

Lecture 13

Lecturer: Pablo A. Parrilo

Scribe: ???

Today we introduce the first basic elements of algebraic geometry, namely ideals and varieties over the complex numbers. This dual viewpoint (ideals for the algebra, varieties for the geometry) is enormously powerful, and will help us later in the development of methods for solving polynomial equations. We also present the notion of quotient rings, which are very natural when considering functions defined on algebraic varieties (e.g., in polynomial optimization problems with equality constraints). Finally, we begin our study of Groebner bases, by defining the notion of term orders. A superb introduction to algebraic geometry, emphasizing the computational aspects, is the textbook of Cox, Little, and O’Shea [CLO97].

1 Polynomial ideals

For notational simplicity, we use $\mathbb{C}[\mathbf{x}]$ to denote the polynomial ring in n variables $\mathbb{C}[x_1, \dots, x_n]$. Specializing the general definition of an ideal to a polynomial ring, we have the following:

Definition 1. A subset $I \subset \mathbb{C}[\mathbf{x}]$ is an ideal if it satisfies:

1. $0 \in I$.
2. If $a, b \in I$, then $a + b \in I$.
3. If $a \in I$ and $b \in \mathbb{C}[\mathbf{x}]$, then $a \cdot b \in I$.

The two most important examples of polynomial ideals for our purposes are the following:

- The set of polynomials that vanish in a given set $S \subset \mathbb{C}^n$, i.e.,

$$\mathbf{I}(S) := \{f \in \mathbb{C}[\mathbf{x}] : f(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in S\},$$

is an ideal, called the *vanishing ideal* of S .

- The ideal generated by a finite set of polynomials $\{f_1, \dots, f_s\}$, defined as

$$\langle f_1, \dots, f_s \rangle := \{f \mid f = g_1 f_1 + \dots + g_s f_s, \quad g_i \in \mathbb{C}[\mathbf{x}]\}. \quad (1)$$

An ideal is *finitely generated* if it can be written as in (1) for some finite set of polynomials $\{f_1, \dots, f_s\}$. An ideal is called *principal* if it can be generated by a single polynomial. The intersection of two ideals is again an ideal. What about the union of ideals?

Example 2. In the univariate case (i.e., the polynomial ring is $\mathbb{C}[x]$), every ideal is principal.

One of the most important facts about polynomial ideals is Hilbert’s finiteness theorem:

Theorem 3 (Hilbert Basis Theorem). Every polynomial ideal in $\mathbb{C}[\mathbf{x}]$ is finitely generated.

We will present a proof of this after learning about Groebner bases. From the computational viewpoint, two very natural questions about ideals are the following:

- Given a polynomial $p(x)$, how to decide if it belongs to a given ideal?
- How to find a “convenient” representation of an ideal? What does “convenient” mean?

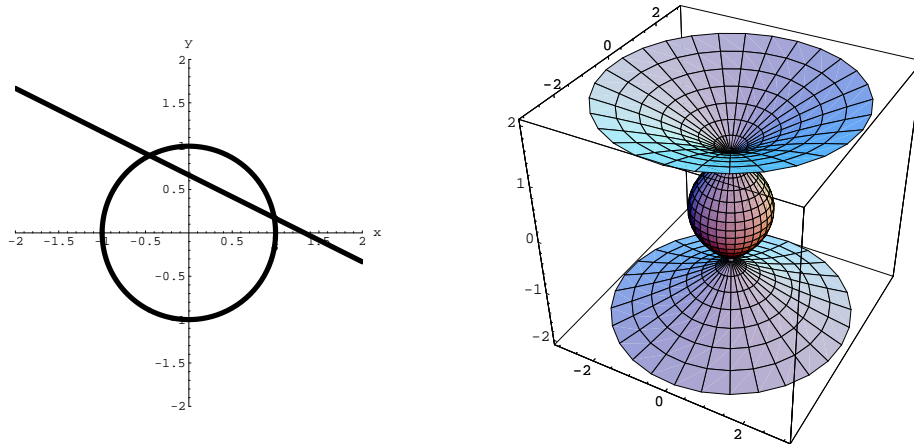


Figure 1: Two algebraic varieties. The one on the left is defined by the equation $(x^2 + y^2 - 1)(3x + 6y - 4) = 0$. The one on the right is a quartic surface, defined by $1 - x^2 - y^2 - 2z^2 + z^4 = 0$.

2 Algebraic varieties

An (affine) algebraic variety is the zero set of a finite collection of polynomials (see formal definition below). The word “affine” here means that we are working in the standard affine space, as opposed to projective space, where we identify $x, y \in \mathbb{C}^n$ if $x = \lambda y$ for some $\lambda \neq 0$.

Definition 4. Let f_1, \dots, f_s be polynomials in $\mathbb{C}[\mathbf{x}]$. Let the set \mathbf{V} be

$$\mathbf{V}(f_1, \dots, f_s) := \{(a_1, \dots, a_n) \in \mathbb{C}^n : f_i(a_1, \dots, a_n) = 0 \quad 1 \leq i \leq s\}.$$

We call $\mathbf{V}(f_1, \dots, f_s)$ the affine variety defined by f_1, \dots, f_s .

A simple example of a variety is a (complex) affine subspace, that corresponds to the vanishing of a finite collection of affine polynomials. A few additional examples of varieties are shown in Figure 1.

It is not too hard to show that *finite* unions and intersections of algebraic varieties are again algebraic varieties. What about the infinite case?

Remark 5. Recall our previous encounter with the Zariski topology, whose closed sets were defined to be the algebraic varieties, i.e., the vanishing set of a finite set of polynomial equations. To prove that this is actually a topology, we need to show that arbitrary intersections of closed sets are closed. Hilbert’s basis theorem precisely guarantees this fact.

Perhaps the most natural question about algebraic varieties is the following:

- Given a variety V , how to decide it is nonempty?

Let’s start connecting ideals and varieties. Consider a finite set of polynomials $\{f_1, \dots, f_s\}$. We already know how to generate an ideal, namely $\langle f_1, \dots, f_s \rangle$. However, we can also look at the corresponding variety $\mathbf{V}(f_1, \dots, f_s)$. Since this variety is a subset of \mathbb{C}^n , we can form the corresponding vanishing ideal, $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$. How do these two ideals related to each other? Is it always the case that

$$\langle f_1, \dots, f_s \rangle = \mathbf{I}(\mathbf{V}(f_1, \dots, f_s)),$$

and if it is not, what are the reasons? The answer to these questions (and more) will be given by another famous result by Hilbert, known as the Nullstellensatz.

3 Quotient rings

Whenever we have an ideal in a ring, we can immediately define a notion of equivalence classes, where we identify two elements in the ring if and only if their difference is in the ideal.

Example 6. Recall that a simple example of an ideal in the ring \mathbb{Z} was the set of even integers. By identifying two integers if their difference is even, we partition \mathbb{Z} into two equivalence classes, namely the even and the odd numbers. More generally, if the ideal is given by the integer multiples of a given number m , then \mathbb{Z} can be partitioned into m equivalence classes.

We can do this for the polynomial ring $\mathbb{C}[\mathbf{x}]$, and any ideal I .

Definition 7. Let $I \subset \mathbb{C}[\mathbf{x}]$ be an ideal, and let $f, g \in \mathbb{C}[\mathbf{x}]$. We say f and g are congruent modulo I , written

$$f \equiv g \pmod{I},$$

if $f - g \in I$.

It is easy to show that this is an equivalence relation, i.e., it is reflexive, symmetric, and transitive. Thus, this partitions $\mathbb{C}[\mathbf{x}]$ into equivalence classes, where two polynomials are “the same” if their difference belongs to the ideal. This allows us to define the quotient ring:

Definition 8. The quotient $\mathbb{C}[\mathbf{x}]/I$ is the set of equivalence classes for congruence modulo I .

The quotient $\mathbb{C}[\mathbf{x}]/I$ inherits the ring structure of $\mathbb{C}[\mathbf{x}]$, with the natural operations. Thus, with these operations now defined between equivalence classes, $\mathbb{C}[\mathbf{x}]/I$ becomes a ring, known as the *quotient ring*.

Quotient rings are particularly useful when considering a polynomial function $p(x)$ over the algebraic variety defined by $g_i(x) = 0$. Notice that if we define the ideal $I = \langle g_i \rangle$, then *any* polynomial q that is congruent with p modulo I takes exactly the same values in the variety.

4 Monomial orderings

In order to begin studying “nice” bases for ideals, we need a way of ordering monomials. In the univariate case, this is straightforward, since we can define $x^a \succ x^b$ as being true if and only if $a > b$. In the multivariate case, there are a lot more options.

We also want the ordering structure to be consistent with polynomial multiplication. This is formalized in the following definition.

Definition 9. A monomial ordering on $\mathbb{C}[\mathbf{x}]$ is a relation \succ on \mathbb{Z}_+^n (i.e., the monomial exponents), such that:

1. The relation \succ is a total ordering.
2. If $\alpha \succ \beta$, and $\gamma \in \mathbb{Z}_+^n$, then $\alpha + \gamma \succ \beta + \gamma$.
3. The relation \succ is a well-ordering (every nonempty subset has a smallest element).

One of the simplest examples of a monomial ordering is the *lexicographic* ordering, where $\alpha \succ_{\text{lex}} \beta$ if the left-most nonzero entry of $\alpha - \beta$ is positive. We will see some other examples of monomial orderings later in the course.

References

[CLO97] D. A. Cox, J. B. Little, and D. O’Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer, 1997.