lines.

To construct the perpendicular bisector of a segment, draw two circles of equal radius on either side:



$$x^2 + y^2 = 1 \tag{1}$$

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

To find their intersections, we need to play the equations off each other. Expand eq. (2) to reveal an $x^2 + y^2$:

$$\begin{aligned}
\underbrace{x^2 + y^2}_{1} - 2x + \cancel{1} &= \cancel{1} \\
1 - 2x &= 0 \\
x &= 1/2. \qquad (3)
\end{aligned}$$

Our system of equations has grown: equations 1, 2 & 3 are all worth keeping. Further algebraic manipulations yield more equations. Of particular interest for this example is finding the corresponding ys:

$$\begin{aligned}
x^2 + y^2 &= 1 \\
x &= 1/2 \\
y^2 &= 3/4 \qquad (4)
\end{aligned}$$

I suppose I lied. We're not really interested in systems of equations. We're interested in the system of equations *and all its consequences*. The particular starting equations aren't so important. We could have started with

$$\begin{aligned}
x^2 + y^2 &= z^2 \\
(x-1)^2 + y^2 &= z^2 \\
z &= 1
\end{aligned}$$

or

$$\begin{aligned}
2x^2 + 2y^2 &= 2 \\
(x-1)^2 + y^2 &= 1
\end{aligned}$$

and would arrive at the same place.

Modernization 1 ❧ Focus on *sets generated by* a system of equations instead of a particular system.

They are ideals

To make this work, we need to take stock of what operations give new equations from old systems. Consider a single equation. If

$$f(x) = g(x),$$

then

$$f(x) + h(x) = g(x) + h(x).$$

Therefore, the placement of the equal sign is arbitrary. The following are equivalent:

$$\begin{aligned} x^2 + y^2 &= 1 \\ x^2 &= 1 - y^2 \\ x^2 + y^2 - 1 &= 0. \end{aligned} \tag{5}$$

To cut down on possibilities, pick a normal form. Put every equation in that last $= 0$ form:

$$F(x, y, z) = 0.$$

So our equation

$$f(x, y, z) = g(x, y, z)$$

becomes

$$f(x, y, z) - g(x, y, z) = 0.$$

This unifies our view of algebraic manipulations. We no longer need a special set of rules for equations: adding $h(x, y, z)$ to both sides becomes

$$f(x, y, z) + h(x, y, z) - h(x, y, z) - g(x, y, z) = 0,$$

the famous fact $h(x, y, z) - h(x, y, z) = 0$.

What can we do with a system of equations to pull out new equations?

1. Rescaling.

$$f = g \implies kf = kg,$$

2. Additivity.

$$\begin{aligned} f &= g \\ \phi &= \gamma \\ (f + \phi) &= (g + \gamma), \end{aligned}$$

3. Multiplicativity. If

$$\begin{aligned} f &= g \\ \phi &= \gamma \end{aligned}$$

then

$$(f\phi) = (g\gamma).$$

This differs from Rescaling because we're multiplying possibly different things on both sides of the equation.

4. Substitution. Take a function $A(t)$. Since we're doing algebraic geometry, $A(t)$ is a polynomial. If

$$f = g$$

then

$$A(f) = A(g).$$

We want to put these into our normal form. Rescaling and Additivity translate directly:

- Rescaling.

$$F = 0 \implies kF$$

- Additivity.

$$\begin{aligned} F &= 0 \\ G &= 0 \end{aligned}$$

then

$$(F + G) = 0.$$

If we tried to translate multiplicativity directly, we'd get

$$f = 0, g = 0 \implies fg = 0,$$

which is just a special case of rescaling. The real translation would be

$$\begin{gathered} f - g = 0 \\ \phi - \gamma = 0 \\ \Downarrow \\ (f\phi - g\gamma) = 0. \end{gathered}$$

We can actually get this using only Additivity and Rescaling in our normal form.

Theorem 1 (Multiplicativity is redundant) *If*

$$\begin{aligned} \alpha - \beta &= 0 \\ \gamma - \delta &= 0, \end{aligned}$$

then

$$\alpha\gamma - \beta\delta = 0.$$

Proof · We need to get an $\alpha\gamma - \beta\delta$, so multiply

$$(\alpha \mp \beta)(\gamma \pm \delta) = 0.$$

Then

$$\begin{array}{c|cc} \times & \gamma & -\delta \\ \hline \alpha & \alpha\gamma & -\alpha\delta \\ +\beta & +\beta\gamma & -\beta\delta \end{array} \qquad \underbrace{(\alpha\gamma - \beta\delta)}_{X} + \underbrace{(-\alpha\delta + \beta\gamma)}_{Y} = 0$$

$$\begin{array}{c|cc} \times & \gamma & +\delta \\ \hline \alpha & \alpha\gamma & +\alpha\delta \\ +\beta & -\beta\gamma & -\beta\delta \end{array} \qquad \overbrace{(\alpha\gamma - \beta\delta)}^{X} + \overbrace{(+\alpha\delta - \beta\gamma)}^{-Y} = 0$$

But then

$$X = -Y \qquad \text{and} \qquad X = Y. \qquad \square$$

Conclude $X = -X$, so* $X = 0$.

This deduction is not valid in every ring.

Substitution, too, is really a consequence of Additivity and Rescaling.

Theorem 2 *If* $P(t)$ *is a polynomial and*

$$f - g = 0,$$

then

$$P(f) - P(g) = 0,$$

and this is a consequence of only Additivity and Rescaling.

Proof · Because P is a polynomial,

$$P(t) = a_0 + a_1 + \dots a_n t^n.$$

By additivity, it suffices to prove the theorem for monomials. By rescaling, it suffices to prove it for exponents only. But if $f - g = 0$, then by theorem 1, $f^n - g^n = 0$. □

Since the right-hand side is just $= 0$, the same for everything now, focus on the left-hand side only. The set of left-hand sides generated by a system of equations must satisfy three properties:

Definition 3 (Ideal) The set $I \subseteq R$ is an *ideal* iff

Because $0 = 0$.

- $0 \in I$.
- Absorbativity (rescaling) under multiplication:

$$\alpha \in I, k \in R \implies k\alpha \in I.$$

I change to absorbativity from rescaling to emphasize that it's true for *any* $k \in R$, *i.e.*, I absorbs multiplication. It's not merely closed.

- Closure under addition:

$$\alpha, \beta \in I \implies \alpha + \beta \in I.$$

This abstracts the idea of systems of equations and their consequences. Recover a system of equations by saying $f(x, y, z) = 0$ for all $f \in I$.

Explicit reference to equations and polynomials have been removed!

Modernization 2 (equations $\to$ ideals) Instead of systems of polynomial equations, work with ideals. Systems of polynomial equations are an important special case.

Where does the notion of ideal make sense? Anywhere with an addition and multiplication operator satisfying the usual rules:

Definition 4 (Ring) A ring is a set R with $+, \cdot$ such that

- $(R, +, 0)$ is a *commutative group*
  - additive identity: $x + 0 = 0 + x = x$
  - negation: $x + (-x) = 0$
  - associativity: $(x + y) + z = x + (y + z)$
  - commutativity: $x + y = y + x$
- Multiplication is associative:

$$(xy)z = x(yz)$$

- There is a multiplicative identity 1:

$$x1 = 1x = x$$

- Multiplication *distributes* over addition:

$$x(y + z) = xy + xz \qquad (y + z)x = yx + zx$$

- Multiplication is commutative:

$$xy = yx$$

Often, commutativity is not required, but for our purposes, it will be

The integers are the original ring. Polynomials over a ring are also rings, denoted

$$R[x, y, z]$$

We're especially interested in $\mathbb{C}[x, y, z]$.

The ideals *generated by* the elements a, b, c, d is written

$$(x, y, z, t) = \{ax + by + cz + dt : a, b, c, d \in R\},$$

i.e., sums of multiples of its generators.

In the integers, something simpler happens:

Theorem 5 *Every ideal of integers* I *is the set of multiples of a single element,* i.e.,

$$I = (x)$$

Proof · If $I = \{0\}$, then $I = (0)$, done.

Otherwise, I has at least one nonzero element. Because of absorbativity of multiplying by -1, pick the smallest positive $x \in I$. Let $y \in I$ be an arbitrary but nonzero. By repeatedly subtracting, starting with $y - x$, (Euclid's algorithm), find $\mathsf{gcd}(x, y) \in I$ by closure. Then

$$0 < \mathsf{gcd}(x, y) \leqslant x,$$

but by assumption, x is the smallest nonzero element. Conclude $\mathsf{gcd}(x, y) = x$, so y is a multiple of x. Because y was arbitrary, this holds for every nonzero element. It is also true for zero because $0x = 0$. □

What about $\mathbb{Q}$? The difference between $\mathbb{Z}$ and $\mathbb{Q}$ is every nonzero element has a multiplicative inverse in $\mathbb{Q}$.

Theorem 6 *If* $x \in R$ *has inverse* x^{-1}*, then*

$$(x) = R.$$

Proof · By hypothesis,

$$xx^{-1} = 1,$$

so $1 \in (x)$. But then $y = y1 \in R$ by absorbativity for every $y \in R$. □

The converse is true too:

Theorem 7 *If $(x) = R$, then x has an inverse in R.*

Proof · By hypothesis, $1 \in (x)$, so 1 is a multiple of x. There is some $y \in R$ such that

$$yx = 1,$$

so $x^{-1} = y \in R$. □

Ideals measure the failure of invertibility. Rings where every inverse exists deserve a name:

> Definition 8 (Field) A field is a ring where every nonzero element has a multiplicative inverse.

$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are rings. So is the set of *rational* functions.

Corollary 9 *The only ideals in a field F are $\{0\}$ and F.*