Algebraic Geometry

Rick Miranda
Colorado State University

I. Basic Definitions of Affine Geometry

II. Projective Geometry

III. Curves and Surfaces

IV. Applications

Glossary

Affine Space The space of n-tuples with coordinates in a field K.

Algebraic Set The set of solutions to a collection of polynomial equations in affine or projective space.

Coordinate Ring Ring of polynomial functions on an algebraic set.

Projective Space The space of $(n+1)$-tuples with coordinates in a field K, not all zero, up to scalar factor. The natural compactification of affine space, which includes points at infinity.

Rational Function A ratio of polynomial functions defined on an algebraic set in affine or projective space.

Regular Function A rational function whose denominator does not vanish at a subset of an algebraic set.

Curve An algebraic variety of dimension one.

Quadric An algebraic variety defined by a single quadratic equation.

Genus The fundamental invariant of curves, equal to the dimension of the space of regular 1-forms.

Moduli Space A topological space (usually an algebraic variety itself) whose points represent algebraic varieties of a specific type.

Algebraic Geometry is, broadly speaking, the study of the solutions of polynomial equations. Since polynomials are ubiquitous in mathematics, algebraic geometry has played a rather central role in the development and study of many mathematical ideas. Its origins can be traced to ancient Greek mathematics, when the study of lines and conics in the plane began. From these relatively simple beginnings, modern algebraic geometry has grown into a subject which draws on and informs nearly every other discipline in mathematics, and modern practitioners develop and use some of the most sophisticated 'mathematical machinery' (including sheaves, cohomology, etc.) available. However, the subject is still rooted in fundamental questions about systems of polynomial equations; the complexity and apparent abstraction of some of the modern tools of practicing algebraic geometers should not be confused with a lack of concern for basic and accessible problems.

I Basic Definitions of Affine Geometry

I.A Affine Space

To be more precise about solutions to polynomial equations, one first specifies a field k of numbers where the coefficients of the polynomials lie, and where one looks for solutions. A field is a set with two binary operations (addition and multiplication) in which all of the usual rules of arithmetic hold, including subtraction and division (by non-zero numbers). The main examples of interest are the field $\mathbb{Q}$ of rational numbers, the field $\mathbb{R}$ of real numbers, and the field $\mathbb{C}$ of complex numbers. Another is the finite field $\mathbb{Z}/p$ of the integers $\{0, 1, \ldots, p-1\}$ under addition and multiplication modulo a prime p.

Solutions to polynomials in n variables would naturally be n-tuples of elements of the field. If we denote the field in question by K, the natural place to find solutions is *affine n-space over K*, denoted by K^n, $\mathbb{A}^n_K$, or simply $\mathbb{A}^n$:

$$\mathbb{A}^n = \{\underline{\mathbf{z}} = (z_1, z_2, \ldots, z_n) \ \mid \ z_i \in K\}.$$

When $n = 1$ we have the affine line, if $n = 2$ we have the affine plane, etc.

I.B Affine Algebraic Sets

Let $f(\underline{\mathbf{x}}) = f(x_1, \ldots, x_n)$ be a polynomial in n variables with coefficients in K. The zeroes of f are denoted by $Z(f)$:

$$Z(f) = \{\underline{\mathbf{z}} \in \mathbb{A}^n \ \mid \ f(\underline{\mathbf{z}}) = 0\}.$$

For example, $Z(y - x^2)$ is a parabola in the plane, and $Z(x^2 - y^2 - z^2 - 4)$ is a hyperboloid in 3-space.

More complicated geometric objects in affine space must be defined by more than one polynomial. Let $\mathcal{S}$ be a set of polynomials (not necessarily finite) all having coefficients in the field K. The common zeroes of all of the polynomials in the set $\mathcal{S}$ is denoted by $Z(\mathcal{S})$:

$$Z(\mathcal{S}) = \{\underline{\mathbf{z}} \in \mathbb{A}^n \ \mid \ f(\underline{\mathbf{z}}) = 0 \text{ for all } f \in \mathcal{S}\}.$$

An *algebraic set* in $\mathbb{A}^n$, or simply an affine algebraic set, is a subset of $\mathbb{A}^n$ of the form $Z(\mathcal{S})$ for some set of polynomials $\mathcal{S}$ in n variables. That is, an affine algebraic set is a set which is exactly the set of common zeroes of a collection of polynomials. Affine algebraic sets are the fundamental objects of study in affine algebraic geometry.

The empty set is an affine algebraic set (it is $Z(1)$) and so is all of affine space (it is $Z(0)$). The intersection of an arbitrary collection of algebraic sets is an algebraic set. The union of a finite number of algebraic sets is also an algebraic set. Therefore the algebraic sets in affine space form the closed sets in a topology; this topology is called the *Zariski topology.*

I.C Ideals Defining Algebraic Sets

The "algebraic" part of algebraic geometry involves the use of the tools of modern algebra to study algebraic sets. Algebra is the study of sets with operations on them, and the most common algebraic structure is the *ring*, which is a set with addition and multiplication, but not necessarily division. The ring of importance in affine algebraic geometry is the ring $K[\underline{\mathbf{x}}] = K[x_1, x_2, \dots, x_n]$ of polynomials in the n variables $\underline{\mathbf{x}} = (x_1, \dots, x_n)$. Sometimes this is called the "affine coordinate ring", since it is generated by the coordinate functions x_i. It is from this ring that we draw the subset $\mathcal{S} \subset K[\underline{\mathbf{x}}]$ of polynomials whose zeroes we want to study.

An *ideal* J in a ring R (like $K[\underline{\mathbf{x}}]$) is a subset of the ring R with the special properties that it is closed under addition and 'outside multiplication': if f and g are in J then $f+g$ is in J, and if g is in J then fg is in J for any f in the ring. An example of an ideal is the collection of all polynomials that vanish at a particular point $p \in \mathbb{A}^n$.

If $\mathcal{S}$ is a subset of the ring, the *ideal generated by* $\mathcal{S}$ is the set of all finite "linear combinations" $\sum_i h_i f_i$ where the h_i's are in the ring and the f_i's are in the given subset $\mathcal{S}$. The reader may check that this set, denoted by $\langle \mathcal{S} \rangle$, is closed under addition and outside multiplication, and so is always an ideal.

Returning to the setting of algebraic sets, it is an easy exercise to see that if $\mathcal{S}$ is any collection of polynomials in $K[\underline{\mathbf{x}}]$, and $J = \langle \mathcal{S} \rangle$ is the ideal in $K[\underline{\mathbf{x}}]$ generated by $\mathcal{S}$, then $\mathcal{S} \subset J$ and $Z(\mathcal{S}) = Z(J)$: the set $\mathcal{S}$ and the ideal J have exactly the same set of common zeroes. This allows algebraic geometers to focus only on the zeroes of ideals of polynomials: every algebraic set is of the form $Z(J)$ for an *ideal* $J \subset K[\underline{\mathbf{x}}]$. It is *not* the case that the ideal defining the algebraic set is unique however: it is possible that two different ideals J_1 and J_2 have the same set of common zeroes, so that $Z(J_1) = Z(J_2)$.

I.D Algebraic Sets Defining Ideals

We saw in the last paragraph that ideals may be used to define all algebraic sets, but that the defining ideal is not unique. In the construction of algebraic sets, we look at a collection of polynomials and take their common zeroes, which is a set of points in $\mathbb{A}^n$. Now we turn this around, and look instead at a subset $X \subset \mathbb{A}^n_K$ of points in affine space, and consider all of the polynomials that vanish on X. We denote this by $I(X)$:

$$I(X) = \{f \in K[\underline{\mathbf{x}}] \mid f(\underline{\mathbf{z}}) = 0 \text{ for all } \underline{\mathbf{z}} \in X\}.$$

No matter what kind of subset X we start with, this is always an ideal of polynomials. Again there is the same possibility of non-uniqueness: it may be that two different subsets X and Y of $\mathbb{A}^n$ have the same ideal, so that $I(X) = I(Y)$. This would happen if every polynomial that vanished on X also vanished on Y and vice-versa.

The ideal $I(X)$ for a subset $X \subset \mathbb{A}^n$ has a special property not shared by all ideals: it is closed under roots. That is, if f is a polynomial, and f^m vanishes on all of the points of X, then it must be the case that f itself vanishes. This means that if $f^m \in I(X)$, then $f \in I(X)$. An ideal with this special property is called a *radical* ideal.

I.E The Z-I Correspondence

These two operations, of taking an ideal of polynomials and using Z to get a subset of affine space, and taking a subset of affine space and using I to get an ideal of polynomials, form the theoretical foundation of affine algebraic geometry. We have the following basic facts:

- If $J_1 \subset J_2 \subset K[\underline{\mathbf{x}}]$ are ideals, then $Z(J_1) \supset Z(J_2)$.
- If $X_1 \subset X_2 \subset \mathbb{A}^n$, then $I(X_1) \supset I(X_2)$.
- If $J \subset K[\underline{\mathbf{x}}]$ is an ideal, then $I(Z(J)) \supset J$.
- If $X \subset \mathbb{A}^n$, then $Z(I(X)) \supset X$.

This last statement can be sharpened to give a criterion for when a subset of $\mathbb{A}^n$ is algebraic, as follows. If X is algebraic, equal to $Z(J)$ for some ideal J, then $I(X) = I(Z(J)) \supset J$, so that $Z(I(X)) = Z(I(Z(J)) \subset Z(J) = X$, forcing $Z(I(X)) = X$. Conversely if $Z(I(X)) = X$, then X is obviously algebraic. Hence

$$X \text{ is an algebraic subset of } \mathbb{A}^n \text{ if and only if } Z(I(X)) = X.$$

This statement addresses the question of which points are additional zeroes of all of the polynomials which vanish on X, stating that if X is algebraic there are no additional such points.

I.F The Nullstellensatz and the Basis Theorem

The Nullstellensatz turns the previous question around, and asks which additional polynomials always vanish at the points which are common zeroes of a given ideal of polynomials. This is a much more subtle question, and the answer is the fundamental theorem in elementary affine geometry. It uses the concept of the *radical* $\mathrm{rad}(J)$ of an ideal J, which is the set of all polynomials for which some power is in J:

$$\mathrm{rad}(J) = \{f \in K[\underline{\mathbf{x}}] \mid f^m \in J \text{ for some } m \geq 1\}.$$

It is always the case that $\mathrm{rad}(J) \supset J$, and that $\mathrm{rad}(J)$ is a radical ideal. Clearly $I(Z(J)) \supset \mathrm{rad}(J)$: if $f^m \in J$, then f will certainly vanish wherever everything in J (in particular wherever f^m) vanishes.

An *algebraically closed* field is a field that contains all roots of all polynomials in one variable. The field $\mathbb{C}$ of complex numbers is algebraically closed; the field $\mathbb{Q}$ of rational numbers, the field $\mathbb{R}$ of real numbers, and all finite fields, are not algebraically closed.

Theorem 1 (Hilbert's Nullstellensatz). *If K is an algebraically closed field, then for any ideal $J \subset K[\underline{\mathbf{x}}]$, $I(Z(J)) = \mathrm{rad}(J)$.*

The power of the Nullstellensatz occurs because in many applications one has access to a polynomial f which is known to be zero when other polynomials $g_1, \ldots, g_k$ are. The conclusion is then that f is in the radical of the ideal generated by the g_i's. Therefore there is a power of f which is a linear combination of the g_i's, and so there is an explicit equation of the form

$$f^m = \sum_i h_i g_i.$$

The Nullstellensatz permits a more detailed correspondence of properties between the algebraic set X and its ideal $I(X)$. Typical statements when K is algebraically closed are:

- There is a 1-1 correspondence between algebraic subsets of $\mathbb{A}^n$ and radical ideals in $K[\underline{\mathbf{x}}]$.
- X is empty if and only if $I(X) = K[\underline{\mathbf{x}}]$.
- $X = \mathbb{A}^n$ if and only if $I(X) = \{0\}$.
- X consists of a single point if and only if $I(X)$ is a maximal ideal.
- X is an irreducible algebraic set (that is, is not a union of two proper algebraic subsets) if and only if $I(X)$ is a prime ideal (that is, $I(X)$ has the property that if $fg \in I(X)$ then either $f \in I(X)$ or $g \in I(X)$).

All of these statements relate geometric properties of the algebraic set X to algebraic properties of the ideal $I(X)$. This is basic theme of algebraic geometry in general.

The other main theorem concerning these general ideas is the Basis Theorem, which addresses the question of the finiteness of the set of equations which may define an algebraic set:

Theorem 2 (Hilbert's Basis Theorem). *Every ideal J in the ring of polynomials $K[\underline{\mathbf{x}}]$ is finitely generated: there is a finite set $\mathcal{S}$ of polynomials such that $J = \langle \mathcal{S} \rangle$. As a consequence, every algebraic set $X \subset \mathbb{A}^n$ may be defined as the set of common zeroes of a finite set of polynomials.*

I.G Regular and Rational Functions

Any polynomial $f \in K[\underline{\mathbf{x}}]$ can be considered as a K-valued function on affine space $\mathbb{A}^n$. If $X \subset \mathbb{A}^n$ is an algebraic set, such a polynomial may be restricted to X to obtain a function on X. Functions on X which are restrictions of polynomial functions are called *polynomial* functions. The polynomial functions on X form a ring, denoted by $K[X]$, and called the *affine coordinate ring of X*. For example, the affine coordinate ring of affine space is the entire polynomial ring: $K[\mathbb{A}^n] = K[\underline{\mathbf{x}}]$.

There is an onto ring homomorphism (restriction) from $K[\underline{\mathbf{x}}]$ to $K[X]$, whose kernel is the ideal $I(X)$; therefore $K[X]$ is isomorphic as a ring to the quotient ring $K[\underline{\mathbf{x}}]/I(X)$.

Irreducible algebraic sets are often referred to as *algebraic varieties*. If X is an algebraic variety, then $I(X)$ is a prime ideal, so that the coordinate ring $K[X]$ is an integral domain (if $fg = 0$ then either $f = 0$ or $g = 0$). The field of fractions of $K[X]$, denoted by $K(X)$, represent *rational functions* on the variety X. Rational functions are more useful than polynomial functions of course, but they have the drawback that any given rational function may not be defined on all of X (where the denominator vanishes). If a rational function is defined at a point p, one says that the function is *regular* at p.

The rational function field $K(X)$ of an algebraic variety X is an extension field of the base field K, and as such has a transcendence degree over K: this is the largest number of algebraically independent rational functions. This transcendence degree is the *dimension* of the variety X. Points have dimension zero, Curves have dimension one, surfaces have dimension two, etc.

Polynomial and rational functions are used to define maps between algebraic sets. In particular, maps between two affine spaces are simply given by a vector of functions. Maps between affine algebraic sets are given by restriction of such a vector of functions. Depending on the type of functions used, such maps are called polynomial or rational maps. Again, rational maps have the property that they may not be defined everywhere. A map is called *regular* if it is given by rational functions but is defined everywhere.

I.H Examples

The most common example of an affine algebraic variety is an *affine subspace*: this is an algebraic set given by *linear* equations. Such a set can always be defined by an $m \times n$ matrix A, and an m-vector $\underline{\mathbf{b}}$, as the vanishing of the set of m equations given in matrix form by $A\underline{\mathbf{x}} = \underline{\mathbf{b}}$. This gives the geometric viewpoint on linear algebra of course. One consequence of the geometric point of view is a deeper understanding of parallelism for linear spaces: geometrically, one begins to believe that parallel lines might be made to intersect "at infinity". This is the germ of the development of *projective geometry.*

No doubt the first nonlinear algebraic sets to be studied were the *conics*. These are the algebraic sets given by a single quadratic equation in two variables, and define a curve in the affine plane. The classification and study of conics go back to antiquity of course. Most familiar is the classification of nonempty irreducible conics over the real numbers $\mathbb{R}$: we have either an ellipse, a parabola, or an hyperbola. Again an appreciation of the points "at infinity" sheds light on this classification: an ellipse has no real points at infinity, a parabola has one real point at infinity, and an hyperbola has two real points at infinity.

Over any field, if an irreducible conic C (given by $f(x, y) = 0$) is non-empty, then it may be *parametrized* using a rational function of one variable. This is done by choosing a point $p = (x_0, y_0)$ on C, writing the line L_t through p with slope t, (given by $y - y_0 = t(x - x_0)$) and intersecting L_t with C. This intersection will consist of the point p of course, and one other point p_t which depends on t. One may solve easily for the coordinates of p_t as rational functions of t, giving a rational parametrization for the conic C. From the point of view of maps, this gives a rational map $\phi : \mathbb{A}^1 \to C$ which has an inverse: for any point (x, y) on C, the t-value is $t = (y - y_0)/(x - x_0)$. Invertible rational maps are called *birational*, and most of the classification efforts of algebraic geometry are classifications up to birational maps.

Applying this procedure to the unit circle C (defined by $x^2 + y^2 = 1$) and choosing the point p to be the point $(-1, 0)$, one finds the parametrization

$$p_t = (\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}).$$

We see here the origins of algebraic number theory, in particular the formulas for the Pythagorean triples. If we look at the case when $t = p/q$ is a rational number, we find (clearing the denominator q) that $(\frac{q^2-p^2}{q^2+p^2}, \frac{2pq}{q^2+p^2})$ is a point on the unit circle. Again clearing the denominator $q^2 + p^2$, we see that this means

$$(q^2 - p^2)^2 + (2pq)^2 = (q^2 + p^2)^2$$

giving the standard paramatrization of Pythagorean triples. This style of argument in elementary number theory goes back to the ancient Greeks, in particular to Appollonius and Diophantus.

In higher dimensions, an algebraic variety given by a single quadratic equation is called a *quadric*. Although the classification of affine quadrics is not difficult, it becomes clearer that the use of projective techniques simplifies the matter considerably.

Algebraic varieties defined by either more equations, or equations of degree larger than two, present a much greater challenge. Even the study of cubic curves in the plane (given by a single equation $f(x, y) = 0$ where f has degree three) is still a subject of modern research, especially over number fields.

I.I Affine Schemes

The theory exposed above was developed in the hundred years ending in the middle of the twentieth century. In the second half of the twentieth century a different foundation to algebraic geometry was developed, which more closely follows the algebra of the rings and ideals in question. Recall that there is a correspondence between algebraic subsets of affine space and radical ideals in the polynomial ring $K[\underline{\mathbf{x}}]$. If the ground field K is algebraically closed, points correspond to maximal ideals, and irreducible algebraic sets to prime ideals. The ring of polynomial functions on X is naturally the ring $K[\underline{\mathbf{x}}]/I(X)$. This ring is a finitely generated K-algebra, with no nilpotent elements (elements $f \neq 0$ such that $f^k = 0$ for some k). From this ring one can recover X, as the set of maximal ideals.

The idea of affine schemes is to start with an arbitrary ring R, and to construct a geometric object X having R as its natural ring of functions. Grothendieck's theory, developed in the 1950's and 60's, uses $\mathrm{Spec}(R)$, the set of prime ideals of R, as the set X. This gives the notion of an *affine scheme*.

II Projective Geometry

II.A Infinity

Consider the affine line $\mathbb{A}^1$, which is simply the ground field K as a set. What should it mean to approach infinity in $\mathbb{A}^1$? Consider a ratio $x/y \in K$; if $y \neq 0$ this is an element of K, but as y approaches 0 for fixed x, this element will "approach infinity". However we cannot let y equal zero in this ratio, since one cannot divide by zero in a field. It makes sense then to separate the numerator and denominator in this ratio, and consider the ordered pair: let us write $[y : x]$ for this. Since we are thinking of this ordered pair as representing a ratio, we should have that $[y : x] = [ay : ax]$ for any nonzero $a \in K$. The ordered pair $[1 : x]$ will represent the number $x \in K$; the ordered pair $[0 : 1]$ will represent a new point, at infinity. We remove the ordered pair $[0 : 0]$ from the discussion, since this would represent an undefined ratio.

II.B Projective Space

The construction above generalizes to n-dimensional affine space $\mathbb{A}^n$, as follows. Define *projective space* $\mathbb{P}^n$ to be the set of all ordered $(n+1)$-tuples $[x_0 : x_1 : \ldots : x_n]$, with each $x_i \in K$, not all equal to zero, subject to the equivalence relation that

$$[x_0 : x_1 : \ldots : x_n] = [\lambda x_0 : \lambda x_1 : \ldots : \lambda x_n]$$

for any nonzero $\lambda \in K$. The x_i's are called the *homogeneous coordinates* of the point $[\underline{\mathbf{x}}]$; note that they are not individually well-defined, because of the scaling condition. However it does make sense to say whether $x_i = 0$ or not.

If $x_0 \neq 0$, we can scale by $\lambda = 1/x_0$ and assume $x_0 = 1$; then all the other n coordinates are well-defined, and correspond to a unique point in affine n-space $\mathbb{A}^n$:

$$p = (x_1, \ldots, x_n) \in \mathbb{A}^n \text{ corresponds to } [1 : x_1 : \ldots : x_n] \in \mathbb{P}^n.$$

However we have a host of new points where $x_0 = 0$ in $\mathbb{P}^n$; these are to be thought of as points "at infinity" of $\mathbb{A}^n$. In this way the points at infinity are brought in to view and in fact become no different than any other point, in projective space.

II.C Projective Algebraic Sets

Let $K[\underline{\mathbf{x}}] = K[x_0, x_1, \ldots, x_n]$ be the polynomial ring generated by the homogeneous coordinates. We can no longer view these polynomials as functions, since (because of the scaling issue) even the coordinates themselves do not have well-defined values. However suppose that a polynomial $F(\underline{\mathbf{x}})$ is *homogeneous*, that is, every term of F has the same degree d. Then $F(\lambda\underline{\mathbf{x}}) = \lambda^d F(\underline{\mathbf{x}})$ for any nonzero λ, and hence whether $F = 0$ or not at a point $[\underline{\mathbf{x}}] \in \mathbb{P}^n$ is well-defined.

We therefore define a *projective algebraic set* to be the set of common zeroes of a collection $\mathcal{S}$ of homogeneous polynomials:

$$Z(\mathcal{S}) = \{[\underline{\mathbf{x}}] \in \mathbb{P}^n \mid F(\underline{\mathbf{x}}) = 0 \text{ for all } F \in \mathcal{S}\}.$$

Correspondingly, given a subset $X \subset \mathbb{P}^n$, we define the *homogeneous ideal* $I(X)$ of X to be the ideal in $K[\underline{\mathbf{x}}]$ generated by all homogeneous polynomials F which vanish at all points of X:

$$I(X) = \langle \{ \text{ homogeneous } F \in K[\underline{\mathbf{x}}] \mid F|_X = 0\} \rangle.$$

The reader will see the possibility of developing exactly the same type of theory, complete with a Z-I correspondence, a Basis Theorem, and a projective version of the Nullstellensatz, all properly interpreted with the extra attention paid to the homogeneity conditions at every turn. This is in fact what happens, and projective geometry attains an algebraic foundation as solid as that of affine geometry.

II.D Regular and Rational Functions

In the context of projective geometry, the polynomial ring $K[\underline{\mathbf{x}}]$ is called the *homogeneous coordinate ring*. It is a *graded* ring, graded by degree: $K[\underline{\mathbf{x}}] = \oplus_{d \geq 0} V_d$ where V_d is the vector space of homogeneous polynomials in $\underline{\mathbf{x}}$ of degree exactly d. If $X \subset \mathbb{P}^n$ is a projective algebraic set, the homogeneous ideal $I(X)$ is also graded: $I(X) = \oplus_d I_d$, and the graded quotient ring $K[X] = K[\underline{\mathbf{x}}]/I(X)$ is called the *homogeneous coordinate ring* of X.

As we have noted above, a polynomial (even a homogeneous one) F does not have well-defined values at points of projective space. However a *ratio* of polynomials $r = F/G$ will have a well-defined value at a point p if both F and G are homogeneous of the *same* degree, and $G(p) \neq 0$. Such a ratio is called a "rational function of degree zero", and these form the foundation of the function theory on projective algebraic sets. A rational function whose denominator does not vanish at p is said to be *regular* at p.

II.E Homogenization

Suppose now that one has an affine algebraic set, given by the vanishing of a polynomial $f(x_1, \dots, x_n)$. We want to investigate how this algebraic set looks at infinity, in projective space. Let d be the largest degree of terms of f. To each term of f we multiply in the appopriate power of the new variable x_0 to make the term have degree exactly d. This produces a homogeneous polynomial $F(x_0, x_1, \dots, x_n)$, which for $x_0 = 1$ has the same zeroes as the original polynomial f. However now for $x_0 = 0$ we have new zeroes, at infinity, in projective space.

For a general affine algebraic set X defined by more than one equation, we do this process for every polynomial in $I(X)$, producing a collection of homogeneous polynomials $\mathcal{S}$. Then $Z(\mathcal{S}) \subset \mathbb{P}^n$ is the *projective closure* $\overline{X}$ of X, and exactly adds the minimal set of points at infinity to X to produce a projective algebraic set.

For example, consider the hyperbola in the affine plane defined by $f(x, y) = x^2 - y^2 - 1 = 0$. We homogenize this to $F(z, x, y) = x^2 - y^2 - z^2$, a homogeneous polynomial of degree two. For $z = 0$, we recover the two points $[0 : 1 : 1]$ and $[0 : 1 : -1]$ at infinity (where $x^2 - y^2 = 0$, up to scalar factors.

II.F Bezout's Theorem

One of the consequences of adding in the points at infinity to form projective space is that algebraic sets which did not intersect in affine space now tend to intersect, at infinity, in projective space. The classic example is that of two parallel lines in the affine plane: these intersect at one point at infinity in the projective plane.

In general, one expects that each time one adds a new equation that must vanish, the dimension of the set of zeroes goes down by one. Therefore, in projective space $\mathbb{P}^n$, which has dimension n, one expects that the projective algebraic set defined by exactly n homogeneous polynomials $F_1 = F_2 = \cdots = F_n = 0$ will have dimension zero; this means that it should be a finite set of points.

Bezout's Theorem deals with the number of such intersections. It may happen that a point of intersection is counted with multiplicity; this is the same phenomenon as when a polynomial in one variable has a double root: it counts for two when the number of roots is being enumerated. In more than one variable, there is a corresponding notion of multiplicity; this is always an integer at least one (for a common isolated root).

Theorem 3 (Bezout's Theorem). *Suppose the ground field K is algebraically closed. Let F_i, $i = 1, \ldots, n$ be homogeneous polynomials in the $n+1$ homogeneous variables of projective n-space $\mathbb{P}^n$. Suppose that F_i has degree d_i. Then:*

(a) The common zero locus $X = Z(\{F_1, \ldots, F_n\})$ is non-empty.

(b) If X is finite, the cardinality of X is at most the product of the degrees $d_1 d_2 \cdots d_n$.

(c) If each point of X is counted according to its multiplicity, the sum of the multiplicities is exactly the product of the degrees $d_1 d_2 \cdots d_n$.

For example, three quadrics (each of degree two) in $\mathbb{P}^3$ always intersect; if the intersection is finite, it is at most eight points; if the points are counted according to their multiplicity, the sum is exactly eight.

As another example, a line and a cubic in the plane will intersect three times, counted with multiplicity. This is the basis for the famous *group law* on a plane projective cubic curve X: given two points p and q on X, the line joining p and q will intersect the curve X in a third point, and this operation forms the basis for a group structure on X.

III Curves and Surfaces

III.A Singularities

Let X be an irreducible algebraic variety, of codimension r, in $\mathbb{A}^n$. If x_i are local affine variables at a point $p \in X$, and the ideal of X is generated near p by polynomials $f_1, \ldots, f_k$, then the Jacobian matrix $J = (\partial f_i / \partial x_j)$ will have rank at most r at every point of X, and will have maximal rank r at all points of X away from a sub-algebraic set $\mathrm{Sing}(X)$. At points of $X - \mathrm{Sing}(X)$, the variety is said to be *non-singular*, or *smooth*; at points of $\mathrm{Sing}(X)$, the variety is said to be *singular*, and $\mathrm{Sing}(X)$ is called the *singular locus* of X. Over the complex numbers, the non-singular points are those points of X where X is a complex *manifold*, locally analytically isomorphic to an open set in $\mathbb{C}^d$, where d is the dimension of X. A common situation is when $\mathrm{Sing}(X)$ is empty; then the variety is said to be *smooth*. At smooth points of algebraic varieties, there are local 'analytic' coordinates $y_1, \ldots, y_d$, equal in number to the dimension of the variety.

III.B 1-Forms

A 1-*form* on a smooth algebraic variety is a collection of local expressions of the form $\sum_i f_i(\underline{\mathbf{y}}) dy_i$, where $\{y_i\}$ are local coordinates on the variety, and the f_i's are rational functions; this collection of expressions must be all equal under changes of coordinates, and at every point of the variety at least one of the expressions must be valid. For a curve, where there is only one local coordinate y, a local 1-form expression has the simple form $f(y)dy$. The set of 1-forms on a variety form a vector space.

III.C The Genus of a Curve

Let X be a smooth projective curve. Let ω be a 1-form on X. If at every point of X, there is a local expression for ω of the form $f(y)dy$ where y is a local coordinate and f is a *regular* function, then we say that ω is a *regular* 1-form. The set of regular 1-forms on a smooth projective curve form a finite-dimensional vector space over K, and the number of linearly independent regular 1-forms, which is the dimension of this vector space, is the most important invariant of the curve, called the *genus*.

If K is the complex numbers, the genus has a topological interpretation also. A smooth projective curve is a compact complex manifold of dimension one, which is therefore a compact orientable real manifold of dimension two. As such, it is topologically homeomorphic to a sphere with g handles attached; this g is the *topological genus*, which is equal to the genus. If $g = 0$, the curve is topologically a sphere; if $g = 1$, the curve is topologically a torus; if $g \geq 2$, the curve is topologically a g-holed torus.

The simplest smooth projective curve is the projective line itself, $\mathbb{P}^1$. It has genus zero.

III.D Plane Curves and Plücker's Formula

The most common projective curves studied over the centuries are the plane curves, which are defined by a single irreducible polynomial $f(x, y) = 0$ in affine two-space, and then closed up with points at infinity to a projective curve defined by the homogenization $F(x, y, z) = 0$ in the projective plane. Plücker's Formula addresses the question of the genus of this curve in relation to the degree of the polynomial F:

Theorem 4 (Plücker's Formula). *Suppose X is a smooth projective plane curve defined by an irreducible polynomial $F(x, y, z)$ of degree d. Then the genus of X is equal to $(d-1)(d-2)/2$.*

Plücker's formula has been generalized to curves with singularities, in particular with simple singularities like nodes (locally like $xy = 0$ or $y^2 = x^2$) and cusps (locally like ($y^2 = x^3$). Then the formula gives the genus of the *desingularization* of the curve: if a plane projective curve of degree d has a finite number of singularities which are all either nodes or cusps, and there are ν nodes and κ cusps, then the genus of the desingularization is

$$g = \frac{(d-1)(d-2)}{2} - \nu - \kappa.$$

III.E Elliptic and Hyperelliptic Curves

Using Plücker's formula we see that smooth plane projective curves of degree 1 or 2 have genus zero. We have in fact seen above that conics may be parametrized by lines, and this is possible precisely because they have the same genus. Smooth projective plane cubic curves have genus one, and they cannot be parametrized by lines. Every smooth projective plane curve over $\mathbb{C}$ has exactly nine inflection points, and if an inflection point is put at the projective point $[0 : 1 : 0]$, and if the line of inflection is the line at infinity, the affine equation of the cubic curve can be brought into *Weierstrass form*

$$y^2 = x^3 + Ax + B$$

for complex numbers A and B, such that $4A^3+27B^2 \neq 0$ (this is the smoothness condition). The form of this equation shows that a cubic curve is also representable as a *double cover* of the x-line: for every x-value there are two y-values each giving points of the curve.

In general, there are curves of every genus representable as double covers, using similar affine equations of the form

$$y^2 = f_d(x)$$

where f_d is a polynomial with distinct roots of degree d. Such a curve is called *hyperelliptic*, and has genus $g = [(d-1)/2]$. In particular these constructions show the existence of curves of any genus $g \geq 0$.

Higher degree coverings of the projective line, such as a curve given by an equation of the form $y^3 = f(x)$, are also important in the classification of curves. Coverings of degree three are called *trigonal* curves; *tetragonal* curves are covers of degree four, etc.

III.F Rational Functions, Forms, and the Riemann-Roch Theorem

The most celebrated theorem in the theory of curves is the theorem of Riemann-Roch, which gives precise information about the rational functions on a smooth projective curve X. The space of rational functions $K(X)$ on X forms a field of transcendence degree one over K, and as such is an infinite-dimensional vector space over K. In order to organize these functions, we concentrate our attention on the zeroes (where the numerator vanishes) and the poles (where the denominator vanishes). Specifically, given a point $p \in X$ and a positive integer m, we may look at all those rational functions on X with either a zero at p, no zero or pole at p, or a pole at p of order at most m. We denote this space by $\mathcal{L}(mp)$. If $m = -n$ is a negative integer, we define $\mathcal{L}(mp) = \mathcal{L}(-np)$ to be the space of rational functions with a zero at p of order at least n.

A *divisor* on X is a function from the points of X to the group of integers $\mathbb{Z}$, such that all but finitely many values are zero. For any divisor D, we define the vector space $L(D)$ to be the space $L(D) = \cap_{x \in X} \mathcal{L}(D(x) \cdot x)$. In plain English this is the space of rational functions with restricted poles (to the set of points with positive D-values) and prescribed zeroes (as the set of points with negative D-values). Part of the Riemann-Roch theorem is that these spaces are finite-dimensional.

We can make the same construction with rational 1-forms also. Recall that a rational 1-form has local expression $f(y)dy$, and we use the function part f to define the zeroes and poles. Given a divisor E, we may then consider the space $\Omega^1(E)$ of rational 1-forms with restricted poles and prescribed zeroes as E indicates. Again, this is a finite-dimensional space of forms.

Theorem 5 (Riemann-Roch). *Let X be a smooth projective curve of genus g. Let D be a divisor on X, and denote by d the sum of the values of D: $d = \sum_x D(x)$. Then*

$$\dim(L(D)) = d + 1 - g + \dim(\Omega^1(-D)).$$

The inequality $\dim(L(D)) \geq d + 1 - g$ was proved by Riemann; Roch supplied the "correction term" related to 1-forms. One of the main uses of the Riemann-Roch Theorem is to guarantee the existence of rational functions with prescribed zeroes and poles, in order to intelligently *embed* the curve in projective space: given rational functions $f_0, \ldots, f_n$ on a curve X, the mapping sending $x \in X$ to the point $[f_0(x), f_1(x), \ldots, f_n(x)]$ will always be well-defined on all of X and under certain circumstances will embed X as a subvariety of $\mathbb{P}^n$.

Using this technique, it can be shown for example that all curves of genus zero are isomorphic to the projective line $\mathbb{P}^1$; all curves of genus one are isomorphic to smooth plane cubic curves; all curves of genus two are hyperelliptic, given by an equation of the form $y^2 = f_6(x)$, where f_6 is a sextic polynomial; all curves of genus three are either hyperelliptic or are smooth plane quartic curves; all curves of genus four are either hyperelliptic or are the intersection of a quadric surface and a cubic surface in $\mathbb{P}^3$; and all curves of genus five are either hyperelliptic, trigonal, or are the intersection of three quadric threefolds in $\mathbb{P}^4$. Of special interest is the so-called *canonical embedding* of a smooth curve, which shows that a curve of genus g is either hyperelliptic or can be embedded as a curve of degree $2g - 2$ in $\mathbb{P}^{g-1}$.

III.G The Moduli Space M_g

Much of the research in algebraic geometry since 1960 has focused on the study of the *moduli spaces* for algebraic varieties. Loosely speaking, a moduli space is a topological space M whose points represent particular geometric objects; the topology on M is such that points which are close in M represent geometric objects which are also "close" to each other. Of particular interest has been the moduli space $\mathcal{M}_g$ for smooth projective curves of genus g. For example, since every curve of genus zero is isomorphic to the projective line, $\mathcal{M}_0$ consists of a single point. The moduli space $\mathcal{M}_1$ classifying curves of genus one is isomorphic to the affine line $\mathbb{A}^1$: the famous j-invariant of elliptic curves classifies curves of genus one by a single number. (For a plane cubic curve of genus one in Weierstrass form $y^2 = x^3 + Ax + B$, $j = 4A^3/(4A^3 + 27B^2)$.) For $g \geq 2$, $\mathcal{M}_g$ is itself an algebraic variety of dimension $3g - 3$.

Of particular interest has been the construction and study of meaningful compactifications of various moduli spaces. For $\mathcal{M}_g$, the most natural compactification $\overline{\mathcal{M}_g}$ was constructed by Deligne and Mumford and the additional points represent *stable* curves of genus g, which are curves without continuous families of automorphisms, and having only nodes as singularities. Even today the construction and elementary properties of moduli spaces for higher-dimensional algebraic varieties (e.g. surfaces) is a challenge. More recently attention has turned to moduli spaces for maps between algebraic varieties, and it is an area of very active research today to compactify and understand such spaces of maps.

III.H Surfaces and Higher Dimensions

The construction and understanding of the moduli spaces $\mathcal{M}_g$ for smooth curves is tantamount to the successful classification of curves and their properties. The classification of higher-dimensional varieties is not anywhere near as complete. Even surfaces, for which a fairly satisfactory classification exists due to Enriques, Kodaira, and others, presents many open problems.

The Enriques classification of smooth surfaces essentially breaks up all surfaces into four categories. The first category consists of those surfaces with a family of genus zero curves on them. Since genus zero curves are all isomorphic to lines, such surfaces are known as *ruled surfaces*, and a detailed understanding of them is possible. The prototype is a product surface $X \times \mathbb{P}^1$ for a curve X. The second category consists of surfaces with a nowhere vanishing regular two-form, or finite quotients of such surfaces. These are the so-called abelian surfaces, $K3$ surfaces, Enriques surfaces, and hyperelliptic surfaces. The third category consists of surfaces with a family of genus one curves on them. Some techniques similar to those used in the study of ruled surfaces are possible, and since genus one curves are very well understood, again a rather detailed description of these surfaces, called *elliptic surfaces*, is available. The last category are the *surfaces of general type*, and "most" surfaces are in this category. Moduli spaces have been constructed, and many elementary invariants are known, but there is still a lot of work to do to understand general type surfaces. An exciting current application area has to do with the connection of algebraic surfaces (which over the complex numbers are real 4-dimensional objects) and the study and classification of 4-manifolds.

For varieties of dimension three or more, there are essentially no areas of complete classification. Basic techniques available for curves and surfaces begin to break down for threefolds, in particular because several fundamental constructions lead immediately to singular varieties, which are much more difficult to handle. However in the last twenty years, starting with the ground-breaking work of Mori, steady progress is being made on fundamental classification constructions.

IV Applications

The origins of algebraic geometry, and the development of projective geometry in the Renaissance, was driven in large part by applications (of the theory of multivariable polynomials) to a variety of problems in geography, art, number theory, etc. Later, in the 1800s, newer problems in differential equations, fluid flows, and the study of integrals were driving development in algebraic geometry. In the 1900s the invention of algebra as we know it today caused a rethinking in the foundations of algebraic geometry, and the energies of working researchers were somewhat siphoned into the development of new structures and techniques: these have culminated in the widespread use of general *schemes*, *sheaves*, and *homological algebra*, as well as slightly more general notions of *algebraic spaces* and *stacks*.

After this period of partial introspection, in the past twenty years algebraic geometry has enjoyed a vigorous return to application areas. We will close this article with brief discussions of a sampling of these.

IV.A Enumeration

One of the fundamental questions of geometry, and of many other subjects in mathematics, is the "how many" question: in algebraic geometry, this expresses itself in counting the number of geometric objects with a given property. In contrast to pure combinatorics, often the geometric approach involves counting objects with *multiplicity*, e.g., roots of a polynomial.

Typical enumerative questions (and answers) ask for: the number of flexes on a smooth cubic curve (9); the number of lines on a smooth cubic surface (27); the number of conics tangent to five given conics (3264); the number of lines on a smooth quintic threefold (2875).

Recent breakthrough developments in *intersection theory* have enabled algebraic geometers to compute such numbers of enumerative interest which have stumped prior generations. New excitement has been brought by totally unexpected relationships with string theory in theoretical physics, where work of Witten and others have found surprising connections between computations relating elementary particles and generating functions for enumerative problems of the above sort in algebraic geometry.

IV.B Computation

Computation with polynomials is a fundamentally algorithmic process which permits in many cases the design of explicit algorithms for calculating a multitude of quantities of interest to algebraic geometers. Usually these quantities are related to either enumerative questions such as those mentioned above, or are the dimensions of vector spaces (typically of functions or forms) arising naturally in either elementary settings or as cohomology spaces.

With the advent of sufficient computing power as represented by modern computers and computer algebra software packages, it has become more possible to actually perform these types of computation via computer. This has led to an explosion of activity in designing efficient and effective algorithms for the computations of interest. These algorithms usually rely in some way on the theory of *Gröbner Bases*, which build on a multivariable version of the division algorithm for polynomials.

Software is now widely available to execute many calculations, and they are typically user-customizable, which has enabled researchers around the world to make fundamental contributions. Softare packages which are widely used include Macaulay, CoCoA, and Schubert.

IV.C Mechanics

Many problems in mechanical engineering and construction involve the precise understanding of the position of various machine parts when the machine is in motion. Robotic analysis is especially concerned with the position and velocity of robot extremities given various parameters for joint motion and extension. There are a few basic motions for machine joints, and these are all describable by simple polynomials (e.g., circular motion of radius r occurs on the circle ($x^2 + y^2 = r^2$). It is not hard to see therefore that in suitable coordinate systems, virtually all such problems can be formulated by polynomial systems.

However mechanical devices with many joints can correspond to algebraic sets in affine spaces with many variables and many equations, making the geometric analysis rather complicated. It is therefore useful to be able to apply more sophisticated techniques of the theory to reduce the complexity of the problem, and here is where the power of algebraic geometry can come into play.

A specific example of the type of problem is the following so-called n-bar configuration. Take a cyclical arrangement of n stiff rods, joined at the ends by joints that can actuate only in a planar way locally. For what initial positions of this arrangement does the configuration actually move and flex? In how many different ways can it be made to flex? When $n = 3$, the configuration must lie in a plane, and no flexing or motion is possible; for $n = 4$ already the flexing configurations, although known, have not been completely analyzed.

IV.D Coding Theory

A *code* is a collection of vectors in K^n for some n, where K is a field; each vector in the collection is a *codeword*. The *Hamming distance* between two codewords is the number of positions where the codewords differ. If each codeword is intended to represent some piece of irreducible information, then desirable properties of a code are:

(a) Size: there should be lots of codewords, so that one can represent lots of information.

(b) Distinctness: the Hamming distance between any two codewords should be large, so that if a codeword is corrupted in some way, by changing the codeword in a small number of positions, the original codeword can be recovered.

(c) Efficiency: The ambient dimension n, which is the number of positions, should be as small as possible.

These three properties tend to act against each other, and the theory of *error-correcting codes* is directed towards the classification and analysis of possible codes and coding schemes.

Algebraic geometry has found an application in this area, by taking the field K to be a finite field, and taking the code to be certain natural spaces of functions or forms on an algebraic variety. Most successful have been attempts to use algebraic curves; this was initiated by Goppa and has been rather successful in producing codes with desirable properties, and in aiding in the classification and uniform treatment of several families of previously known codes.

IV.E Automatic Theorem Proving

It is often the case, especially in elementary geometry, that geometric statements can be expressed by having some polynomial vanish. For example, three points (x_1, y_1), (x_2, y_2), and (x_3, y_3) in the plane are collinear if and only if the determinant of the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix}$$

(which is the polynomial $x_2y_3 - x_3y_2 - x_1y_3 + x_3y_1 + x_1y_2 - x_2y_1$) is zero.

A typical theorem therefore might well be viewed as a collection of hypothesis polynomials $h_1, \ldots, h_k$, and a conclusion polynomial g. The truth of the theorem would be equivalent to saying that wherever the hypothesis polynomials all vanish, the conclusion polynomial is also zero. This exactly says that $g \in I(Z(\{h_1, \ldots, h_k\}))$, using the language of the Z-I correspondence of affine algebraic geometry.

If the field is algebraically closed, the Nullstellensatz says that the conclusion polynomial g is in this ideal if and only if some power of g is a linear combination of the h_i's, i.e., there is some equation of the form

$$g^r = \sum_i f_i h_i$$

where f_i are other polynomials. A "proof" of the theorem would be given by an explicit collection of polynomials f_i, which exhibited the equation above for some r, and this can be easily checked by a computer. Indeed, algorithms exist which check for the existence of such an expression for g, and are therefore effective in determining the truth of a given proposed theorem.

IV.F Interpolation

A general problem in approximation theory is to construct easy-to-evaluate functions with specified behavior. Typically this behavior involves either the values of the function at prescribed loci, or values of the derivatives of the functions, or both. Polynomial interpolation is the method whereby polynomial functions are used in this manner, and algebraic geometry has found recent applications and new problems of interest in this field in recent decades.

Lagrange interpolation is the name for finding polynomial functions with specified values c_k at a specified set of points $p_k \in \mathbb{A}^n$. In one variable there is a relatively easy formula for writing down the desired polynomial, and this is taught in most first-year calculus courses; however in higher dimensions no such formula exists. However the problem is a linear problem, and so is a straightforward application of linear algebra techniques.

Hermite interpolation is the name for finding polynomial functions with specified *derivative* values. This is a significantly more complicated generalization, and open questions exist even for polynomials in two variables.

Spline interpolation is the name for finding piece-wise polynomial functions, which stitch together to have a certain degree of global smoothness, but which also have specified behavior at given points. Cubic splines are the most popular in one variable, and with the advent of computer graphics two and three-variable splines are becoming more widely known and used in elementary applications.

In all of these settings, techniques of algebraic geometry are brought to bear in order to determine the dimension of the space of suitable interpolating functions. Usually it is a simple matter to find a lower bound for such dimensions, and the harder problem is to find sharp upper bounds.

IV.G Graphics

The origins of projective geometry lie in the early Renaissance, when artists and architects began to be interested in accurately portraying objects in perspective properly. The correct treatment of horizon lines and vanishing points in artwork of the period led directly to a new appreciation of points at infinity and eventually to a mathematically sound theory of projective geometry.

With the recent explosion of capabilities in computer speed, resolution of displays, and amount and interest of visualizing data, an appreciation of projective geometry, homogeneous coordinates, and projective transformations have lately become standard fare for computer graphics specialists and novices alike.

Although initially the application of the ideas of projective geometry were rather elementary, lately more sophisticated techniques are being brought to bear, especially involving problems in computer vision and pattern recognition. In particular it now seems feasible to use rather subtle projective invariants to discriminate between scene objects of either different types at the same perspective or the same type at different perspectives.

Bibliography

Beauville, A. (1996) *Complex Algebraic Surfaces, Second Edition.* Cambridge University Press.

Cox, D., Little, J., and O'Shea, D. (1997). *Ideals, Varieties, and Algorithms; An Introduction to Computational Algebraic Geometry and Commutative Algebra, Second Edition.* Springer-Verlag, New York.

Cox, D., Little, J., and O'Shea, D. (1997). *Using Algebraic Geometry.* Graduate Texts in Mathematics, v. 185, Springer-Verlag, New York.

Eisenbud, D. (1996). *Commutative Algebra With a View Toward Algebraic Geometry.* Graduate Texts in Mathematics, v. 150, Springer-Verlag, New York.

Fulton, W. (1997). *Intersection Theory, Second Edition.* Springer-Verlag, New York.

Harris, J. (1992) *Algebraic Geometry; A First Course.* Springer-Verlag, New York.

Harris, J. and Morrison, I. (1998). *Moduli of Curves.* Springer-Verlag, New York.

Hartshorne, R. (1979). *Algebraic Geometry.* Springer-Verlag, New York.

Griffiths, P. and Harris, J. (1978). *Principles of Algebraic Geometry.* Wiley Interscience, New York.

Kirwan, F. (1992). *Complex Algebraic Curves.* Cambridge University Press.

Miranda, R. (1995). *Algebraic Curves and Riemann Surfaces.* American Mathematical Society, Providence.

Reid, M. (1988). *Undergraduate Algebraic Geometry.* Cambridge University Press.

Shafarevich, I. (1994). *Basic Algebraic Geometry, 2 volumes.* Springer-Verlag, New York.

Sturmfels, B. (1996) *Grobner Bases and Convex Polytopes.* American Mathematical Society, Providence.

Ueno, K. (1999) *Algebraic Geometry I: from Algebraic Varieties to Schemes.* American Mathematical Society, Providence.