Class 22

September 19, 2024

Polynomial Rings

Let R be a ring. Then $R[x] = \left\{\sum_{i=0}^{n} a_i x^i | a_i \in R, n \in \mathbb{Z}\right\}$ is the ring of polynomials over R in the indeterminate x. A few things to note

- We sometimes call x the variable (Especially when solving equations with polynomials)
- n can be as large as needed. If it isn't specified, we take n to be arbitrarily large. If not, closure becomes a problem.
- We often will focus on commutative rings, rings with unity, and fields.

We will define equality of polynomials as follows: for $p(x) = \sum_{i=0}^{n} p_i x^i,\ q(x) = \sum_{i=0}^{m} q_i x^i$, we say

$$p(x) = q(x)$$

if

$$p_i = q_i \ \forall i$$

The largest i such that $p_i \neq 0$ is the degree of $p(x)$. We set the higher order coefficients to 0. For the purposes of this class, we will assume that every polynomial has a finite degree (even though the sum in the polynomial definition will contain infinitely many 0 terms). In this polynomial ring, we define addition and multiplication as follows:

$$p(x) + q(x) = \sum_{i=0}^{\max\{n,m\}} (p_i + q_i) x^i$$

$$p(x) q(x) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} (p_j q_{i-j}) \right) x^i$$

Let's show this forms a ring!

Proof

First, let's show $R[x]$ is closed under addition and multiplication. Then

$$p_i + q_i \in R \ \forall i$$

as $p_i, q_i \in R$ and R is closed under addition, thus

$$p(x) + q(x) = \sum_{i=0}^{\max\{n,m\}} (p_i + q_i) x^i \in R[x]$$

Similarly, as R is closed under addition and multiplication:

$$\sum_{j=0}^{i} (p_j q_{i-j}) \in R \ \forall i$$

thus

$$p(x)\,q(x) = \sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(p_j q_{i-j})\right)x^i \in R[x]$$

Now, let's show each of the ring axioms. First, commutativity under addition:

$$p(x) + q(x) = \sum_{i=0}^{\max\{n,m\}}(p_i + q_i)\,x^i$$

as the elements of a ring commute under addition:

$$= \sum_{i=0}^{\max\{n,m\}}(q_i + p_i)\,x^i = q(x) + p(x)$$

Now, let's show that we have associativity under addition. Let $r(x) = \sum_{i=0}^{k} r_i x^i$. Then

$$(p(x) + q(x)) + r(x) = \sum_{i=0}^{\max\{n,m\}}(p_i + q_i)\,x^i + \sum_{i=0}^{k}(r_i)\,x^i = \sum_{i=0}^{\max\{n,m,k\}}((p_i + q_i) + r_i)\,x^i$$

as R has associativity under addition:

$$= \sum_{i=0}^{\max\{n,m,k\}}(p_i + (q_i + r_i))\,x^i = \sum_{i=0}^{n} p_i x^i + \sum_{i=0}^{\max\{m,k\}}(q_i + r_i)\,x^i = p(x) + (q(x) + r(x))$$

Now, for additive identity and inverse. Let $0 = \sum_{i=0}^{n} 0x^i$. Then

$$p(x) + 0 = \sum_{i=0}^{n}(p_i + 0)\,x^i = \sum_{i=0}^{n} p_i x^i = p(x)$$

We will define the additive inverse as $-p(x) = \sum_{i=0}^{n} -p_i x^i$. As R is a ring, then $-p_i \in R\ \forall i$, thus

$$p(x) + (-p(x)) = \sum_{i=0}^{n}(p_i + -p_i)\,x^i = \sum_{i=0}^{n} 0x^i = 0$$

Now that we have shown all of the addition axioms, let's show the multiplication axioms. First, associativity:

$$(p(x)\,q(x))\,r(x) = \left(\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(p_j q_{i-j})\right)x^i\right)\left(\sum_{i=0}^{k} r_i x^i\right)$$

$$= \sum_{i=0}^{n+m+k}\left(\sum_{j=0}^{i}\left(\sum_{l=0}^{j}(p_k q_{j-l})\right)r_{i-j}\right)x^i$$

Distribute

$$= \sum_{i=0}^{n+m+k}\left(\sum_{j=0}^{i}\left(\sum_{l=0}^{j}(p_l q_{j-l} r_{i-j})\right)\right)x^i = \sum_{i=0}^{n+m+k}\left(\sum_{j=0}^{i}\left(\sum_{l=0}^{j} p_l\,(q_{j-l} r_{i-j})\right)\right)x^i$$

For these sums, the important thing is that the sum of the indices $k, j-k, i-j$ is always equal to i. We can re-index these to get the equivalent expression:

$$= \sum_{i=0}^{n+m+k}\left(\sum_{j=0}^{i}\left(\sum_{l=0}^{j} p_{i-j}\,(q_{j-l} r_l)\right)\right)x^i = \sum_{i=0}^{n+m+k}\left(\sum_{j=0}^{i} p_{i-j}\left(\sum_{l=0}^{j}(q_{j-l} r_l)\right)\right)x^i$$

$$= \sum_{i=0}^{n+m+k} \left(\sum_{j=0}^{i} p_{i-j} \left(\sum_{l=0}^{j} \left(q_l r_{j-l} \right) \right) \right) x^i$$

Now, after re-indexing we can use the definition of multiplication of polynomials:

$$= \left(\sum_{j=0}^{i} p_i x^i \right) \left(\sum_{i=0}^{m+k} \left(\sum_{j=0}^{i} \left(q_j r_{i-j} \right) \right) x^i \right) = p(x) \left(q(x) r(x) \right)$$

Now, we will show the distributive laws.

$$p(x) \left(q(x) + r(x) \right) = \left(\sum_{i=0}^{n} p_i x^i \right) \left(\sum_{i=0}^{\max\{m,k\}} \left(q_i + r_i \right) x^i \right)$$

$$= \sum_{i=0}^{n+\max\{m,k\}} \left(\sum_{j=0}^{i} p_j \left(q_{i-j} + r_{i-j} \right) \right) x^i = \sum_{i=0}^{n+\max\{n,k\}} \left(\sum_{j=0}^{i} \left(p_j q_{i-j} + p_j r_{i-j} \right) \right) x^i$$

Break up the sums

$$= \sum_{i=0}^{n+\max\{n,k\}} \left(\sum_{j=0}^{i} p_j q_{i-j} + \sum_{j=0}^{i} p_j r_{i-j} \right) x^i$$

Distribute the x^i

$$= \sum_{i=0}^{n+\max\{n,k\}} \left(\sum_{j=0}^{i} p_j q_{i-j} x^i + \sum_{j=0}^{i} p_j r_{i-j} x^i \right) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} p_j q_{i-j} \right) x^i + \sum_{i=0}^{n+k} \left(\sum_{j=0}^{i} p_j r_{i-j} \right) x^i$$

$$= p(x) q(x) + p(x) r(x)$$

Similarly, we can show the right distributive law. Thus $R[x]$ is a ring.

Thm

If D is an integral domain, then $D[x]$ is an integral domain.

Proof

We need to show $D[x]$ has a unity, $D[x]$ is commutative under multiplication, and $D[x]$ has no zero divisors. First, let's show $D[x]$ has a unity. Let 1 be the unity in D. Then

$$1 = 1x^0 + 0x^1 + 0x^2 + \ldots = \sum_{i=0}^{n} c_i x^i$$

Let $p(x) = \sum_{i=0}^{n} p_i x^i$. Then

$$1p(x) = \sum_{i=0}^{n+0} \left(\sum_{j=0}^{i} \left(c_j p_{i-j} \right) \right) x^i$$

as $c_i = 0$ for all $i \neq 0$, then

$$= \sum_{i=0}^{n} \left(c_0 p_i \right) x^i = \sum_{i=0}^{n} \left(1 p_i \right) x^i = \sum_{i=0}^{n} p_i x^i = p(x)$$

Thus $D[x]$ has a unity. Now, let's show commutativity under multiplication. Let $q(x) = \sum_{i=0}^{m} q_i x^i$

$$p(x)\,q(x)=\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(p_jq_{i-j})\right)x^i=\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(q_{i-j}p_j)\right)x^i$$

re-index the p,q terms

$$=\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(q_jp_{i-j})\right)x^i=q(x)\,p(x)$$

Thus $D[x]$ is commutative under multiplication. Now, let's show $D[x]$ has no zero divisors. Suppose $p(x),q(x)\in D[x]$ such that $p(x),q(x)\neq 0$. Suppose that $p(x)$ and $q(x)$ have degrees n and m respectively. Then

$$p(x)\,q(x)=\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(p_jq_{i-j})\right)x^i$$

Consider the x^{n+m} term:

$$\sum_{j=0}^{n+m}(p_jq_{i-j})=p_nq_m$$

as $p_i=0\ \forall i>n,\ q_i=0\ \forall i>m$. As $p_nq_m\neq 0$, then $p_nq_m\neq 0$ as D is an integral domain. Thus

$$\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(p_jq_{i-j})\right)x^i\neq 0$$

as $p_nq_mx^{n+m}\neq 0x^{n+m}$. As we have shown $D[x]$ satisfies all three properties, then $D[x]$ is an integral domain.

Division

Recall that for any two integers a,b there exist unique integers r,n such that $0\leq r<|b|$ and

$$a=nb+r$$

We call r the remainder. If $r=0$, then we say b is a factor of a. A similar statement exists for polynomials over fields.

Thm

Let F be a field and let $f(x),g(x)\in F[x]$, where $g(x)\neq 0$. Then there exists unique $q(x),r(x)\in F[x]$ such that

$$f(x)=q(x)\,g(x)+r(x)$$

and such that $r(x)=0$ or $\deg r(x)<\deg g(x)$.

Pf

For convenience, let $f(x)=\sum_{i=0}^{n}f_ix^i$, $g(x)=\sum_{i=0}^{m}g_ix^i$, $q(x)=\sum_{i=0}^{\infty}g_ix^i$ If $f(x)=0$ or $\deg f(x)<\deg g(x)$, then we take $q(x)=0$ and let $r(x)=f(x)$, thus

$$f(x)=0*g(x)+f(x)=f(x)$$

This is analogous to taking $\frac{a}{b}$ when $a<b$. If so, we get 0 remainder a. To get the more interesting case, suppose $\deg f(x)\geq\deg g(x)$. Then we can prove this statement using induction. For convenience, let $\deg f(x)=n,\deg g(x)=m$. Then the base case is the case where $n=0$. This means $f(x)=f_0\in F$. Thus $g(x)=g_0\in F$. This yields the equation

$$f_0=q(x)\,g_0+r(x)$$

If we set $r = 0$, then

$$f_0 = q(x) g_0$$

further, as $g(x) \neq 0$, then $g_0 \neq 0$ and $q(x) = q_0 \in F$.

$$f_0 = q_0 g_0$$

as every non-zero element in a field has an inverse, we can find q_0.

$$f_0 g_0^{-1} = q_0$$

Thus we have found $q(x) = q_0, r(x) = 0$. Now, for the induction step, suppose this claim holds for all $0 \leq k < n$. Then we can let

$$F_1(x) = f(x) - f_n g_m^{-1} x^{n-m} g(x)$$

The idea here is to subtract the highest degree term from $f(x)$. Here, we have two cases. If $F_1(x) = 0$, then

$$0 = f(x) - f_n g_m^{-1} x^{n-m} g(x)$$

$$g(x) = \left(f_n g_m^{-1} x^{n-m}\right) g(x) + 0$$

Thus $r(x) = 0$. If $F_1(x) \neq 0$, then $\deg F_1(x) < n$, thus

$$F_1(x) = Q_1(x) g(x) + R_1(x)$$

for some $Q_1(x) \in F[x]$ and some $R_1(x)$ such that $R_1(x) = 0$ or $\deg R_1(x) < m$. If we substitute for $F_1(x)$

$$F_1(x) = f(x) - f_n g_m^{-1} x^{n-m} g(x)$$

$$Q_1(x) g(x) + R_1(x) = f(x) - f_n g_m^{-1} x^{n-m} g(x)$$

$$f(x) = Q_1(x) g(x) + R_1(x) + f_n g_m^{-1} x^{n-m} g(x)$$

$$f(x) = \left(Q_1(x) + f_n g_m^{-1} x^{n-m}\right) g(x) + R_1(x)$$

Thus $q(x) = Q_1(x) + f_n g_m^{-1} x^{n-m}$ and $R_1(x) = r(x)$ and $r(x) = 0$ or $\deg r(x) < m$. Now, let's prove uniqueness. Suppose

$$f(x) = q_1(x) g(x) + r_1(x)$$

$$f(x) = q_2(x) g(x) + r_2(x)$$

such that $q_1(x), q_2(x), r_1(x), r_2(x) \in F[x]$ such that $r_1(x) = 0$ or $\deg r_1(x) < m$ and $r_2(x) = 0$ or $\deg r_2(x) < m$. Then, we can set equations equal to each other to yield:

$$q_1(x) g(x) + r_1(x) = q_2(x) g(x) + r_2(x)$$

We can rearrange to yield

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

This yields one of two cases. Case 1, suppose $r_2(x) \neq r_1(x)$. Then

$$\deg(r_2(x) - r_1(x)) \leq \max\{\deg r_1(x), \deg r_1(x)\} < m$$

but

$$\deg\left(\left(q_1\left(x\right)-q_2\left(x\right)\right)g\left(x\right)\right)\geq \deg g\left(x\right)=m$$

thus

$$\deg\left(r_2\left(x\right)-r_1\left(x\right)\right)\neq \deg\left(\left(q_1\left(x\right)-q_2\left(x\right)\right)g\left(x\right)\right)$$

and $\left(q_1\left(x\right)-q_2\left(x\right)\right)g\left(x\right)\neq r_2\left(x\right)-r_1\left(x\right)$! To avoid contradiction, suppose

$$r_2\left(x\right)-r_1\left(x\right)=0$$

Then

$$r_2\left(x\right)=r_1\left(x\right)$$

and

$$\left(q_1\left(x\right)-q_2\left(x\right)\right)g\left(x\right)=0$$

As F is a field (and thus an integral domain), then $F\left[x\right]$ is an integral domain, thus

$$q_1\left(x\right)-q_2\left(x\right)=0 \text{ or } g\left(x\right)=0$$

but we are assuming that $g\left(x\right)\neq 0$, thus

$$q_1\left(x\right)-q_2\left(x\right)=0$$

and thus

$$q_1\left(x\right)=q_2\left(x\right)$$

So we get uniqueness.