Ideals and Varieties

Thang Pang Ern

Briefly speaking, linear algebra studies solutions to systems of linear equations; algebraic geometry studies solutions of polynomial equations. If you are interested in algebraic geometry after reading this, I strongly recommend the book *Beginning in Algebraic Geometry* by Emily Clader and Dustin Ross.

In this article, we fix a field k (take for example the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$). It is interesting that the notation k to denote a field actually comes from the German word körper. A linear subspace $W \subseteq k^n$ can be described in two equivalent ways. Geometrically, it is a subset closed under addition and scalar multiplication; algebraically, it is the common zero set of a collection of linear functionals, which is written as follows:

$$W = \{\mathbf{x} \in k^n : \ell_1(\mathbf{x}) = \cdots = \ell_m(\mathbf{x}) = 0\}$$

Let[1]

$$W^\perp = \{\ell \in (k^n)^* : \ell(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in W\} \quad \text{denote the orthogonal complement of } W.$$

Then,

$$W = \left\{\mathbf{x} : \ell(\mathbf{x}) = 0 \text{ for all } \ell \in W^\perp\right\}.$$

This duality between subspaces and linear equations is the prototype of algebraic geometry. As an example to the above, let $k = \mathbb{R}$ denote the field of real numbers and we consider the linear subspace

$$W = \left\{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0\right\}.$$

Geometrically. W is a two-dimensional plane through the origin in $\mathbb{R}^3$. It is closed under addition and scalar multiplication so it is a subspace of $\mathbb{R}^3$. Define the linear functional

$$\ell : \mathbb{R}^3 \to \mathbb{R} \quad \text{where} \quad (x, y, z) \mapsto x + y + z.$$

The collection of linear functionals consists of a single functional ℓ. So, $W = \{\mathbf{x} \in \mathbb{R}^3 : x + y + z = 0\}$. We then compute the orthogonal complement $W^\perp$, which is

$$W^\perp = \left\{\phi \in (\mathbb{R}^3)^* : \phi(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in W\right\}.$$

Note that ϕ denotes the set of linear transformations from $\mathbb{R}^3$ to $\mathbb{R}$, which is of the form $\phi(x, y, z) = ax + by + cz$, where $a, b, c \in \mathbb{R}$. The condition $\phi \in W^\perp$ means that we are finding all ϕ such that $x + y + z = 0$. We choose two linearly independent vectors $(1, -1, 0)$ and $(1, 0, -1)$ in W to obtain $a - b = 0$ and $a - c = 0$, so $a = b = c$. As such, $W^\perp = \text{span}\{(1, 1, 1)\}$.

We can replace linear functions by polynomials. For any field k, let $k[x_1, \ldots, x_n]$ denote the ring of polynomial functions on k^n (will be covered in MA3201 Algebra II). A polynomial $f(x_1, \ldots, x_n)$ is a non-linear analogue of a linear function. Instead of hyperplanes (think of this intuitively as planes in $\mathbb{R}^4, \mathbb{R}^5, \ldots$ as an extension of planes in $\mathbb{R}^3$ when studying systems of linear equations), we get what is known as algebraic varieties. These are

$$V(f) = \{\mathbf{x} \in k^n : f(\mathbf{x}) = 0\}.$$

[1] For any vector space V over a field k, recall that the dual space V^* is defined to be $\text{Hom}_k(V, k)$, the set of homomorphisms from V to k over k. In this context, $(k^n)^*$ denotes the set of linear transformations $k^n \to k$.

More generally, for a set of polynomials $S \subseteq k[x_1, \ldots, x_n]$, define

$$V(S) = \{\mathbf{x} \in k^n : f(\mathbf{x}) = 0 \text{ for all } f \in S\}.$$

These sets are the basic objects of algebraic geometry. For example, let

$$f(x, y, z) = x^2 + y^2 + z^2 - 1 \in k[x, y, z].$$

Then,

$$V(f) = \left\{(x, y, z) \in k^3 : x^2 + y^2 + z^2 = 1\right\}.$$

If $k = \mathbb{R}$, then $V(f)$ denotes the unit sphere in $\mathbb{R}^3$.

When we write down several polynomial equations at once, it is convenient to package them into an algebraic object. This is where the notion of an *ideal* is useful. An ideal $I \subseteq k[x_1, \ldots, x_n]$ is a subset satisfying the following conditions:

(i) If $f, g \in I$, then $f + g \in I$.

(ii) If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$.

Condition **(ii)** is the key difference between an ideal and a vector subspace: for a vector subspace $W \subseteq V$, we only require closure under scalar multiplication in k, whereas for an ideal, we require closure under multiplication by any polynomial.

Given a set of polynomials $S \subseteq k[x_1, \ldots, x_n]$, the ideal generated by S is

$$\langle S \rangle = \left\{\sum_{i=1}^{m} h_i f_i : m \geq 1, f_i \in S, h_i \in k[x_1, \ldots, x_n]\right\}.$$

For example, the ideal $\langle x, y \rangle \subseteq k[x, y]$ consists of all polynomials with zero constant term or equivalently, those polynomials that vanish at $(0, 0)$. To see why,

$$\langle x, y \rangle = \{h_1 x + h_2 y : m \geq 1, h_i \in k[x, y]\} = \left\{\sum_{i=1}^{m} (a_i x + b_i y) : m \geq 1, a_i, b_i \in k[x, y]\right\}.$$

Conversely, if we start with a subset $X \subseteq k^n$, we may consider all polynomials that vanish on X. For any $X \subseteq k^n$, define the vanishing ideal

$$I(X) = \{f \in k[x_1, \ldots, x_n] : f(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in X\}.$$

It is easy to check that $I(X)$ is an ideal because sums of polynomials that vanish on X still vanish on X, and multiplying by any polynomial still gives a polynomial that vanishes on X. Similarly, given an ideal $I \subseteq k[x_1, \ldots, x_n]$, we define its zero set to be

$$V(I) = \{\mathbf{x} \in k^n : f(\mathbf{x}) = 0 \text{ for all } f \in I\}.$$

This generalises the earlier definition $V(S)$, because $V(S) = V(\langle S \rangle)$.

For example, we can consider a parabola as a variety. Let $k = \mathbb{R}$ and consider the polynomial $f(x, y) = y - x^2 \in \mathbb{R}[x, y]$. Then,

$$V(f) = \left\{(x, y) \in \mathbb{R}^2 : y = x^2\right\}$$

which is the usual parabola. The ideal generated by f is $\langle y - x^2 \rangle$, and $V(\langle y - x^2 \rangle) = V(f)$. If we take $X = V(f)$ and form $I(X)$, then certainly $y - x^2 \in I(X)$. In fact, over an algebraically closed field k such as the set of complex numbers[2] $\mathbb{C}$, one can say that $I(V(I))$ is the *radical* of I, denoted by $\sqrt{I}$. This nice correspondence is known as *Hilbert's Nullstellensatz* (German for 'theorem of zeros' or 'zero locus theorem), which was proven by David Hilbert in 1893 and it became a foundational result in algebraic geometry. We will discuss the nullstellensatz shortly.

At this juncture, one should observe that the maps $X \mapsto I(X)$ and $I \mapsto V(I)$ reverse inclusions. That is to say,

(i) If $X \subseteq Y$, then $I(Y) \subseteq I(X)$

(ii) If $I \subseteq J$, then $V(J) \subseteq V(I)$

These results should be intuitive — if $X \subseteq Y$, then $I(Y) \subseteq I(X)$ means that more points implies more vanishing conditions. To see why, take some $f \in I(Y)$. Then, $f \in k[x_1, \ldots, x_n]$ such that $f(\mathbf{x}) = 0$ for all $\mathbf{x} \in Y$. Since this holds for all $\mathbf{x} \in Y$, then it must hold for all $\mathbf{x} \in X$ since $X \subseteq Y$, so $f \in k[x_1, \ldots, x_n]$ such that $f(\mathbf{x})$ for all $\mathbf{x} \in X$. This shows that the reverse inclusion holds for ideals. As for varieties, having more equations implies fewer solutions. To see why, take $\mathbf{x} \in V(J)$. Then, $\mathbf{x} \in k^n$ such that $f(\mathbf{x}) = 0$ for all $f \in J$. Again, this holds for all $f \in I$, so the result follows.

We now formalise the notion of a radical ideal, which appeared implicitly in the discussion above. We say that an ideal $I \subseteq k[x_1, \ldots, x_n]$ is radical if whenever $f^m \in I$ for some $m \in \mathbb{Z}^+$, we already have $f \in I$. Equivalently, we define the radical of an ideal to be

$$\sqrt{I} = \left\{ f \in k[x_1, \ldots, x_n] : f^m \in I \text{ for some } m \in \mathbb{Z}^+ \right\}.$$

Geometrically, taking radicals corresponds to ignoring multiplicities of solutions. For example, the ideals $\langle x \rangle$ and $\langle x^2 \rangle$ define the same zero set in k (which is $\{0\}$) even though algebraically they are different ideals.

We now state one of the central theorems in algebraic geometry, known as the weak form of Hilbert's nullstellensatz. It states that if k is an algebraically closed field and $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, then

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

This is what the weak nullstellensatz means in words. Say we start with an ideal I, pass it to its zero set $V(I)$, and then take all polynomials that vanish on this zero set. Then, we recover the radical of I. This theorem explains why radicals are exactly the ideals that arise as vanishing ideals of algebraic sets.

We now revisit the parabola example to see this theorem in action. Consider $I = \langle y - x^2 \rangle \subseteq \mathbb{C}[x, y]$. The variety $V(I)$ consists of all points $(x, y) \in \mathbb{C}^2$ such that $y = x^2$. If a polynomial $g(x, y)$ vanishes on all such points, then the nullstellensatz guarantees that $g \in \sqrt{\langle y - x^2 \rangle}$. Since $\langle y - x^2 \rangle$ is already radical, we conclude that $I(V(I)) = \langle y - x^2 \rangle$. More explicitly,

$$I(V(I)) = \{ f \in \mathbb{C}[x, y] : f(x, y) = 0 \text{ for all } x, y \in V(I) \}$$

which is equal to $\langle y - x^2 \rangle$. Thus, the parabola is encoded algebraically by a single irreducible polynomial.

This example highlights an important principle: algebraic geometry studies *geometric objects via their coordinate rings.* To every variety $X \subseteq k^n$, we associate the quotient ring

$$k[X] = k[x_1, \ldots, x_n] / I(X)$$

[2] $\mathbb{C}$ is the most common example of an algebraically closed field. Another example is $\overline{\mathbb{F}_p}$, the algebraic closure of the finite field of p elements, which can be regarded as the union of $\mathbb{F}_{p^n}$.

called the coordinate ring of X. Geometric properties of X are reflected in algebraic properties of $k[X]$. The correspondence between ideals and varieties provides a powerful dictionary translating geometry into algebra and vice versa. The nullstellensatz formalises this relationship and justifies why algebraic geometry can be studied through commutative algebra.