(Commutative) Rings and Things

Sean Sather-Wagstaff

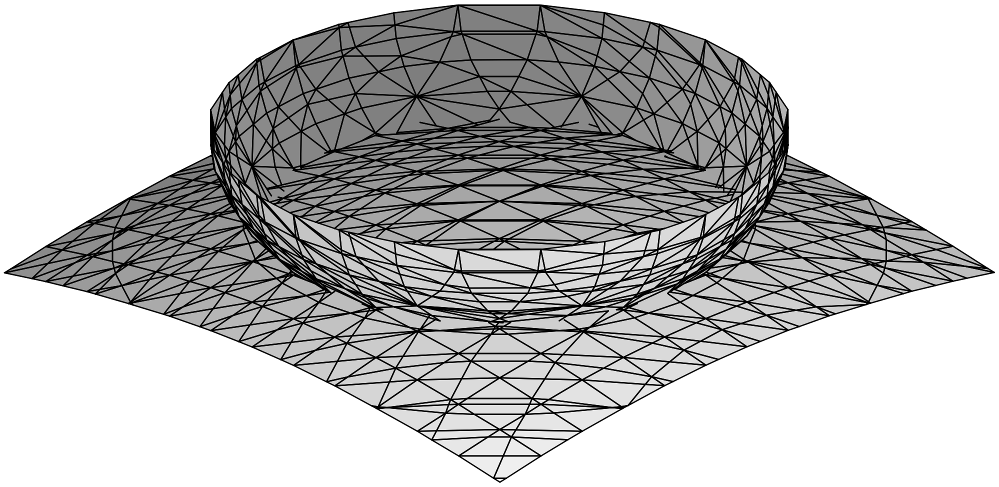
7 September 1999

ABSTRACT

Algebra is one of the most fundamental subjects in mathematics. It is usually the first subject encountered by young mathematicians on their paths to other subjects. Many students fail to realize that algebra is a beautiful area which is not only interesting in its own right but also incredibly useful as a language and tool for working in a variety of other fields. In particular, commutative ring theory is one of the powerful tools used by algebraic geometers in the study of modern geometric questions. In this talk, I will introduce the basic objects of study in commutative algebra, especially focusing on rings of polynomials and their geometric counterparts.

Question. Which of the following is a ring?

(a) The geometric object?



(the intersection of the two surfaces)

(b) The algebraic object?

$$\boxed{k[x,y,z]/\langle x^2+y^2-z^2+1, x^2+y^2+0.2z^2-1\rangle}$$

Answer. Both (a) and (b).

I. RINGS

In our careers as mathematicians, we have come across many examples of *number systems*. For example, we are more or less familiar with

- The integers $\mathbb{Z}$.
- The rational numbers $\mathbb{Q}$.
- The real numbers $\mathbb{R}$.
- The complex numbers $\mathbb{C}$.

There are other examples which we may not think of in the same way even though they share similar characteristics:

- The set of polynomials of the form $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $a_n, \ldots, a_0$ in $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$.

- The set of rational functions $\dfrac{f(x)}{g(x)}$ where $f(x)$ and $g(x)$ are polynomials.

- The set $M_n(\mathbb{Z})$ of $n \times n$ matrices with entries in $\mathbb{Z}$.

- The set of functions (continuous functions, differentiable functions) $f : \mathbb{R} \to \mathbb{R}$ with point-wise addition and multiplication.

- The set of even integers.

What traits do these examples share?

Each is a *ring*: a set R with two binary operations "$+$" and "$\cdot$" defined on R satisfying the following properties:

R1 (Associativity) $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

R2 (Commutativity of Addition) $a+b = b+a$ for all $a, b \in R$.

R3 (Distributivity) $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

R4 (Additive Identity) There is $0 \in R$ such that $a + 0 = a = 0 + a$ for all $a \in R$.

R5 (Additive inverses) For every $a \in R$ there exists $b \in R$ such that $a + b = 0$.

In commutative ring theory, we restrict our attention to *commutative rings with identity*, that is, rings which also satisfy the following properties.

C1 (Commutativity of Multiplication)
$a \cdot b = b \cdot a$ for all $a, b \in R$.

C2 (Multiplicative Identity) There is $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a$ for all $a \in R$.

Example. The matrix ring $M_n(\mathbb{Z})$ has a multiplicative identity

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

However, multiplication is not commutative for $n \geq 2$.

Warning! We do not require that multiplicative inverses exist in a ring. For example, even though the number 2 is an integer, the number $\frac{1}{2}$ is not an integer.

Exercise. For $n = 2, 3, \ldots$, find matrices $M, N \in M_n(\mathbb{Z})$ such that $M \cdot N \neq N \cdot M$. (Hint: Start with $n = 2$.)

Exercise. Prove that the matrix ring $M_1(\mathbb{Z})$ is a commutative ring with identity.

Exercise. Prove that the multiplication on the ring of even integers is commutative.

Exercise. Prove that the ring of even integers does not contain a multiplicative identity.

Exercise. Of the other rings listed above, which are commutative rings with identity?

Historical note. The term “ring” was first used by Dieudonné. Allegedly, he chose this word to express the fact that the absence of division in a ring is a fundamental defect; hence, a ring has a hole.

II. POLYNOMIAL RINGS

Our first intuition about rings comes from $\mathbb{Z}$. However, this is too specific. Our perspective will be broadened considerably by considering rings of polynomials.

For the rest of this talk, let K be $\mathbb{R}$ or $\mathbb{C}$.

Definition. A *polynomial* in $x_1, \ldots, x_n$ with coefficients in K is a finite sum whose terms are of the form $ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ where $a \in K$ and each α_i is a nonnegative integer.

Example. Polynomials in $x_1, \ldots, x_6$ with coefficients in $\mathbb{R}$:

$$\begin{aligned} f &= 1 + x_1 + x_1^2 - x_1 x_2^3 \\ g &= 3 + x_1 - 5x_1^2 x_3^5 + \sqrt{2} x_2 x_3 x_5 - \pi x_4^7 x_6^8 \end{aligned}$$

Polynomials with coefficients in $\mathbb{C}$:

$$\begin{aligned} h &= (4 + i)x_1 - i x_4 x_5 \\ k &= 4 + 3x_6^4 + (3 + \pi i)x_5 \end{aligned}$$

We denote the set of polynomials in $x_1, \ldots, x_n$ with coefficients in K as $K[x_1, \ldots, x_n]$. (We will often use the letters x, y in place of x_1, x_2.)

As with the polynomials in one variable, $K[x_1, \ldots, x_n]$ has the structure of a commutative ring with identity.
The additive identity is the constant polynomial 0, and the multiplicative identity is the constant polynomial 1.

We add polynomials term-by-term, and we multiply them by distributing and collecting like terms—a long version of FOIL.

Example.
$(2x+ixy)+((1+i)x+3y^2) = (3+i)x+ixy+3y^2$

Example.

$$
\begin{aligned}
&(2x + y) \cdot (x^2 - xy + z) \\
&\quad = 2x \cdot x^2 - 2x \cdot xy + 2x \cdot z + y \cdot x^2 - y \cdot xy + y \cdot z \\
&\quad = 2x^3 - 2x^2y + 2xz + x^2y - xy^2 + yz \\
&\quad = 2x^3 - x^2y + 2xz - xy^2 + yz
\end{aligned}
$$

Exercise. Write down two polynomials in $\mathbb{C}[x, y, z, w]$. Now add them and multiply them.

III. AFFINE SPACE AND POLYNOMIALS AS FUNCTIONS

Definition. Given a positive integer n, we define n-dimensional *affine space* as the set

$$K^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in K\}$$

Example. If $K = \mathbb{R}$, then $K^1 = \mathbb{R}^1$ is the real line. $\mathbb{R}^2$ is the real plane (or the Cartesian plane) consisting of all 2-vectors with real entries. $\mathbb{R}^3$ is real 3-space, and so on.

With a polynomial $f(x)$ in one variable, we may substitute values for the variable. This gives us a function $f : K \to K$.

Example. If $f(x) = 3x^4 - 5x + 1 \in \mathbb{C}[x]$, then the function $f : \mathbb{C} \to \mathbb{C}$ is given by the rule $f(a) = 3a^4 - 5a + 1$ for $a \in \mathbb{C}$. For example, $f(i) = 3(i)^4 - 5i + 1 = 3 - 5i + 1 = 4 - 5i$.

Often, we are interested in solving the equation $f(x) = 0$, that is, in finding all elements $a \in K$ such that $f(a) = 0$. The solution set is a subset of $K = K^1$.

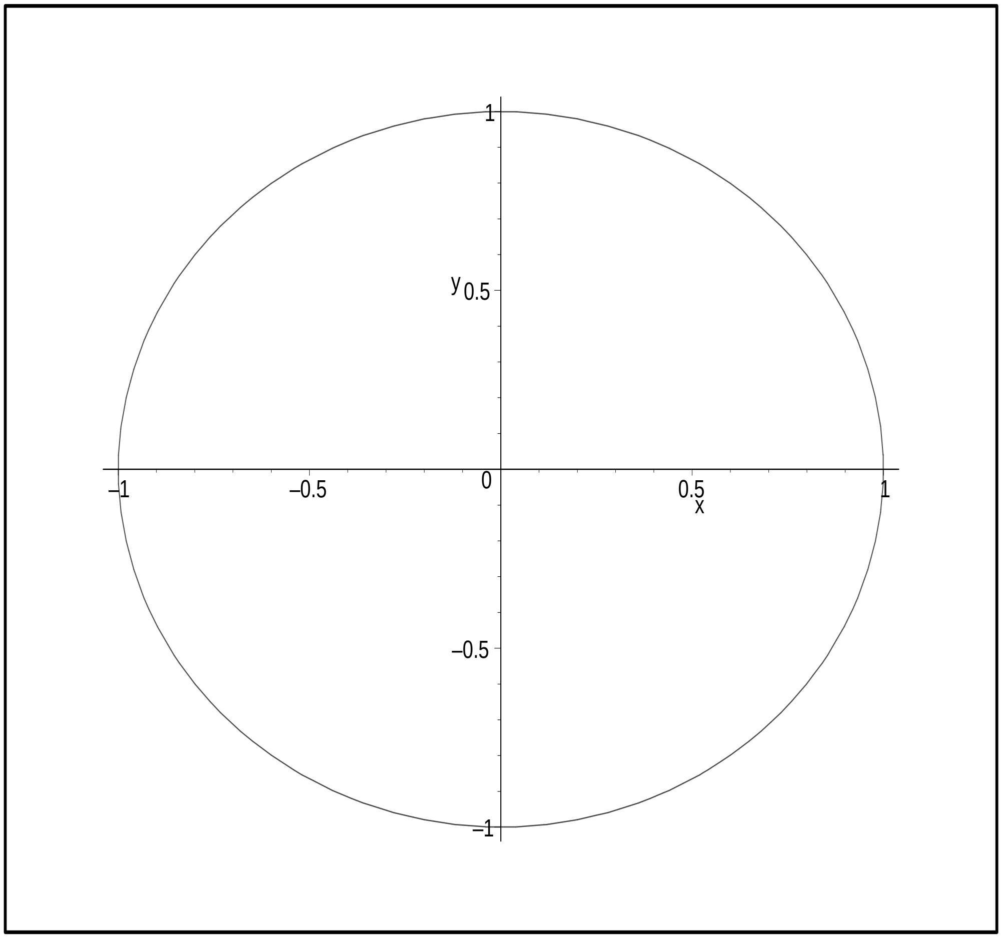
When we increase the number of variables and consider polynomials $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, there are n variables to substitute for. This gives us a function $f : K^n \to K$.

Example. If $f(x_1, x_2, x_3) = x_1^2 - x_2x_3$ considered in $\mathbb{C}[x_1, x_2, x_3]$, then

$$f(1, 2i, -3) = (1)^2 - (2i)(-3) = 1 + 6i.$$

Again, we will be interested in solving the equation $f(x_1, \ldots, x_n) = 0$. The solution set is a subset of K^n.

Example. Let $K = \mathbb{R}$ and consider the polynomial $f(x, y) = x^2 + y^2 - 1$. The solution set of the equation $x^2 + y^2 - 1 = 0$ is exactly the unit circle in $\mathbb{R}^2$



because the equation is equivalent to the equation $x^2 + y^2 = 1$.

Example. Let $K = \mathbb{R}$ still and consider the polynomial $g(x, y) = x^2 + y^2 + 1$. There are no solutions to the equation $x^2 + y^2 + 1 = 0$ because this equation is equivalent to the equation $x^2 + y^2 = -1$ and the sum of the squares of two real numbers is positive. Notice how sensitive $\mathbb{R}$ is to subtle changes in the polynomial. Just by changing the constant term from -1 to 1 we change from an infinite number of solutions to no solutions.

Example. Let $K = \mathbb{C}$ this time and consider the same polynomial $g(x, y) = x^2 + y^2 + 1$. It is straightforward to find solutions to this equation, for example, $(\pm i, 0)$ and $(\pm i\sqrt{2}, \pm 1)$. It is impossible for us to graph the solution set in $\mathbb{C}^2$ because this corresponds to $\mathbb{R}^4$.

Exercise. Graph the solution set of the equation $y^2 - x^2(x + 1) = 0$ in $\mathbb{R}^2$. Can you find any solutions in $\mathbb{C}^2$ which are not in $\mathbb{R}^2$?

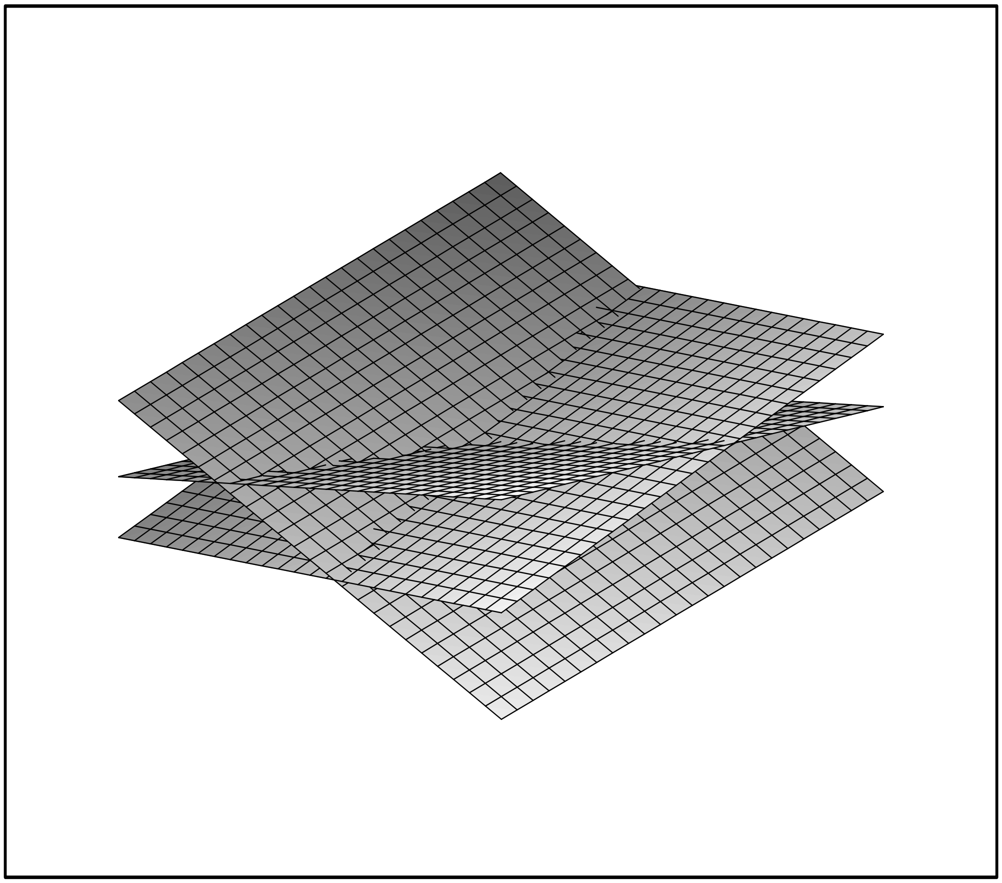
IV. AFFINE VARIETIES: GEOMETRY HELPS THE ALGEBRAIST

In college algebra we learned to solve linear equations like $3x + 5y - 7 = 0$. Then we learned to solve *systems* of linear equations.

$$\begin{array}{r}3x+5y-7z=1\\2x-3y+6z=2\\-x-4y-8z=4\end{array}$$

Algebraically, we solve the system using Gaussian elimination. Geometrically, the solution set to the system is the set of points where the graphs of the individual equations intersect.

Sometimes we want to know the solution set exactly. Other times, however, we only care about certain properties of the solution set. Are there any solutions? If so, are there finitely many or infinitely many? Inspection of the graph often leads to more insight.



Because we are a visual species, viewing solution sets as pictures helps us tremendously.

More generally, we can try to solve systems of polynomial equations. Determining the properties of the solution sets of such systems is one of the central motivating problems of classical algebraic geometry.

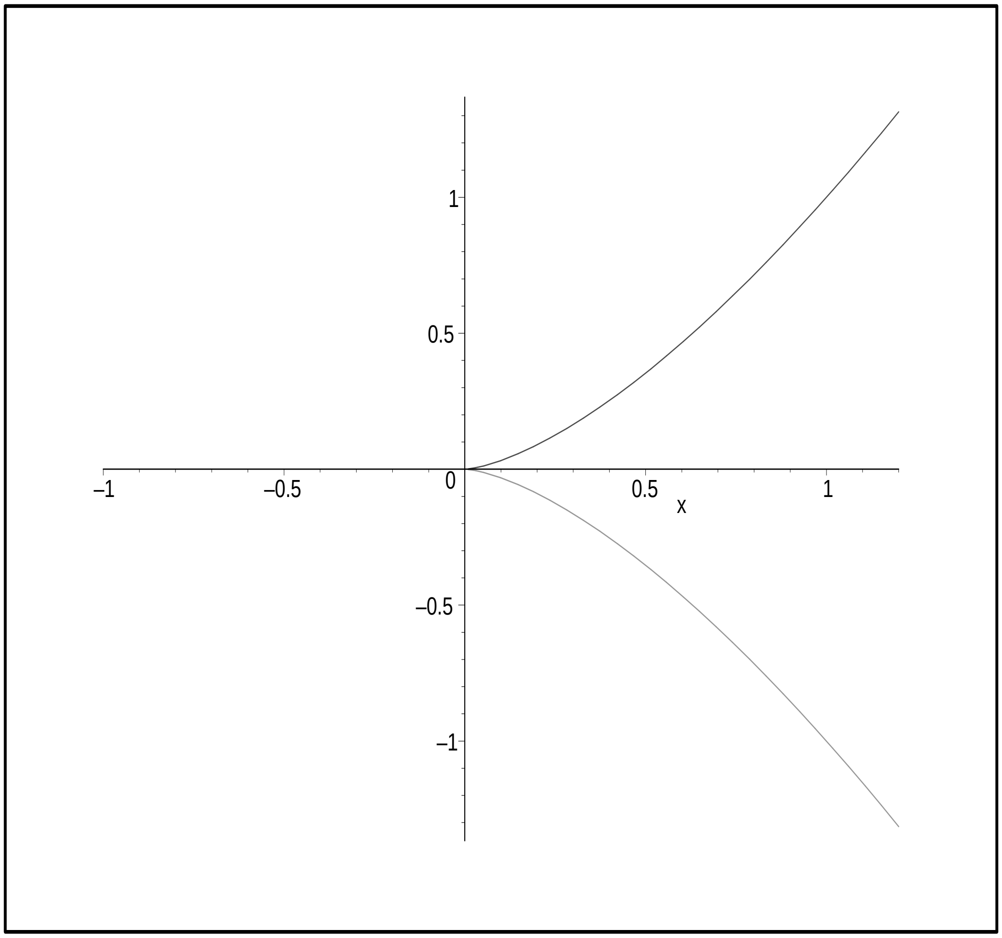
Definition. Let $f_1, \ldots, f_s$ be polynomials in $K[x_1, \ldots, x_n]$. The *affine variety* determined by $f_1, \ldots, f_s$, denoted $V(f_1, \ldots, f_s)$, is the subset of K^n consisting of all elements $(a_1, \ldots, a_n) \in K^n$ such that

$$f_i(a_1, \ldots, a_n) = 0, \qquad i = 1, \ldots, s$$

In other words, $V(f_1, \ldots, f_s)$ is the zero locus of the polynomials $f_1, \ldots, f_s$.

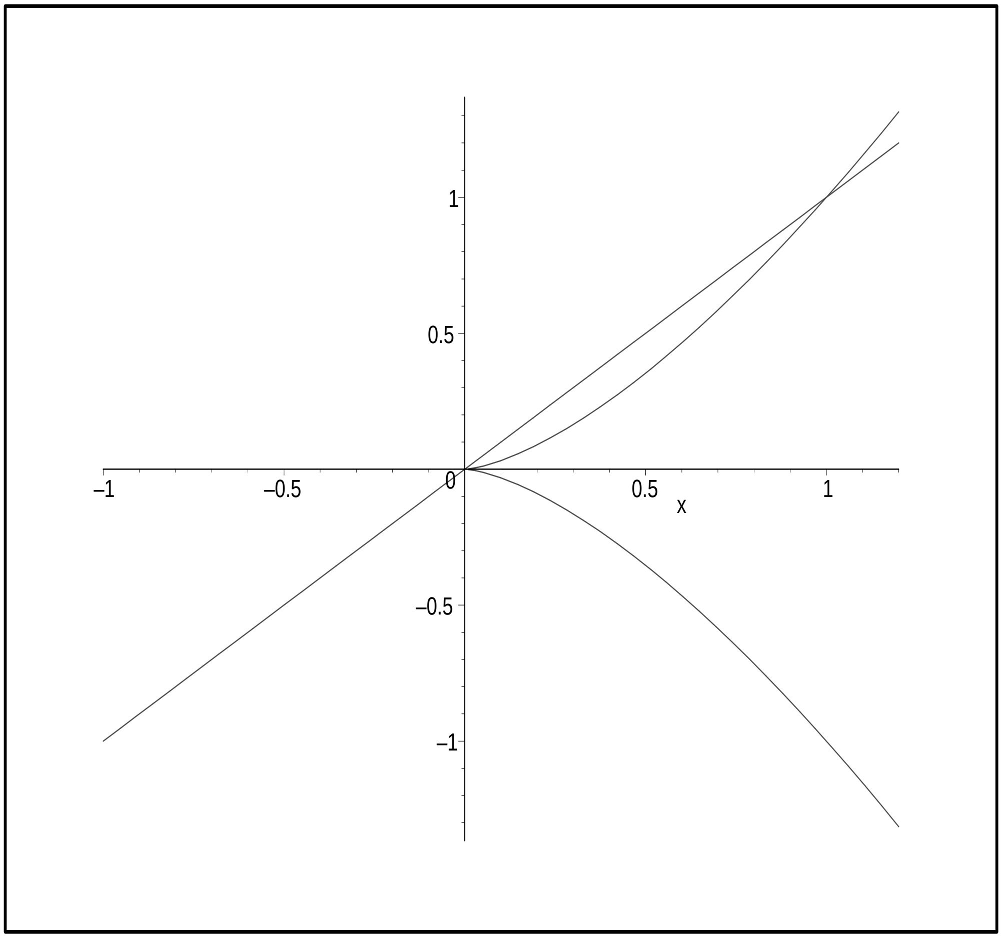
Analogous to our system of linear equations, $V(f_1, \ldots, f_s)$ is the set of points of K^n which are in the intersection of the varieties $V(f_1), \ldots, V(f_s)$.

Example. The set $V(x^3 - y^2)$ in $\mathbb{R}^2$ is the graph of the equation $x^3 - y^2 = 0$.



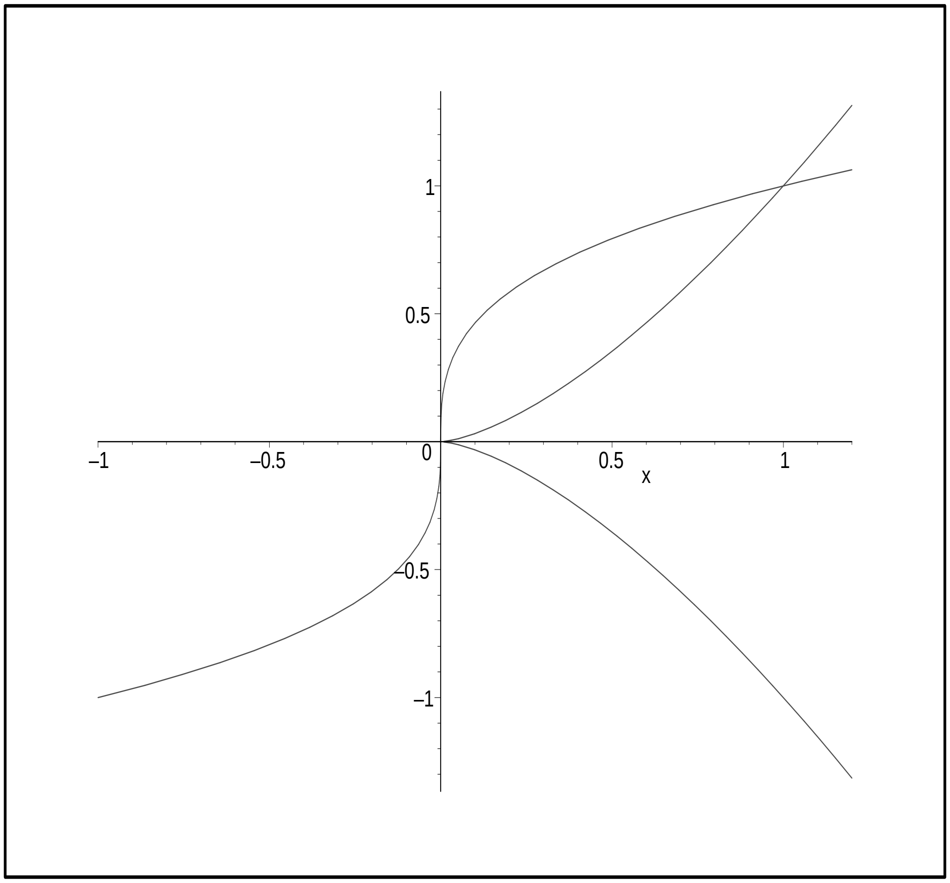
It is called the *cuspidal cubic* due to the cusp at the origin and the fact that the polynomial defining it has degree 3.

Example. The set $V(x^3 - y^2, x - y)$ in $\mathbb{R}^2$ is the intersection of the graphs of the equations: $x^3 - y^2 = 0, \quad x - y = 0$



It is the intersection of the cuspidal cubic with the line $y = x$. Solving this system by substitution shows that the points $(0, 0)$ and $(1, 1)$ are the only points in this set.

Example. The set $V(x^3 - y^2, x - y^3)$ in $\mathbb{R}^2$ is the intersection of the graphs of the equations: $x^3 - y^2 = 0, \quad x - y^3 = 0$



It is the intersection of the cuspidal cubic with the cubic $y^3 = x$. Again, we see that the points $(0, 0)$ and $(1, 1)$ are the only points in this set. Notice that this is the same variety as in the previous example, even though the equations are not the same.

When we consider the previous two examples over $\mathbb{C}$ instead of over $\mathbb{R}$, we find that the first still has 2 points, while the second has 8 points. Thus, over different fields, varieties defined by the same equations can have different numbers of points. (We knew this from the example $x^2 + y^2 = -1$.)

The complex numbers are very special for a number of reasons. The first reason is known as the Fundamental Theorem of Algebra.

Theorem. Any nonconstant polynomial with coefficients in $\mathbb{C}$ has a zero in $\mathbb{C}$.

We shall see other reasons later.

Fundamental Question. Given two sets of polynomials $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ in $K[x_1, \ldots, x_n]$, when are the varieties $V(f_1, \ldots, f_s)$ and $V(g_1, \ldots, g_t)$ equal?

Exercise. Find the 8 points of $V(x^3 - y^2, x - y^3)$ in $\mathbb{C}^2$. (Hint: One new point has y-coordinate $y = cos(\frac{2\pi}{7}) + i\,\mathrm{sin}(\frac{2\pi}{7})$.)

Exercise. Find the sets $V(x^3 - y^2, x - y^2)$ and $V(x^3 - y^2, x^2 - y^2)$ in $\mathbb{R}^2$ and in $\mathbb{C}^2$.

V. IDEALS: ALGEBRA HELPS THE GEOMETER

Let us return to Earth for a moment and consider the ring of integers. Let $2\mathbb{Z}$ denote the set of even integers, that is,

$$2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$$

As we noted previously, $2\mathbb{Z}$ is a commutative ring without identity. This is essentially the statement that

$$\text{(even)} + \text{(even)} = \text{(even)}.$$

We also know that any number multiplied by an even number yields an even number. This follows from the fact that

$$\text{(number)(even)} = (m)(2n) = 2mn = \text{even}$$

Similarly, if r is any integer, we let

$$r\mathbb{Z} = \{rn : n \in \mathbb{Z}\}.$$

Each of these sets is closed under addition, that is, if you add any two multiples of r you get another multiple of r. Furthermore, if we multiply any integer by a multiple of r, we get another multiple of r. Finally, since $0 = r \cdot 0$, we see that 0 is in $r\mathbb{Z}$. This says that $r\mathbb{Z}$ is an *ideal* of $\mathbb{Z}$. More generally, we have

Definition. Let R be a commutative ring with identity and let I be a subset of R. Then I is an *ideal* in R if the following are satisfied.

I1 $0 \in I$.

I2 For all $a, b \in I$, $a + b \in I$.

I3 For all $a \in I$ and $c \in R$, $c \cdot a \in I$.

Notice that **I3** says that if we multiply something inside the ideal by anything, whether from inside or outside the ideal, the result is inside the ideal.

The term "ideal" comes from number theory. When number theorists were attempting to generalize the ring of integers to general rings, they looked for "ideal numbers" which were subsets of rings which had the same properties as the sets $r\mathbb{Z}$.

Example. Let $\mathcal{C}(\mathbb{R})$ denote the ring of continuous functions $f : \mathbb{R} \to \mathbb{R}$ with pointwise addition and multiplication. This is a commutative ring with identity. (Why?) Let I denote the set of continuous functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(0) = 0$. We verify that this is an ideal.

I1 The constant function 0 is continuous and $0(0) = 0$.

I2 If f and g are continuous functions such that $f(0) = g(0) = 0$, then the function $f + g$ is continuous and

$$(f + g)(0) = f(0) + g(0) = 0 + 0 = 0$$

I3 If f and h are continuous functions and $f(0) = 0$, then the product function $h \cdot f$ is continuous and

$$(h \cdot f)(0) = h(0) \cdot f(0) = h(0) \cdot 0 = 0$$

Example. Let $f_1, \ldots, f_s$ polynomials in $K[x_1, \ldots, x_n]$. Let $V = V(f_1, \ldots, f_s)$ be the variety determined by the f_i, and let $I(V)$ denote the set of polynomials $f \in K[x_1, \ldots, x_n]$ such that

$$f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V$$

This is similar to the previous example, as we are considering the set of all (polynomial) functions which vanish on a certain set. As in the previous example, $I(V)$ is an ideal of $K[x_1, \ldots, x_n]$. Furthermore, each $f_i \in I(V)$.

Example. Let $f_1, \ldots, f_s$ be polynomials in $K[x_1, \ldots, x_n]$ and let $\langle f_1, \ldots, f_s \rangle$ denote the set of sums of the form

$$h_1 f_1 + \cdots + h_s f_s$$

with $h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$ This is called the *ideal generated by* $f_1, \ldots, f_s$. It is, in fact, an ideal in $K[x_1, \ldots, x_n]$ and contains the f_i. Furthermore, it is the smallest such ideal.

Exercise. Prove that the sets $I(V)$ and $\langle f_1, \ldots, f_s \rangle$ from the above examples are ideals in $K[x_1, \ldots, x_n]$ which contain $f_1, \ldots, f_s$. Prove that $\langle f_1, \ldots, f_s \rangle \subseteq I(V)$.

Example. Let I be any ideal in $K[x_1, \ldots, x_n]$ and let $\sqrt{I}$ denote the set of polynomials $f \in K[x_1, \ldots, x_n]$ such that

$$f^m \in I \text{ for some positive integer } m$$

$\sqrt{I}$ is called the *radical* of I. It is also an ideal, and it contains I.

Bonus Exercise. Prove that $\sqrt{I}$ is an ideal containing I.

The preceding three examples are of the most important algebraic tools in classical algebraic geometry.

Fundamental Question. Given two sets of polynomials $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ in $K[x_1, \ldots, x_n]$, when are the ideals $\langle f_1, \ldots, f_s \rangle$ and $\langle g_1, \ldots, g_t \rangle$ equal?

Fundamental Question. Given two sets of polynomials $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ in $K[x_1, \ldots, x_n]$, when are the ideals $I(V(f_1, \ldots, f_s))$ and $I(V(g_1, \ldots, g_t))$ equal?

It turns out that the answers to these questions is deeply related to our first Fundamental Question.

Theorem. Given two sets of polynomials $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ in $K[x_1, \ldots, x_n]$, if the ideals $\langle f_1, \ldots, f_s \rangle$ and $\langle g_1, \ldots, g_t \rangle$ are equal then the varieties $V(f_1, \ldots, f_s)$ and $V(g_1, \ldots, g_t)$ are equal.

Note that the converse is not true. As we noted previously, the varieties $V(x^3 - y^2, x - y)$ and $V(x^3 - y^2, x - y^3)$ in $\mathbb{R}^2$ are equal. However, with a little work, we can check that the ideals $\langle x^3 - y^2, x - y \rangle$ and $\langle x^3 - y^2, x - y^3 \rangle$ are not equal. In general over $\mathbb{R}$, the ideals generated by two sets of polynomials can be quite different. This can not happen over $\mathbb{C}$, however.

Theorem. (Hilbert's Nullstellensatz) Given a set of polynomials $f_1, \ldots, f_s$ in $\mathbb{C}[x_1, \ldots, x_n]$

$$I(V(f_1, \ldots, f_s)) = \sqrt{\langle f_1, \ldots, f_s \rangle}$$

Corollary. Given two sets of polynomials $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ in $\mathbb{C}[x_1, \ldots, x_n]$, the varieties $V(f_1, \ldots, f_s)$ and $V(g_1, \ldots, g_t)$ are equal if and only if the ideals $\sqrt{\langle f_1, \ldots, f_s \rangle}$ and $\sqrt{\langle g_1, \ldots, g_t \rangle}$ are equal.

Exercise. Prove that the ideals $\langle x^3 - y^2, x - y \rangle$ and $\langle x^3 - y^2, x - y^3 \rangle$ are not equal in $K[x, y]$.

VI. PERSPECTIVES: HISTORICAL AND OTHERWISE

From this discussion, one might be tempted to think that algebra preceded geometry historically. This is, of course, not the case, at least in western mathematics. The ancients were geometers, describing their objects of study in terms of points and distances.

It was only later, due to the influence of the Arabic and other “eastern” cultures, that Descartes devised Cartesian geometry. This is the system which allows us to describe the geometric objects studied by the Greeks (conic sections, surfaces, etc.) as solutions to equations or systems of equations. (The term “algebra” actually comes from the Arabic word “Al-jabr” meaning “the reduction”.) A similar relationship is held by number theory and algebra.

These subjects are now so interwoven that it is hard to separate them. The algebraist uses geometric and number theoretic methods and intuition to prove algebraic results. The geometer borrows from the algebraists and the number theorists (as well as from the physicists) to understand geometry. And so on.

Introductory References.

Cox, Little and O'Shea, *Ideals, Varieties, and Algorithms.*

Reid, M., *Undergraduate Algebraic Geometry.*

Advanced References.

Atiyah and MacDonald, *Introduction to Commutative Algebra.*

Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry.*

Hartshorne, R., *Algebraic Geometry.*

Matsumura, H., *Commutative Ring Theory.*

Shafarevich, I., *Basic Algebraic Geometry.*