Varieties and Ideals

J.M. Selig
Faculty of Business
London South Bank University,
London SE1 0AA, UK

1 Introduction

This talk is the first in what I hope will be a series of a few talks on Gröbner bases. There are quite a few ideas and concepts to understand so the actual main subject of the talk will take some time to make its appearance. That is, it will be quite a while before we can actually say what a Gröbner basis is.

However, it is probably useful to begin with some idea of where this is all heading. The idea is that we want to be able to solve, or at least get some insight into the solution of, systems of polynomial equations. Crudely speaking the Gröbner basis is a kind of analogue of the upper triangular form for systems of linear equations. We begin by introducing some very basic notions.

It is traditional in the subject to be coy about which field we are working over. This is because most authors want to be very general and hint at the possibility of working over finite field or the field of real numbers. But, to be honest, I'm really only interested in the case where the ground field is the complex numbers $\mathbb{C}$. This is because the field of complex numbers are closed, and hence the result we obtain are more extensive. (The other thing that makes for better results is to consider everything to be projective, so that polynomial must be homogeneous. This is an extra complication which we will not bother with here.) To follow standard texts we will write the field as K but as mentioned we will almost always mean $K = \mathbb{C}$.

Affine space of n dimensions will be written K^n. Point in this space will be written as n-tuples, $(a_1,\, a_2, \ldots, a_n)$, where $a_i \in K$ for all $1 \leqslant i \leqslant n$.

A **monomial** is a product of powers of variables, of the form $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$. The exponents α_i, are often condensed into a multi-index $\alpha = (\alpha_1,\, \alpha_2, \ldots, \alpha_k) \in \mathbb{Z}^k_{\geqslant 0}$. A monomial can then be written concisely as x^α.

A **term** is a monomial multiplied by an element of the ground field,

$$ax^\alpha = ax_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k} \qquad \text{with} \quad a \in K.$$

A **polynomial** is a sum of terms: $f = f(x) = a_1 x^\alpha + a_2 x^\beta + \cdots + a_j x^\xi$.

The **ring of polynomials** in n variables will be denoted $K[x_1,\, x_2, \ldots, x_n]$. This comprises all possible polynomials,

$$K[x_1,\, x_2, \ldots, x_n] = \{f : f(x) = \sum_\alpha a_1 x^\alpha + a_2 x^\beta + \cdots + a_j x^\xi\}$$

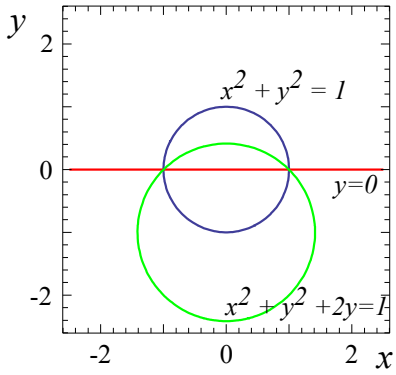

Figure 1: A Variety consisting of Two Points

2 Affine Varieties

An affine variety is the zero set of a collection of polynomial. This can be defined as:

$$\begin{aligned}\mathbf{V}(f_1,\, f_2, \ldots, f_k) \quad &= \quad \{(a_1, a_2, \ldots, a_n) \in K^n : f_1(a_1, a_2, \ldots, a_n) = 0, \\ &\qquad f_2(a_1, a_2, \ldots, a_n) = 0, \ldots, f_k(a_1, a_2, \ldots, a_n) = 0\}\end{aligned}$$

As an example consider a two variable example, $\mathbf{V}(x^2+y^2-1,\, y) = \{(1, 0),\, (-1, 0)\}$, see figure 1. Notice that if we add multiples of the polynomials then the zero-set stays the same, for example,

$$\mathbf{V}((x^2 + y^2 - 1) + 2y,\, y) = \mathbf{V}(x^2 + y^2,\, y) = \{(1, 0),\, (-1, 0)\}.$$

In this particular case the equation, $0 = (x^2 + y^2 - 1) + 2y = x^2 + (y + 1)^2 - 2$ represents a circle centred on the point $(0, -1)$ with radius $\sqrt{2}$ units.

More generally we can multiply the polynomials of the system by any other polynomial, however this may introduce more zeros. So it is easy to see that,

$$\mathbf{V}(f_1,\, f_2, \ldots, f_k) \subseteq \mathbf{V}(h_1,\, h_2, \ldots, h_l)$$

if for all i, $h_i(x) = \sum_{j=1}^{k} g_j(x) f_j(x)$ where $g_j(x) \in K[x_1, \ldots, x_n]$.

The set of all functions of the form $h(x) = \sum_{j=1}^{k} g_j(x) f_j(x)$ where $g_j(x) \in K[x_1, \ldots, x_n]$ is thus interesting and useful to study.

3 Ideals

This introduces the notion of an ideal. In any ring, but particularly in the ring of polynomials $K[x_1, \ldots, x_n]$, an **ideal** is a subset of elements $I \subseteq K[x_1, \ldots, x_n]$ with the following properties,

1. $0 \in I$

2. if $f,\, g \in I$ then $f + g \in I$

3. if $f \in I$ then the product $hf \in I$ for any $h \in K[x_1, \ldots, x_n]$.

This is an analogue of the zero element in a ring, and in any ring the subset $\{0\}$ is always an ideal—the zero ideal. Another ideal of any ring is the ring itself. Notice that if I is an ideal of $K[x_1, \ldots, x_n]$ and $1 \in I$ then it is easy to see that $I = K[x_1, \ldots, x_n]$. If we want to exclude the possibility that the ideal may be the whole of the ring we can talk about proper ideals.

For us the most important example of an ideal is the ideal introduced above, the set of all polynomials of the form $h(x) = \sum_{j=1}^{k} g_j(x) f_j(x)$ where $g_j(x) \in K[x_1, \ldots, x_n]$, this will be written,

$$< f_1,\, f_2, \ldots, f_k > \quad = \quad \{h \in K[x_1, \ldots, x_n] : h(x) = \sum_{j=1}^{k} g_j(x) f_j(x) \quad \text{where} \quad g_j(x) \in K[x_1, \ldots, x_n]\}$$

and called the ideal generated by the polynomials, $f_1, \ldots, f_k$. Moreover, given an ideal of the form $< f_1,\, f_2, \ldots, f_k >$, the polynomials $f_1, \ldots, f_k$ are called the basis of the ideal. Our ultimate aim is to describe a particular type of basis for any ideal, known as the Gröbner basis for the ideal.

A key theorem of Hilbert is that any ideal in $K[x_1, \ldots, x_n]$ has the form $< f_1,\, f_2, \ldots, f_k >$, that is any ideal is generated by a finite set of polynomials. With some luck we will be able to give a constructive proof of this latter.

4 Some Particular Types of Ideals

A **principal ideal** is an ideal generated by a single polynomial, $< f >$. In $\mathbb{C}[x]$, that is complex polynomials in one variable, all ideals are principal, indeed $< f, g >=< \gcd(f, g) >$. That is an ideal generated by two polynomials is the same as the ideal generated by their greatest common divisor. In particular, if f and g are coprime $\gcd(f, g) = 1$ then $< f, g >= \mathbb{C}[x]$ the whole ring.

A **maximal ideal** is a proper ideal that is not contained in any other proper ideal. This is usually stated as follows,

$$I \quad \text{is maximal} \Leftrightarrow I \subset J \Rightarrow J = K[x_1, \ldots, x_n]$$

A **monomial ideal** is an ideal generated by monomials, $< x^{\alpha}, x^{\beta}, \ldots, x^{\xi} >$. Notice that elements of such an ideal will not generally be monomials. Indeed general element of such an ideal will have the form,

$$h(x) = g_{\alpha}(x) x^{\alpha} + g_{\beta}(x) x^{\beta} + \cdots + g_{\xi}(x) x^{\xi},$$

for some polynomials $g_i(x) \in K[x_1, \ldots, x_n]$. Hence given an arbitrary ideal, it may be quite difficult to tell if it is a monomial ideal or not.

Consider the ideal in two variables $< x^2, y^2 >$, notice that the polynomials $x,\ y$ and xy are not in this ideal. However, any other polynomial,

$$f(x,y) = \sum_{\max(i,j)\geqslant 2} a_{ij}x^i y^j$$

does lie in this ideal. The radical of an ideal, written $\sqrt{I}$ is given by the set of polynomials which have a power lying in I,

$$\sqrt{I} = \{f : f^r \in I, \quad \text{for some finite positive integer} \quad r\}$$

Clearly, in the example above, $\sqrt{< x^2, y^2 >} =< x, y >$. Now a **radical ideal** is an ideal which is its own radical; $\sqrt{I} = I$. Notice that in our example $< x, y >$ is a radical ideal.

Finally here, a **prime ideal** is an ideal which satisfies the following,

$$I \quad \text{is prime} \Leftrightarrow f(x)g(x) \in I \Rightarrow f(x) \in I \quad \text{or} \quad g(x) \in I.$$

Notice that a principal ideal, an ideal generated by a single polynomial, is prime if and only if the polynomial generating it is irreducible. The notion of a prime ideal generalises this concept of irreducibility to general ideals.

5 Correspondence Between Ideals and Varieties

As we have, sort of, seen above; a variety determines an ideal. To be more formal, given a variety, we may define the ideal of all polynomials which vanish on the variety. This can be written,

$$\mathbf{I}(V) = \{f(x) \in K[x_1, \ldots, x_n] : f(x) = 0 \quad \text{if} \quad x \in V\}.$$

On the other hand it is also possible to define a variety given an ideal. In this case we have,

$$\mathbf{V}(I) = \{x \in K^n : f(x) = 0 \quad \text{if} \quad f \in I\}.$$

So there is a correspondence between the ideals and the varieties. This correspondence is a contravariant functor. In particular the variety $V = K^n$, that is the whole of the affine space, corresponds to the zero ideal $\mathbf{I}(K^n) = \{0\} =< 0 >$. On the other hand the variety corresponding to the whole of $K[x_1, \ldots, x_n]$ is the null variety, $\mathbf{V}(K[x_1, \ldots, x_n]) = \varnothing$.

More generally, if $I \subseteq J$ then $\mathbf{V}(J) \subseteq \mathbf{V}(I)$, notice the change of order here. To see this notice that if $f_1,\ f_2 \in I$ then from the definitions,

$$\mathbf{V}(I) \subseteq \mathbf{V}(< f_1 >) \cap \mathbf{V}(< f_2 >).$$

So if there is a polynomial $g \in J$ but $g \notin I$, then,

$$\mathbf{V}(J) \subseteq \mathbf{V}(I) \cap \mathbf{V}(< g >) \subseteq \mathbf{V}(I).$$

This also works for varieties, suppose $U \subseteq V$ are varieties, then $\mathbf{I}(V) \subseteq \mathbf{I}(U)$. Suppose there is a point a in V that is not in U. Now all the polynomials that vanish on V must also vanish on the subset U but there may be functions which vanish on U but don't vanish at a say.

Now what happens if we find the zero set of an ideal and then take the ideal of this variety. We could also do this the other way around; find the ideal of a variety and then find the zero set of this ideal.

It is not hard to see that $\mathbf{V}(\mathbf{I}(V)) = V$ but $\mathbf{I}(\mathbf{V}(I)) \supseteq I$. If we recall the example above concerning radical ideals we can understand this. Notice that $\mathbf{V}(< x^2, y^2 >) = \{(0,0)\}$, the variety corresponding to this ideal is simply the point at the origin. Now $\mathbf{I}(\{(0,0)\}) =< x, y >$, the ideal of polynomials vanishing at the origin are generated by the polynomials x and y. So we see that, $\mathbf{I}(\mathbf{V}(< x^2, y^2 >)) =< x, y >$. It is possible to show that (for $K = \mathbb{C}$) if I is a radical ideal then $\mathbf{I}(\mathbf{V}(I)) = I$.

This correspondence between ideals and varieties goes much deeper. For example, maximal ideals correspond to points in K^n. Principal ideals to hypersurfaces and prime ideals to irreducible varieties. Finally here, the addition of ideals corresponds to the intersection of varieties.

6 Addition of ideals

Ideal can be added, multiplied and intersected, here we just look at addition. Let I and J be ideals the sum $I + J$ is defined as,

$$I + J = \{f + g : f \in I \quad \text{and} \quad g \in J\}$$

The sum of two ideals is again an ideal. Moreover, we have that,

$$< f_1, f_2, \ldots f_k > + < g_1, g_2, \ldots, g_l >=< f_1, f_2, \ldots f_k, g_1, g_2, \ldots, g_l > .$$

A simple consequence of this is that,

$$< f_1, f_2, \ldots, f_k >=< f_1 > + < f_2 > + \cdots + < f_k >$$

References

[1] Cox, D. Little, J. and O'Shea, D., 1996, "Ideals, Varieties, and Algorithms an Introduction to ALgebraic Geometry and Commutative Algebra (second ed.)", Springer Verlag, Berlin.