2 Multivariate polynomials and algebraic sets

We will work out a division algorithm for polynomials in several variables.

Example 1 An easy problem in geometry. Consider the plane $k^2$ with coordinates $x, y$. Let $f_1 = y^2 - 1$ and $f_2 = xy + 1$. If $X \subset k^2$ is the the set of points $(a, b)$ where both $f_1(a, b) = 0$ and $f_2(a, b) = 0$, how can we tell whether a third polynomial also vanishes on $X$? For example, does $f = xy^2 + xy + y^3 + 1$ vanish on $X$?

The answer is that, yes, $f$ does vanish on every point of $X$. One way to see it is to observe that $X = \{(1, -1), (-1, 1)\}$ and then to evaluate $f$ at these two points and see that it is zero at each. Or instead we can check that $f = yf_1 + (y + 1)f_2$, so that $f$ automatically vanishes wherever both $f_1$ and $f_2$ do. And if we could have seen that in advance we would not needed to know details of $X$ at all.

2.1 Polynomials in many variables

We will give pedantic definitions of polynomials and ideals, even though you surely already know how to work with polynomials in several variables. We also state Hilbert’s Basis Theorem which is not so trivial. Let $x_1, \ldots, x_n$ be independent indeterminates.

Definition 1 A monomial in $x_1, \ldots, x_n$ is an expression $x_1^{i_1} \cdots x_n^{i_n}$ for a tuple $i = (i_1, \ldots, i_n) \in \mathbb{N}^n$. A term in $x_1, \ldots, x_n$ over $k$ is an expression $am$ where $a \in k$ and $m$ is a monomial. A polynomial in $x_1, \ldots, x_n$ over $k$ is a finite $k$-linear combination of monomials, or equivalently it is a finite sum of terms.

We often write a polynomial as $f = \sum a_m m$ where the sum is taken over all monomials $m$ and it is understood that only finitely many of the coefficients $a_m$ are non zero. The set of all polynomials in $x_1, \ldots, x_n$ over $k$ is denoted $k[x_1, \ldots, x_n]$. It is, of course, a commutative ring under the usual addition and multiplication, and it is even an integral domain.

As in the univariate case, we can define the degree of a polynomial and we still denote it by $\deg(f)$, although since this will have a number of different interpretations later on we refer to it as the ‘total degree’.

Definition 2 The total degree of a monomial $m = x_1^{i_1} \cdots x_n^{i_n}$ is $\deg(m) = i_1 + \cdots + i_n$. Let $f = \sum a_i m_i$ be a polynomial, where $a_i \in k$ and $m_i$ are monomials. Then the total degree of $f$ is

$$\deg(f) = \max\{\deg(m_i) : a_i \neq 0\}.$$
leading. With that decision made, the leading term of \( x^2 + y^2 \) would be \( x^2 \). This kind of pragmatism is good, but the general solution below allows much greater freedom.

### 2.2 Ideals and Hilbert’s basis theorem

**Definition 3** A subset \( I \subset k[x_1, \ldots, x_n] \) is an ideal of \( k[x_1, \ldots, x_n] \) if and only if whenever \( f, g \in I \) then \( f + g \in I \) and whenever \( f \in I \) and \( p \in k[x_1, \ldots, x_n] \) then \( pf \in I \).

If \( f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \) then the set 
\[
\{ p_1 f_1 + \cdots + p_s f_s : p_1, \ldots, p_s \in k[x_1, \ldots, x_n] \} \subset k[x_1, \ldots, x_n]
\]
is an ideal, and it is denoted \((f_1, \ldots, f_s)\). More generally, if \( F \subset I \) is any subset, possibly infinite, then the set 
\[
\left\{ \sum_{\text{finite}} p_i f_i : f_i \in F, p_i \in k[x_1, \ldots, x_n] \right\}
\]
is an ideal denoted \((F) \subset k[x_1, \ldots, x_n] \).

**Definition 4** Let \( I \subset k[x_1, \ldots, x_n] \) be an ideal and \( F \subset I \). There is an inclusion of ideals \((F) \subset I \), and we say that \( F \) generates \( I \), or that \( F \) is a basis of \( I \), whenever this inclusion is an equality \((F) = I \).

An ideal \( I \subset k[x_1, \ldots, x_n] \) which has a basis consisting of exactly one polynomial \( \{f\} \) is called a principal ideal, written \( I = (f) \), and the polynomial is referred to as a principal generator for \( I \).

In fact, every ideal in \( k[x_1, \ldots, x_n] \) has a basis of finitely many elements. This is Hilbert’s Basis Theorem which we state here and will prove in the next section.

**Theorem 5 (Hilbert’s Basis Theorem)** Let \( I \subset k[x_1, \ldots, x_n] \) be an ideal. Then there are polynomials \( f_1, \ldots, f_s \subset I \) so that \( I = (f_1, \ldots, f_s) \).

**Notation for variables** We will frequently change the notation used for the variables. In statements of theorems we will continue to use \( k[x_1, \ldots, x_n] \), and also \( k[y_1, \ldots, y_m] \) if we need two polynomial rings. But most examples involve only two or three variables at a time. In these cases, we will write \( k[x, y] \) or \( k[u, v] \) or \( k[t, a, b] \) or \( k[x, y, z] \) or \( k[u_0, u_1, u_2, v] \) or whatever we feel like at the time. This could not possibly be confusing, could it?

### 2.3 Affine algebraic sets and the solutions of polynomials

By analogy with the univariate case, a solution of a polynomial \( f \in k[x_1, \ldots, x_n] \) is a tuple \((a_1, \ldots, a_n)\) of elements \( a_i \in k \) so that \( f(a_1, \ldots, a_n) = 0 \). Of course, we can ask for solutions that lie in extensions of \( k \), just as we might for solutions of univariate polynomials. Even so, there is a lot more to say about the solutions of multivariate polynomials than those of univariate polynomials.
The solution of systems of polynomials  We define \( n \)-dimensional affine space over \( k \), denoted \( \mathbb{A}_k^n \), to be the set of \( n \)-tuples of elements of \( k \), that is, \( \mathbb{A}_k^n \) is the Cartesian product \( k^n \). Polynomials \( f \in k[x_1, \ldots, x_n] \) can be regarded as functions on \( \mathbb{A}_k^n \) by evaluation:

\[
f : \mathbb{A}_k^n \rightarrow k \text{ where } (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n),
\]

and we usually abbreviate \( f(a_1, \ldots, a_n) \) to \( f(a) \) where \( a = (a_1, \ldots, a_n) \).

**Definition 6** The solution of a polynomial \( f \in k[x_1, \ldots, x_n] \) is the set of points \( a \in \mathbb{A}_k^n \) for which \( f(a) = 0 \): it is denoted \( V(f) \), so that

\[
V(f) = \{ a \in \mathbb{A}_k^n : f(a) = 0 \}.
\]

For instance, a unit circle is \( V(x^2 + y^2 - 1) \subset \mathbb{A}_{\mathbb{R}}^2 \). This notation works equally well for the solution of more than one polynomial at a time: if \( f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \) then we define

\[
V(f_1, \ldots, f_s) = \{ a \in \mathbb{A}_k^n : f_1(a) = \cdots = f_s(a) = 0 \}
\]

which is the set of solutions common to all the \( f_i \). It is also common to write

\[
(f_1 = \cdots = f_s = 0) \subset \mathbb{A}_k^n
\]

in place of \( V(f_1, \ldots, f_s) \) even though it is not any shorter.

**Example 1 (continued)** We can write \( X \), the common solutions of \( f_1, f_2 \), as \( X = V(f_1, f_2) \subset \mathbb{A}_{\mathbb{R}}^2 \). This is only a change in notation. ♥

Although not every subset of \( k^n \) that we can think of is defined as the solution space of finitely many polynomial equations—there are some examples in the exercises—there are sufficiently many interesting examples that these geometrical objects have a name.

**Definition 7** A subset \( S \subset \mathbb{A}_k^n \) is an algebraic set if and only if there are finitely many polynomials \( f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \) such that \( S = V(f_1, \ldots, f_s) \).

It is reasonable to think of algebraic sets as being rather rigidly defined: if \( X \subset \mathbb{A}_k^n \) is an algebraic set, then if you wiggle \( X \) a bit, or remove a point, or cut it in half, or take its image by a map \( \mathbb{A}_k^n \rightarrow \mathbb{A}_k^n \), then the result is unlikely to be another algebraic set (although that is not a rule). But there is some good news.

**Lemma 8** If \( X, Y \subset \mathbb{A}_k^n \) are algebraic sets, then \( X \cup Y \subset \mathbb{A}_k^n \) and \( X \cap Y \subset \mathbb{A}_k^n \) are also algebraic sets.
Proof: By definition, there are polynomials $f_i, g_j \in k[x_1, \ldots, x_n]$ so that
\[ X = (f_1 = \cdots = f_s = 0) \quad \text{and} \quad Y = (g_1 = \cdots = g_t = 0). \]
The proof is completed by exhibiting polynomials that define the intersection and the union. It is easy to see that
\[ X \cap Y = (f_1 = \cdots = f_s = g_1 = \cdots = g_t = 0) \]
and that $X \cup Y$ is defined by the collection of products $f_i g_j$ for $1 \leq i \leq s$ and $1 \leq j \leq t$.

What do we mean, then, by solving a system of polynomial equations
\[ f_1 = \cdots = f_s = 0 \quad \text{over a field } k \text{ in variables } x_1, \ldots, x_n? \]
We are asking for information about the corresponding algebraic set, $V(f_1, \ldots, f_s) \subset \mathbb{A}_k^n$. Or is it empty or not? And if not, is it a finite set or not? If so, what are the coordinates of its points, and are there yet more points defined over an extension of $k$? If not, what are the dimensions of its components?

The V–I transformations: We have made a link between algebra and geometry, and we make this more practical with a pair of functors that translate between algebraic sets and ideals.

**Definition 9** For any subset $X \subset \mathbb{A}_k^n$ define $I(X) \subset k[x_1, \ldots, x_n]$ by
\[ I(X) = \{ f : f \in k[x_1, \ldots, x_n] | f(p) = 0 \text{ for all } p \in X \}. \]
For any subset $F \subset k[x_1, \ldots, x_n]$ define $V(F) \subset \mathbb{A}_k^n$ by
\[ V(F) = \{ p : p \in \mathbb{A}_k^n | f(p) = 0 \text{ for all } f \in F \}. \]
(The definition of $V(F)$ extends the notation $V(f_1, \ldots, f_s)$ that we already use for algebraic sets.) It is easy to see that for any subset $X \subset \mathbb{A}_k^n$, the subset $I(X) \subset k[x_1, \ldots, x_n]$ is an ideal. Indeed, if $f, g$ both vanish at every point of $X$, then so does $f + g$, and so does $pf$ where $p \in k[x_1, \ldots, x_n]$ is any other polynomial.

**Lemma 10** If $F_1, F_2 \subset k[x_1, \ldots, x_n]$ generate the same ideal $(F_1) = (F_2)$, then $V(F_1) = V(F_2)$. For any subset $F \subset k[x_1, \ldots, x_n]$, the subset $V(F) \subset \mathbb{A}_k^n$ is an algebraic set.

**Proof** Let $J = (F_1)$ be the ideal generated by $F_1$. We first check that $V(F_1) = V(J)$. Let $p \in V(F_1)$. If $f \in J$ then $f = \sum p_i f_i$ for $f_i \in F_1$, so that $f(p) = \sum p_i(p) f_i(p) = 0$. This arguments works for any $f \in J$, so $p \in V(J)$. The converse is more obvious since $F_1 \subset J$. This shows that $V(F_1) = V(F_2)$.

Now by Hilbert’s Basis Theorem, we can find polynomials $f_1, \ldots, f_s$ so that $J = (f_1, \ldots, f_s)$. The proof is completed by noting exactly as in the first step that
\[ V(J) = V(f_1, \ldots, f_s). \]

Q.E.D.

This lemma shows that an algebraic set $V(f_1, \ldots, f_s)$ depends only on the ideal generated by $f_1, \ldots, f_s$, so when trying to solve these polynomials we are free to change the basis of the ideal without changing the solution to the problem.