Gröbner bases: theory and applications

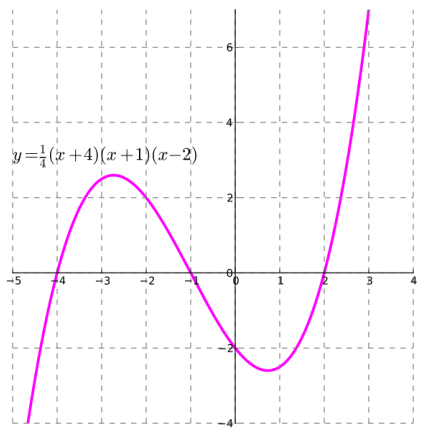
Steven Sam

Miller Institute lunch talk
November 25, 2014

Algebraic geometry is the study of polynomial functions.

Example

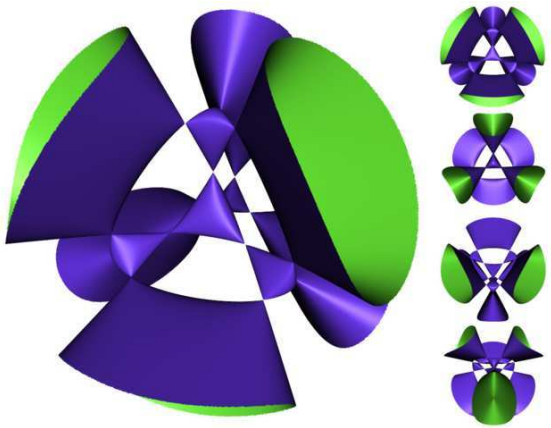
Polynomial functions on $\mathbf{C}^2$ are polynomials in two variables, like $x^2 + 2xy + y + 1$ or $x^3 + y^5$.



Polynomial functions on $\mathbf{C}^n$ are polynomials in n variables $x_1, x_2, \ldots, x_n$.
(x_i is the function which measures the ith coordinate of a point in $\mathbf{C}^n$.)

Given n-variable polynomials $f_1, f_2, f_3, \ldots$, the **zero set (algebraic variety)** is the common solutions, i.e., all $(z_1, \ldots, z_n)$ such that

$$f_1(z_1, \ldots, z_n) = f_2(z_1, \ldots, z_n) = \cdots = 0.$$



Theorem (Hilbert? 1890)

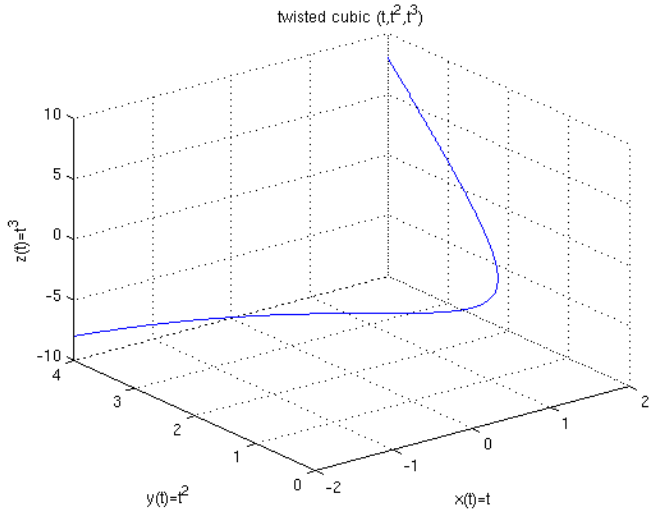
An algebraic variety has a description using finitely many polynomials.

Theorem (Eisenbud–Evans 1973)

In fact, only need n polynomials for description.

Algebraic varieties can be given by parametrizations:

Let $X \subset \mathbf{C}^3$ be the set of points of the form (t, t^2, t^3) (the rational normal cubic).



Alternatively, X is the zero set of
$x^2 - y, \qquad xy - z, \qquad xz - y^2.$

Generally, we might be given a polynomial map $\mathbf{C}^m \to \mathbf{C}^n$.
Implicitization problem: describe the image as a zero set.

An **ideal** is a collection of polynomials closed under addition and outside multiplication.

Dedekind

Theorem (Hilbert basis theorem 1890)

Every ideal is finitely generated.

Ideal membership problem: How do you determine if g is in the ideal generated by $f_1, \ldots, f_r$?

In one variable case, all ideals are generated by *one* polynomial.

The ideal membership problem reduces to long division and checking if the remainder is 0:

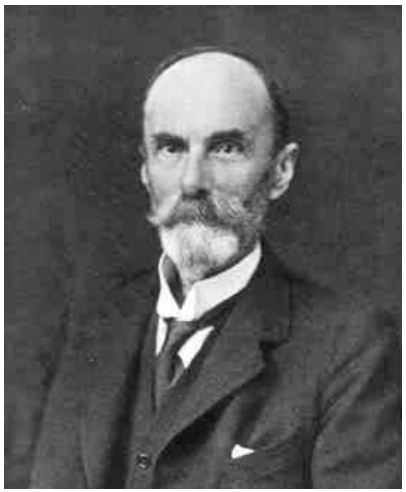
Euclid

Example

Dividing $x^3 + x^2 - 1$ by $x - 1$ gives remainder of 1:

$$x^3 + x^2 - 1 = (x^2 + 2x + 2)(x - 1) + 1$$

So $x^3 + x^2 - 1$ is not in the ideal generated by $x - 1$.


Macaulay

Long division works in one variable because we know what the "biggest" term in a univariate polynomial is.

But what about two variables? What is the biggest term of $x^2 + xy + y^2$?

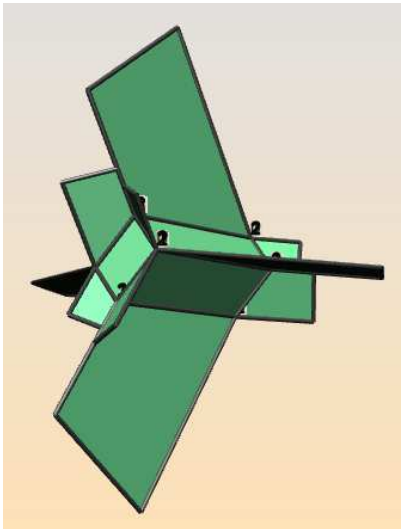
An option: compare terms by degree and then by dictionary order.

(First compare the exponent of x_1; if they're the same, move on to the exponent of x_2, etc.)

In the example above, x^2 is the biggest term ("leading term").

Division algorithm

Let $f_1, \ldots, f_r$ be a set of generators for an ideal I. We want to test if g is in I.



Check if the leading term of g is divisible by the leading term of some f_i.

If so, subtract a suitable multiple of f_i from g to get a polynomial with smaller leading term.

Example

If $g = x^3 + xy^2$ and $f = x^2 + xy + y^2$, then subtract xf from g to cancel the x^3 term.

Then repeat: when you can't proceed, you get a remainder. If the remainder is 0, then g is in the ideal.

Potential problem with division algorithm

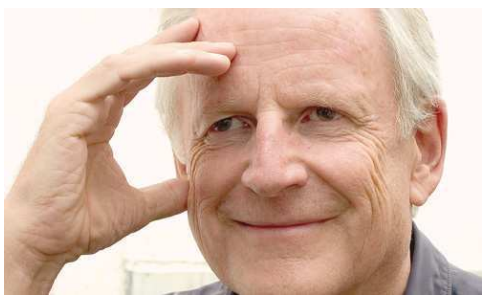
Problem: g might be in the ideal but still have nonzero remainder.

Example

$f_1 = x^3 + xy^2$ and $f_2 = x^3 + x^2y + y^3$.
Then $g = xy^3 - y^4$ is in the ideal

$$g = (x + 2y)f_1 + (-x - y)f_2$$

but g is its own remainder: leading term xy^3 isn't divisible by x^3.



Buchberger

A **Gröbner basis** is a generating set with the property that the division algorithm always works.

How to construct a Gröbner basis:

If the division algorithm fails for g, then add the remainder of g to the generating set.

Repeat: if no such g exists after a finite number of steps, the result is a Gröbner basis.


Gordon

This algorithm always terminates because of Dickson's lemma:

Lemma (Dickson)

Given a list of monomials $m_1, m_2, \ldots$, you can always find two indices $i < j$ so that m_i divides m_j.

Implicitization problem, revisited

Recall our rational normal cubic is the set of points (t, t^2, t^3).

Introduce new variables x, y, z and consider ideal generated by

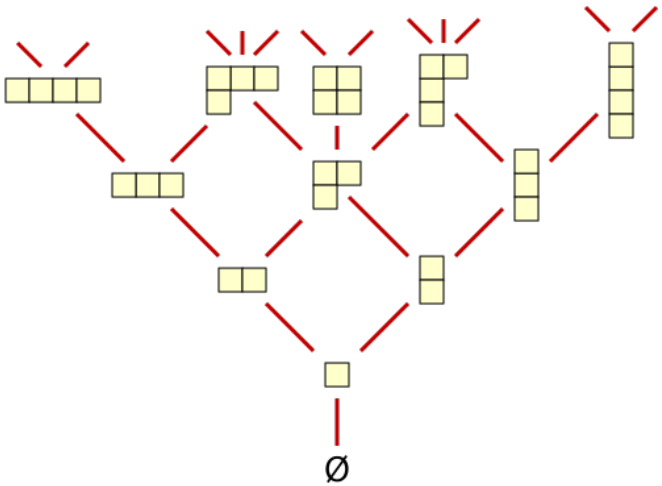
$$x - t, \qquad y - t^2, \qquad z - t^3.$$

Compute Gröbner basis with ordering $t < x < y < z$ and you get:

$$y^3 - z^2, \qquad xz - y^2, \qquad xy - z, \qquad x^2 - y, \qquad t - x$$

The polynomials that don't use t give zero set description of rational normal cubic.
($y^3 - z^2 = -y(xz - y^3) + z(xy - z)$ is redundant)

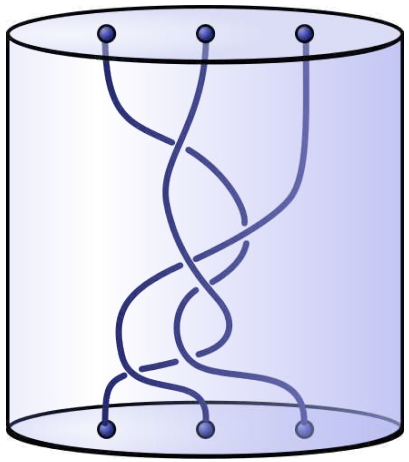
I've recently been interested in algebraic structures that arise in "representation stability" and "equivariant noetherianity".



Noether

A common theme is to identify new algebraic structures that govern existing mathematical objects and to study their properties to get new information.

My research



I'm studying analogues of Hilbert's basis theorem and Gröbner bases for new algebraic structures which give finite generation statements for objects such as:

- Cohomology of configuration spaces
- Homology of congruence subgroups
- Syzygies of Segre varieties

Our work solved the Lannes–Schwartz artinian conjecture in algebraic topology which was open for 25 years.
(Recently featured in Séminaire Bourbaki)

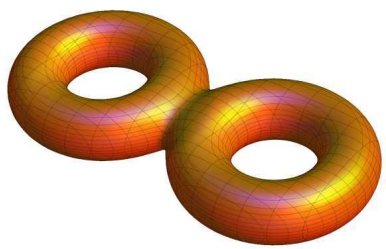
Here are two sample questions we still can't answer.

Question

Fix r. Is there a constant $d(r)$ so that the ideal of polynomials vanishing on the tensors of (border) rank $\leq r$ is generated in degree $\leq d(r)$?

Question

Can the homology of the Torelli group of a genus g surface be described in terms of the homology of lower genus Torelli groups for $g \gg 0$?



Thanks!

- Miller Institute
- Talk coaches: Francesco, Shayan
- Faculty hosts: David Eisenbud, Bernd Sturmfels
- Collaborators: Andy Putman (Rice), Andrew Snowden (Michigan)