21MAB143 Rings and Polynomials: Week 2

1 Polynomial Rings

You are probably already very familiar with polynomials and how to work with them. The following definition is just a formal restatement of what you already know.

Definition 1.1. *Let* K *be a field. We define* $K[x]$, *the* **polynomial ring** *over* K, *to be the set of all expressions*

$$\sum_{i\geq 0} a_i x^i$$

in which each a_i *is an element of* K *and only* **finitely many** *of the* a_i *are nonzero.*

The ring operations are defined as follows:

$$\left(\sum_{i\geq 0} a_i x^i\right) + \left(\sum_{i\geq 0} b_i x^i\right) = \sum_{i\geq 0} (a_i + b_i)\, x^i$$
$$\left(\sum_{i\geq 0} a_i x^i\right) \times \left(\sum_{i\geq 0} b_i x^i\right) = \sum_{i\geq 0} \left(\sum_{j+k=i} a_j b_k\right) x^i$$

For a polynomial $p = \sum_{i\geq 0} a_i x^i \in K[x]$, *we define its* **degree** $\deg(p)$ *to be the maximum* n *for which the coefficient* a_n *is nonzero. The degree of the zero polynomial* $p = 0$ *is defined to be* $\deg(0) = -\infty$.

Notation: From now on we will omit the symbol $\times$ for multiplication in the polynomial ring $K[x]$. So if p and q are two polynomials in $K[x]$ we will just write pq or sometimes $p \cdot q$ instead of $p \times q$.

Example Let's consider an example. Here we take our field K to be the rational numbers $\mathbf{Q}$, and we consider the following two (more or less random) polynomials $p,\ q \in \mathbf{Q}[x]$:

$$p = \frac{1}{2}x^3 + 4x - 3$$
$$q = x^5 - \frac{1}{2}x^3 - 2x^2 - \frac{1}{4}$$

Then

$$p + q = x^5 - 2x^2 + 4x - \frac{13}{4}$$
$$pq = \frac{1}{2}x^8 + \frac{15}{4}x^6 - 4x^5 - 2x^4 - \frac{53}{8}x^3 + 6x^2 - x + \frac{3}{4}$$

What are the degrees of all these polynomials? We see

$$\begin{aligned} \deg(p) &= 3 \\ \deg(q) &= 5 \\ \deg(p+q) &= 5 \\ \deg(pq) &= 8 \end{aligned}$$

So $\deg(p+q)$ is the maximum of the degrees of p and q, while $\deg(pq)$ is the sum of the degrees.

The following lemma explains how degrees interact with the ring operations in general:

Lemma 1.2. *For any two polynomials* p *and* q *in* $K[x]$, *we have the following relations:*

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

Proof. Since every polynomial has only finitely many nonzero terms, we can write our polynomials as

$$p = \sum_{i=0}^{k} a_i x^i \quad \text{and} \quad q = \sum_{j=0}^{l} b_j x^j$$

for some k and l, with the "leading" coefficients a_k and b_l nonzero. So we have $\deg(p) = k$ and $\deg(q) = l$.

Now, to see the first statement, suppose that $k \geq l$: then the sum $p + q$ has no terms of the form x^{k+1}, x^{k+2}, and so on. So its degree is $\deg(p+q) \leq k = \max\{k, l\}$. We argue similarly if $l > k$.

For the second statement, the term of highest degree in pq is $a_k b_l x^{k+l}$. Since a_k and b_l are nonzero, so is their product $a_k b_l$, as proved on Problem Sheet 1. □

There are many similarities between polynomial rings $K[x]$ and the ring of integers $\mathbf{Z}$. The next theorem is a good example of this: note how similar it is to the corresponding statement for integers.

Theorem 1.3 (Division theorem). *Let* f *and* g *be polynomials in* $K[x]$ *with* $g \neq 0$. *Then there exist* **unique** *polynomials* q *and* r *in* $K[x]$ *such that*

$$f = qg + r \quad \textit{and}$$
$$\deg(r) < \deg(g).$$

Notation: If the remainder r in the above formula is zero, we say that g **divides** f, and write $g \mid f$. In other words, "g divides f" means that $f = qg$ for some polynomial $q \in K[x]$.

Proof. First we prove that such q and r exist. If $\deg(f) < \deg(g)$, the claim is obvious: we can write

$$f = 0 \cdot g + f$$

and so the polynomials $q = 0$, $r = f$ do the job.

Now suppose $\deg(f) \geq \deg(g)$. Let's prove the claim by induction on the natural number $\deg(f)$. Suppose that we know that the statement is true for all polynomials f' with $\deg(f') < \deg(f)$. We want to deduce the statement for f. By induction, this will complete the proof of existence.

Suppose g has leading term $a_k x^k$, and f has leading term $b_l x^l$ (we have assumed that $l \geq k$). Consider the polynomial

$$f' = f - \left(\frac{b_l}{a_k}\right) x^{l-k} g.$$

By construction, the coefficient of x^l in f' is zero, so $\deg(f') < \deg(f)$. Now apply our induction hypothesis: then we can write

$$f' = q'g + r'$$

where $\deg(r') < \deg(g)$. But then

$$\begin{aligned} f &= f' + \left(\frac{b_l}{a_k}\right) x^{l-k} g \\ &= q'g + r' + \left(\frac{b_l}{a_k}\right) x^{l-k} g \\ &= \left(q' + \left(\frac{b_l}{a_k}\right) x^{l-k}\right) g + r'. \end{aligned}$$

So setting $q = q' + \left(\frac{b_l}{a_k}\right) x^{l-k}$ and $r = r'$, we have proved that the existence statement is true for f.

Finally we must prove that given f and g, there are *unique* q and r satisfying our conditions. To see this, suppose there were two such expressions:

$$\begin{aligned} f &= q_1 g + r_1 \\ &= q_2 g + r_2. \end{aligned}$$

with $\deg(r_1), \deg(r_2) < \deg(g)$. Subtracting gives

$$(q_1 - q_2)g = r_1 - r_2.$$

If $q_1 \neq q_2$ then the left-hand side has degree at least $\deg(g)$, while the right-hand side has degree at most $\max\{\deg(r_1), \deg(r_2)\} < \deg(g)$. This is a contradiction. So we must have $q_1 = q_2$, and hence also $r_1 = r_2$. $\square$

The Division Theorem gives a quick way to check whether a polynomial has a *linear* factor (i.e. a polynomial of degree 1 that divides it with zero remainder):

Corollary 1.4 (Factor Theorem)**.** *Let* $f \in K[x]$*, and let* $a \in K$ *be any element of the field* K*. Then* $(x - a) \mid f$ *if and only if* $f(a) = 0$*.*

Proof. By the Division Theorem there exists polynomials $q, r \in K[x]$ such that

$$f = (x - a)q + r \tag{1}$$

and $\deg(r) < \deg(x - a) = 1$. But this means that $\deg(r) \leq 0$. In other words r is just a constant polynomial, either $r = 0$ (in which case $\deg(r) = -\infty$) or $r \neq 0$ (in which case $\deg(r) = 0$).

Now substituting $x = a$ in Equation (1) gives $f(a) = r$. So we conclude that

$$(x - a) \mid f \;\Leftrightarrow\; r = 0 \;\Leftrightarrow\; f(a) = 0.$$

$\square$

1.1 Examples

Let's do some examples of division in polynomial rings. Notice that Theorem 1.3 is valid for $K[x]$ where K is any field. So for example we can divide polynomials whose coefficients are rational numbers, or elements of some finite field $\mathbf{Z}_p$.

1. **Division in** $\mathbf{Q}[x]$ Consider

$$\begin{aligned} f &= x^4 - 3x + 2 \\ g &= x^2 - 1 \end{aligned}$$

Let's find q and r with $f = qg + r$ and $\deg(r) < \deg(g)$.

We do this by polynomial long division:

$$\begin{array}{rl} & x^2 + 1 \\ \cline{2-2} x^2 - 1 \big) & x^4 - 3x + 2 \\ & -(x^4 - x^2) \\ \cline{2-2} & x^2 - 3x + 2 \\ & -(x^2 - 1) \\ \cline{2-2} & -3x + 3 \end{array}$$

At this point, our remainder $-3x + 3$ has degree 1, which is less than $\deg(g) = 2$, so we STOP.

We have

$$f = qg + r$$

where

$$\begin{aligned} q &= x^2 + 1 \\ r &= -3x + 3. \end{aligned}$$

2. **Division in $\mathbf{Z}_3[x]$** In this example we consider polynomials with coefficients in $\mathbf{Z}_3 = \{0, 1, 2\}$ and we do all our calculations modulo 3. So take

$$\begin{aligned} f &= x^5 + x^3 + x^2 + x \\ g &= x^2 + 2 \end{aligned}$$

Again let's find q and r with $f = qg + r$ and $\deg(r) < \deg(g)$, using polynomial long division. Here we are working in the ring $\mathbf{Z}_3[x]$, so all calculations should be done mod 3:

$$\begin{array}{rl}
 & \ x^3 + 2x + 1 \\
x^2+2 & \big)\overline{\ x^5 + x^3 + x^2 + x\ } \\
 & \ \ \underline{x^5 + 2x^3} \\
 & \qquad 2x^3 + x^2 + x \\
 & -\ \underline{(2x^3 + x)} \\
 & \qquad\qquad x^2 \\
 & \qquad -\ \underline{(x^2 + 2)} \\
 & \qquad\qquad\quad 1
\end{array}$$

At this point the remainder has degree 0, which is less than $\deg(g) = 2$, so we STOP.

We get

$$f = qg + r$$

where

$$\begin{aligned} q &= x^3 + 2x + 1 \\ r &= 1. \end{aligned}$$

2 Ideals in $K[x]$

Now that we have an interesting example of a ring, let's think about what ideals in this ring look like.

Week 1 Proposition 2.4 says that if $f : K[x] \to R$ is any homormorphism from $K[x]$ to another ring, then its kernel $\mathrm{Ker}(f)$ is an ideal in $K[x]$. One example of such homomorphisms is evaluation of polynomials, also known as "plugging in". To show this we first need a lemma:

Lemma 2.1 (Taylor expansion)**.** *Let K be a field and let $a \in K$ be an element. For any polynomial $p \in K[x]$ of degree n there exist elements $a_0, a_1, \dots, a_n \in K$ such that*

$$p = a_n(x-a)^n + a_{n-1}(x-a)^{n-1} + \cdots + a_0.$$

Proof. Let $a_0 = p(a)$. Then the polynomial $p_1 = p - a_0$ has the property that $p_1(a) = 0$. Hence by the Factor Theorem (Corollary 1.4) we see that $(x-a)$ divides p_1: that is,

$$\begin{aligned} p_1 &= (x-a)p_2 \qquad \text{for some } p_2 \in K[x], \text{ so} \\ p &= a_0 + (x-a)p_2 \end{aligned}$$

Repeating the process for p_2 we get

$$\begin{aligned} p_2 &= a_1 + (x-a)p_3 \qquad \text{and therefore} \\ p &= a_0 + a_1(x-a) + (x-a)^2 p_3 \end{aligned}$$

Continuing in this way we end up with an expression

$$p = a_0 + a_1(x-a) + \cdots a_n(x-a)^n + (x-a)^{n+1}q$$

for some polynomial q. But the left-hand side has degree n, therefore we must have $q = 0$, and so we have obtained the claimed expression for p. $\square$

Now we can prove that evaluation or "plugging in" really gives a homomorphism.

Proposition 2.2. *Let K be a field and let $a \in K$ be an element. Then the evaluation-at-a map*

$$\begin{aligned} \mathrm{ev}_a \colon K[x] &\to K \\ p &\mapsto p(a) \end{aligned}$$

is a ring homomorphism. Its kernel is the ideal

$$\langle x-a \rangle = \{p \in K[x] \mid p = (x-a)q \text{ for some } q \in K[x]\}.$$

In other words, the kernel of ev_a consists of exactly those polynomials $p \in K[x]$ such that $(x-a) \mid p$.

Proof. First we prove the map is a ring homomorphism. Let p, $q \in K[x]$ be two polynomials. By Lemma 2.1 we can expand them both in powers of $x - a$:

$$\begin{aligned} p &= a_0 + a_1(x-a) + \cdots + a_n(x-a)^n \\ q &= b_0 + b_1(x-a) + \cdots + b_m(x-a)^m \end{aligned}$$

Therefore we have

$$\begin{aligned} p + q &= a_0 + b_0 + (x-a)r \\ pq &= a_0 b_0 + (x-a)s \end{aligned}$$

for some polynomials r, $s \in K[x]$. Hence

$$\begin{aligned} \mathrm{ev}_a(p+q) &= (p+q)(a) \\ &= a_0 + b_0 \\ &= \mathrm{ev}_a(p) + \mathrm{ev}_a(q) \end{aligned}$$

and

$$\begin{aligned} \mathrm{ev}_a(pq) &= (pq)(a) \\ &= a_0 b_0 \\ &= \mathrm{ev}_a(p) \cdot \mathrm{ev}_a(q) \end{aligned}$$

Finally

$$\mathrm{ev}_a(1) = 1$$

So the map ev_a is a ring homomorphism.

To prove the statement about the kernel, since $p(a) = a_0$, we see that $p \in \mathrm{Ker}(\mathrm{ev}_a)$ if and only if $a_0 = 0$, in other words if p is of the form

$$\begin{aligned} p &= a_1(x-a) + \cdots + a_n(x-a)^n \\ &= (x-a)\left(a_1 + \cdots + a_n(x-a)^{n-1}\right) \end{aligned}$$

So the elements of $\mathrm{Ker}(\mathrm{ev}_a)$ are exactly those polynomials p such that $(x-a) \mid p$ as claimed. $\square$

Let's give a formal definition of the notation we used in the statement of this proposition.

Definition 2.3. *Let* R *be a commutative ring and let* $a_1, \ldots, a_n$ *be a finite set of elements in* R. *Then the subset* $\langle a_1, \ldots, a_n \rangle \subset R$ *defined as follows:*

$$\langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$$

is called the **ideal generated** *by the elements* $a_1, \ldots, a_n$.

Of course, for this definition to make sense, we need to be able to show that the set $\langle a_1, \dots, a_n \rangle$ as defined above actually is an ideal:

Proposition 2.4. *The set* $\langle a_1, \dots, a_n \rangle$ *as defined above is an ideal of* R*.*

Proof. Denote this set by I. We have to show that I satisfies the definition of an ideal from Week 1. First taking each r_i equal to 0, we see that 0 belongs to the set I. Next, we need to show that I is closed under addition. Let's take two elements of I, say

$$\begin{aligned} a &= r_1 a_1 + \cdots + r_n a_n, \\ b &= s_1 a_1 + \cdots + s_n a_n. \end{aligned}$$

Then

$$a + b = (r_1 + s_1)a_1 + \cdots + (r_n + s_n)a_n$$

which is again of the right form to be an element of I.

To complete the proof that I is an ideal, we need to show that for $a \in I$ and $r \in R$ we have $ra \in I$. But if as before we have $a = r_1 a_1 + \cdots + r_n a_n$, and an arbitrary element $r \in R$, then

$$ra = (rr_1)a_1 + \cdots + (rr_n)a_n$$

which again has the correct form to be an element of I. This completes the proof that I is an ideal as claimed. $\square$

There is an equivalent way to define $\langle a_1, \dots, a_n \rangle$: namely, it is the smallest ideal in R that contains all the a_i. See Problem Sheet 2 Question 2 for more on this equivalence.

We finish by giving a complete description of ideals in the polynomial ring $K[x]$: every ideal is generated by a **single element**. Rings with this property are called *principal ideal domains*; we will return to them later in the module, time permitting.

Theorem 2.5. *Let* K *be any field, and* $K[x]$ *the ring of polynomials with coefficients in* K*. If* $I \subset K[x]$ *is an ideal, there exists a polynomial* $f \in K[x]$ *such that* I *is generated by* f*, in other words*

$$I = \langle f \rangle .$$

Moreover two polynomials generate the same ideal if and only if they differ by a nonzero constant multiple:

$$\langle f \rangle = \langle g \rangle \Leftrightarrow f = kg \text{ for some } k \in K, k \neq 0.$$

Proof. First we prove that every ideal $I \in K[x]$ is generated by a single element. If $I = \{0\}$, the zero ideal, then it is generated by the zero polynomial $f = 0$. So we can assume I contains a nonzero polynomial.

Let us consider the following set of natural numbers:

$$D(I) = \{\deg(p) \mid p \in I, p \neq 0\}$$

Since I contains at least one nonzero polynomial, $D(I)$ is a nonempty set of natural numbers, so by the Least Integer Principle it has a smallest element d say. So every polynomial $g \in I$ has degree at least d. Choose any polynomial $f \in I$ with degree equal to d. We will show that $I = \langle f \rangle$.

To see this, suppose $g \in I$ is any polynomial. By the Division Theorem 1.3 we can divide g by f: we get

$$g = fq + r$$

for some q and some r such that $\deg(r) < \deg(f)$. We can rearrange the above equation as $r = g - fq$, and since f and g are both in the ideal I this shows r is in the ideal I. Since $\deg(r) < \deg(f)$ and f has the smallest degree among nonzero elements of I, we must have $r = 0$. That means $g = fq$, showing that $g \in \langle f \rangle$. Our argument is valid for any element $g \in I$, so we have proved $I = \langle f \rangle$ as claimed. Finally suppose $\langle f \rangle = \langle g \rangle$. This means that there exist polynomials p, q such that

$$g = pf \text{ and } f = qg.$$

Putting these together we get $f = qpf$. Comparing the degrees of the two sides using Lemma 1.2, we get

$$\deg(f) = \deg(q) + \deg(p) + \deg(f)$$

so this can only happen if both q and p are nonzero polynomials of degree 0, in other words nonzero constant polynomials. □

2.1 Example

In the ring $\mathbf{Q}[x]$ consider the two polynomials

$$f = x^3 - 3x - 1$$
$$g = x^2 - 2$$

Let's try to find a polynomial $p \in \mathbf{Q}[x]$ such that

$$\langle f, g \rangle = \langle p \rangle .$$

According to the proof of Theorem 2.5, we can take p to be any nonzero polynomial of least degree in $\langle f, g \rangle$.

We see that f and g have degrees 3 and 2 respectively, so the least degree of a nonzero element can be at most 2. Can we find an element $p \in \langle f, g \rangle$ of degree 0 or 1?

The Division Theorem 1.3 says we can divide f by g and get a remainder of smaller degree. Let's divide:

$$
\begin{array}{r l}
 & x \\
x^2-2 \,\big) & x^3-3x-1 \\
 & \underline{x^3-2x} \\
 & \quad -x-1
\end{array}
$$

So we obtain $r = -x - 1$.

Note that $r = f - qg$, so by Definition 2.3 the remainder r is an element of the ideal $\langle f,\, g\rangle$, with degree 1.

Can we find an element of degree 0, in other words a constant, in $\langle f,\, g\rangle$? Let's divide again, this time dividing g by r: the Division Theorem tells us we will get

$$g = q'r + r'$$

with $\deg(r') < \deg(r)$. Dividing:

$$
\begin{array}{r l}
 & -x+1 \\
-x-1 \,\big) & x^2-2 \\
 & \underline{-(x^2+x)} \\
 & \quad -x-2 \\
 & \quad \underline{-(-x-1)} \\
 & \qquad -1
\end{array}
$$

So we end up with $r' = -1$.

Again we have

$$
\begin{aligned}
r' = g - q'r &= g - q'(f - qg) \\
&= -q'f + (1 + q)g
\end{aligned}
$$

which again is an element of $\langle f,\, g\rangle$.

The polynomial r' has degree 0, which is the smallest degree of a nonzero polynomial, so we have

$$\langle f,\, g\rangle = \langle r'\rangle = \langle -1\rangle\,.$$

Notice that any polynomial $p \in \mathbf{Q}[x]$ can be written as $p = (-p)(-1)$, so in fact $\langle -1\rangle = \mathbf{Q}[x]$.

So $\langle f,\, g\rangle = \mathbf{Q}[x]$. This means that any polynomial $p \in \mathbf{Q}[x]$ can be written in the form

$$p = af + bg$$

for some $a,\, b \in \mathbf{Q}[x]$.

Next week: we'll generalise this example to any two polynomials f and g, by introducing the *greatest common divisor* and a method to compute it called the *Euclidean algorithm*.