21MAB143 Rings and Polynomials: Week 5

1 Polynomials in many variables

In Week 2 we defined the polynomial ring $K[x]$ in one variable over a field K. But our definition only used addition and multiplication in K, so it applies just as well to any commutative ring R. In other words, we can consider the ring $R[x]$ for any commutative ring R. This allows us to give a concise definition of polynomial rings in many variables, as follows:

Definition 1.1. *Let R be any commutative ring. Define the polynomial ring $R[x]$ just as we did in Week 2: $R[x]$ is the set of all expressions $\sum_{i\geq 0} a_i x^i$ where $a_i \in R$ and only finitely many are nonzero.*

Now let n be a positive integer. We define $R[x_1, \dots, x_n]$, the **polynomial ring in n variables over** R*, inductively as follows:*

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])\,[x_n]$$

In other words, given any commutative ring R, we can form the ring $R[x_1]$ of polynomials with coefficients in R, as above. Then we can define $R[x_1, x_2]$ as $(R[x_1])\,[x_2]$: that is, we now take $R[x_1]$ as our ring of coefficients, and form the ring of polynomials with coefficients in this ring to get the ring $(R[x_1])\,[x_2]$, which by definition is $R[x_1, x_2]$. Iterating, we get in this way a polynomial ring with any chosen number of variables.

Notation: We will often use different letters to denote our variables, rather than $x_1, \dots, x_n$. In particular if $n = 2$, we will usually write our variables as x, y instead of x_1, x_2. If $n = 3$ we will usually write the variables as x, y, z instead of x_1, x_2, x_3.

Example: Definition 1.1 may look abstract, but again it just encapsulates the properties of polynomials that you are already familiar with. To see this in practice, let's consider $\mathbf{R}[x, y, z]$, the polynomial ring in three variables over the real numbers. Take the two polynomials:

$$\begin{aligned} f &= 3xyz + 2yz + z + 1 \\ g &= -2y^3 + 3yz - z + 2 \end{aligned}$$

Then their sum and product in $\mathbf{R}[x, y, z]$ are calculated in the familiar way:

$$\begin{aligned} f + g &= 3xyz - 2y^3 + 5yz + 3 \\ fg &= -6xy^4z - 4y^4z + 9xy^2z^2 - 3xyz^2 + 6y^2z^2 \\ &\quad - 2y^3 + 6xyz + yz^2 + 7yz - z^2 + z + 2 \end{aligned}$$

Definition 1.2. *Let* K *be a field and* $K[x_1, \dots, x_n]$ *the ring of polynomials in* n *variables over* K*. A* **monomial** *in* $K[x_1, \dots, x_n]$ *is a polynomial of the form*

$$m = a x_1^{d_1} \cdots x_n^{d_n}$$

where a *is an nonzero element of the field* K*, and each exponent* d_i *is a non-negative integer. The* **degree** *of the monomial above is*

$$\deg(m) = d_1 + \cdots + d_n.$$

Any polynomial $f \in K[x_1, \dots, x_n]$ *can be written as a sum of monomials, and we define*

$$\deg(f) = \max\{\deg(m) \mid m \text{ is a monomial appearing in } f\}.$$

As usual, the zero polynomial $f = 0$ *is defined to have degree equal to* $-\infty$*.*

Degrees of sums and products behave in just the same way here as they did in the single-variable case (Week 2 Lemma 1.2):

Lemma 1.3. *For any two polynomials* p *and* q *in* $K[x_1, \dots, x_n]$*, we have the following relations:*

$$\deg(p + q) \leq \max\{\deg(p), \deg(q)\}$$
$$\deg(pq) = \deg(p) + \deg(q).$$

The proof is almost the same as that of Week 2 Lemma 1.2 but more complicated to write out, so we omit it.

Example: Returning to our polynomials above we have

$$\begin{aligned} \deg(f) &= 3 \\ \deg(g) &= 3 \\ \deg(f + g) &= 3 \\ \deg(fg) &= 6. \end{aligned}$$

The monomial of maximum degree in pq is $-6xy^4z$.

1.1 Ideals in $K[x_1, \dots, x_n]$

In Week 2 Theorem 2.5 we proved that every ideal $I \subset K[x]$ can be generated by a single element. But this is **not true** in the multi-variable case. This is perhaps the key difference between polynomial rings in one and many variables. It means that the multi-variable cases is unavoidably more complicated, but at the same time richer and more interesting.

Example The simplest example of an example that is not generated by a single element is the ideal

$$I = \langle x, y \rangle \subset K[x, y].$$

To see this, note that by Week 2 Proposition 2.4 every element in I is of the form $ax + by$ for polynomials a, $b \in K[x, y]$. So every element of I has constant term equal to zero.

Now suppose there were a polynomial $f \in K[x, y]$ such that $I = \langle f \rangle$. Since $x \in I$, this would imply that $f \mid x$: in other words, there is some other polynomial $g_1 \in K[x, y]$ such that $fg_1 = x$. In particular, this implies that $\deg(f)$ is equal to either 0 or 1. If it equals 1, then g_1 must be a nonzero constant, and thererefore $f = ax$ for some constant $a \in K$. But now applying the same argument to y instead of x we would also get $f = by$ for some constant $b \in K$. This is a contradiction.

The only remaining possiblity is that f has degree 0, in other words it is a nonzero constant. But since $f \in I$, this contradicts the fact mentioned above that every element of I has constant term equal to zero.

1.2 Example: ideals with many generators

In this example, we will see that in fact there is no bound for the smallest possible number of generators of an ideal in $K[x, y]$. In other words, for any fixed n, there is an ideal that needs at least $n + 1$ elements to generate it.

Here is the precise statement.

Claim: Fix a non-negative integer n. Let $I_n \subset K[x, y]$ be the ideal defined as follows:

$$I_n = \left\langle x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n \right\rangle .$$

Then there is no set of $k \leq n$ polynomials $\{f_1, \ldots, f_k\}$ in $K[x, y]$ such that

$$I_n = \langle f_1, \ldots, f_k \rangle .$$

Proof of Claim: Let $f \in I_n$. According to Week 2 Proposition 2.4, this means that f can be written in the form

$$f = r_n x^n + r_{n_1} x^{n-1} y + \cdots + r_0 y^n$$

for some polynomials $r_i \in K[x, y]$. So every monomial in f has degree $\geq n$.

Now suppose that there were k such polynomials $f_1, \ldots, f_k$ which generate I_n. By the previous paragraph, every monomial in f_i must have degree $\geq n$.

Again using Week 2 Proposition2.4, each monomial $x^i y^{n-i}$ could be written in the form

$$x^i y^{n-i} = \rho_{i1} f_1 + \cdots + \rho_{ik} f_k$$

for some polynomials ρ_{ik}. But the only way to get monomials of degree exactly n on the right-hand side is to multiply the constant term of ρ_{ij} by a monomial of degree n in f_j. So we have

$$x^i y^{n-i} = \widetilde{\rho_{i1}} \widetilde{f_1} + \cdots + \widetilde{\rho_{ik}} \widetilde{f_k} \qquad (*)$$

where $\widetilde{\rho_{ij}}$ denotes the constant term in ρ_{ij} and $\widetilde{f_j}$ denotes the sum of all monomials of degree n in f_j.

Now let $K[x, y]_{=n}$ denote the vector space of polynomials in which every term has degree equal to n, together with the zero polynomial 0.

On one hand, $K[x, y]_{=n}$ contains all the monomials $x^i y^{n-i}$ and it is easy to check that these are linearly independent, so $K[x, y]_{=n}$ has dimension at least $n + 1$.

On the other hand, Equation $(*)$ shows that each $x^i y^{n-i}$ can be written as a linear combination of the polynomials $\widetilde{f_k}$, so $K[x, y]_{=n}$ is spanned by the k polynomials $\widetilde{f_k}$. This is a contradicition, showing that it is impossible to find a set of $k \leq n$ polynomials generating the ideal I_n.

2 Ideals in $K[x_1, \ldots, x_n]$ and algebraic subsets of K^n

One of the main reasons to be interested in ideals in $K[x_1, \ldots, x_n]$ is that they can be used to describe interesting geometric objects. This idea is the basis of "Algebraic Geometry", a central topic in modern mathematics.

Here's how it works.

Definition 2.1. *Let K be a field, and let $I \subset K[x_1, \ldots, x_n]$ be an ideal. The* **algebraic set defined by** I *is the set*

$$V(I) = \{(a_1, \ldots, a_n) \in K^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\} \subset K^n.$$

In other words, $V(I)$ is the set of common zeroes of all the polynomials in I. We'll shortly look at some examples to see what kind of geometric objects we get in this way. First we need a lemma that makes $V(I)$ easier to understand.

Lemma 2.2. *Let $I \subset K[x_1, \ldots, x_n]$ be an ideal of the form*

$$I = \langle f_1, \ldots, f_k \rangle .$$

Then for a point $(a_1, \ldots, a_n) \in K^n$ we have

$$(a_1, \ldots, a_n) \in V(I) \quad \text{if and only if} \quad f_i(a_1, \ldots, a_n) = 0 \text{ for all } i = 1, \ldots, k.$$

This means that to find all the common zeroes of all the polynomials in I, it is enough to find the common zeroes of the generators if I.

Proof. In one direction, by definition if $(a_1, \ldots, a_n) \in V(I)$ then every element of I is zero at $(a_1, \ldots, a_n)$. In particular, each of the f_i is zero at $(a_1, \ldots, a_n)$.

Conversely, suppose each of the f_i is zero at $(a_1, \ldots, a_n)$. According to Week 2 Proposition 2.4, every element of the ideal I can be written in the form

$$f = r_1 f_1 + \cdots + r_k f_k$$

for some polynomials $r_i \in K[x_1, \ldots, x_n]$. So we get

$$\begin{aligned} f(a_1, \ldots, a_n) &= r_1(a_1, \ldots, a_n) f_1(a_1, \ldots, a_n) + \cdots + r_k(a_1, \ldots, a_n) f_k(a_1, \ldots, a_n) \\ &= 0. \end{aligned}$$

□

Examples In these examples we'll stick to the case $K = \mathbf{R}$ and $n = 2$ so that we can easily visualise our algebraic sets. So we are considering ideals in $\mathbf{R}[x, y]$ and subsets in the usual plane $\mathbf{R}^2$.

1. First let's consider $I_1 = \langle x^2 + y^2 - 1 \rangle$. By Lemma 2.2 above, we have

$$V(I_1) = \left\{(a_1, a_2) \in \mathbf{R}^2 \mid a_1^2 + a_2^2 - 1 = 0\right\}.$$

   This is just the unit circle centred at the origin in $\mathbf{R}^2$.

2. Sticking to ideals generated by a single element, now we consider $I_2 = \langle (x^2 + y^2)^3 - 4x^2y^2 \rangle$. Again using Lemma 2.2 we have

$$V(I_2) = \left\{(a_1, a_2) \in \mathbf{R}^2 \mid (a_1^2 + a_2^2)^3 - 4a_1^2a_2^2 = 0\right\}.$$

   This is a more complicated curve in $\mathbf{R}^2$, sometimes called the **quadrifolium**.

3. Finally we consider an ideal generated by more than one element. So take

$$I_3 = \langle x^2 + y^2 - 1, (x^2 + y^2)^3 - 4x^2y^2 \rangle.$$

   Then

$$\begin{aligned} V(I_3) &= \left\{(a_1, a_2) \in \mathbf{R}^2 \mid a_1^2 + a_2^2 - 1 = (a_1^2 + a_2^2)^3 - 4a_1^2a_2^2 = 0\right\} \\ &= V(I_1) \cap V(I_2) \\ &= \{p_1, p_2, p_3, p_4\} \end{aligned}$$

   where the p_i are all the points with coordinates of the form $p_i = \left(\pm\frac{1}{\sqrt{2}}, \pm\frac{1}{\sqrt{2}}\right)$.

Each of these algebraic sets is shown in Figure 1.

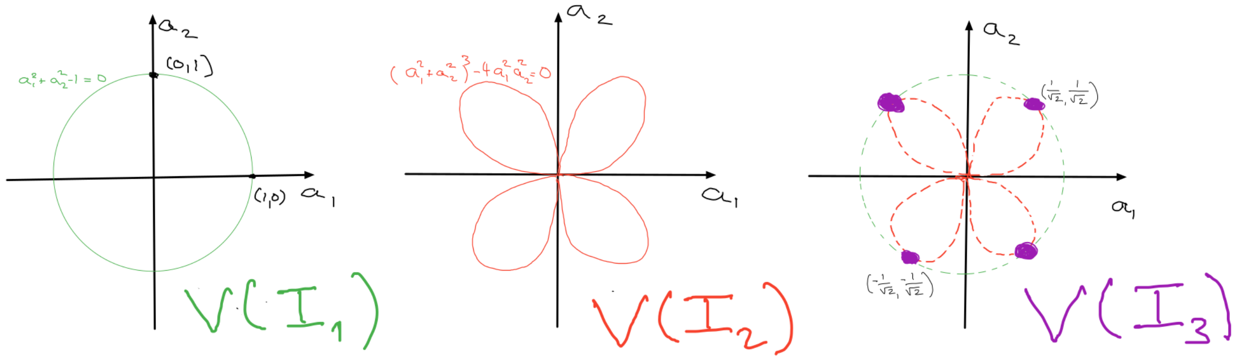

Figure 1: The algebraic sets defined by the ideals I_1, I_2, and I_3.

In general it is not easy to find the intersection points of two arbitrary algebraic sets. For the special case of two curves in the plane, there is a good method based on the **multivariable resultant** — we will see this in Week 6.

Remark: In these examples, ideals in $\mathbf{R}[x,y]$ defined algebraic subsets in $\mathbf{R}^2$, but in general over the real numbers, there is not a good correspondence between ideals in the polynomial ring and algebraic sets. For example Problem Sheet 5 Question 3(b) asks you to find an ideal $I \subset \mathbf{R}[x_1, \dots, x_n]$ such that $V(I) = \emptyset$.

For this reason, algebraic geometry usually starts by working with polynomials in $\mathbf{C}[x_1, \dots, x_n]$ and algebraic sets in $\mathbf{C}^n$. In that context, the correspondence between ideals and algebraic sets is almost perfect. The Part C Algebraic Geometry module will explore this theme much further.

2.1 Example: curves in $\mathbf{R}^3$

In this example we will study two algebraic sets in three-dimensional space $\mathbf{R}^3$. So in the polynomial ring $\mathbf{R}[x,y,z]$ consider the two ideals

$$I_1 = \langle y - x^2,\, z - xy \rangle$$
$$I_2 = \langle y - x^2,\, z^2 - xy - 1 \rangle$$

Notice that each of the ideals I_1 and I_2 is generated by two polynomials of degree 2.

What can we say about the algebraic sets $V(I_1)$ and $V(I_2)$ in this case?

- $V(I_1)$: this is the set of points $(a_1, a_2, a_3) \subset \mathbf{R}^3$ where we have

  $$a_2 - a_1^2 = 0$$
  $$a_3 - a_1 a_2 = 0$$

  We can rearrange the first equation to say $a_2 = a_1^2$ and then substitute into the second to get $a_3 = a_1^2$. So we have

  $$V(I_1) = \left\{ (a_1, a_1^2, a_1^3) \mid a_i \in \mathbf{R} \right\} \subset \mathbf{R}^3$$

  Note that this curve can be parametrised by $\mathbf{R}$: there is a map

  $$\varphi \colon \mathbf{R} \to \mathbf{R}^3$$
  $$t \mapsto (t, t^2, t^3)$$

  which is injective (one-to-one) and whose image is exactly $V(I_1)$.

  The curve $V(I_1)$ is often calle the "twisted cubic curve". It has degree 3, meaning that for a general plane $\Pi \subset \mathbf{R}^3$, the intersection $V(I_1) \cap \Pi$ will consist of 3 distinct points. To see this, let Π be a plane given by an equation

  $$\Pi \colon c_1 x + c_2 y + c_3 z + c_4 = 0$$

  A point (a_1, a_2, a_3) on this plane must satisfy

  $$c_1 a_1 + c_2 a_2 + c_3 a_3 + c_4 = 0$$

Substituting $a_3 = a_1^3$ and $a_2 = a_1^2$ we get an equation

$$c_3 a_1^3 + c_1 a_1 + c_2 a_1^2 + c_4 = 0$$

For a general choice of the coefficients c_i this equation will have 3 solutions for a_1, giving 3 points in the intersection $V(I_1) \cap \Pi$.

- $V(I_2)$: this is the set of points $(a_1, a_2, a_3) \subset \mathbf{R}^3$ where we have

$$a_2 - a_1^2 = 0$$
$$a_3^2 - a_1 a_2 - 1 = 0$$

Again by rearranging and substitution, we get $a_2 = a_1^2$ and $a_3^2 = a_1^3 + 1$.

Again let Π be a general plane in $\mathbf{R}^3$, given by an equation

$$\Pi\colon c_1 x + c_2 y + c_3 z + c_4 = 0$$

for some constants c_1, c_2, c_3, c_4. Rearranging this equation gives

$$c_3 z = -c_1 x - c_2 y - c_4$$

so a point (a_1, a_2, a_3) on this plane must satisfy

$$c_3 a_3 = -c_1 a_1 - c_2 a_2 - c_4$$

Squaring both sides and substituting $a_2 = a_1^2$ and $a_3^2 = a_1^3 + 1$ we get an equation

$$c_3^2 \left(a_1^3 + 1\right) = \left(-c_1 a_1 - c_2 a_2^2 - c_4\right)^2$$

This is an equation of degree 4 in a_1, so for general coefficients c_1, c_2, c_3, c_4, we will find 4 distinct solutions for a_1 and hence 4 points of $V(I_2) \cap \Pi$.

So $V(I_2)$ is a curve of degree 4. This curve cannot be parametrised like the twisted cubic, but that is hard to prove! In fact $V(I_2)$ is an example of an "elliptic curve", and these curves are the topic of an entire Part C module.