4.6 Polynomials over the Rationals

In this section we look at polynomials over the rational field $\mathbb{Q}$, which have a number of interesting and useful properties.

Our first lemma says that, except for multiplication by a constant rational factor, when considering polynomials over $\mathbb{Q}$ it suffices to consider polynomials with integer coefficients.

Lemma
If $f \in \mathbb{Q}[x]$, then we can write

$$f(x) = \frac{u}{m}\left(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n\right)$$

where $u, m, a_0, \ldots, a_n$ are integers, u, m are relatively prime (i.e., $\frac{u}{m}$ is in lowest terms) and $a_0, \ldots, a_n$ are relatively prime (no common factors).

Proof: Exercise (or see text).

Idea: We know that, by definition,

$$f(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_n}{c_n}x^n.$$

Find a common denominator & cancel all common factors.

Now we need a lemma on the relationships between $R[x]$, $I[x]$, & $(R/I)[x]$, where I is an ideal in a ring R.

To motivate this result, recall that R/I is the set of cosets of I:

$$R/I = \{a+I : a \in R\}.$$

This is a ring, so we can consider polynomials over this ring. In particular, if p is a polynomial in $(R/I)[x]$, then by definition

$$p(x) = (a_0+I) + (a_1+I)x + \cdots + (a_n+I)x^n \qquad (*)$$

for some $n \geq 0$ & $a_0+I, \ldots, a_n+I \in R/I$.

On the other hand, if (as we will see) $I[x]$ is an ideal in $R[x]$, then we can also consider the polynomial ring $R[x]/I[x]$. The elements of this ring are the cosets of $I[x]$:

$$R[x]/I[x] = \{f + I[x] : f \in R[x]\}.$$

Thus, a typical (i.e., generic) element of $R[x]/I[x]$ has the form

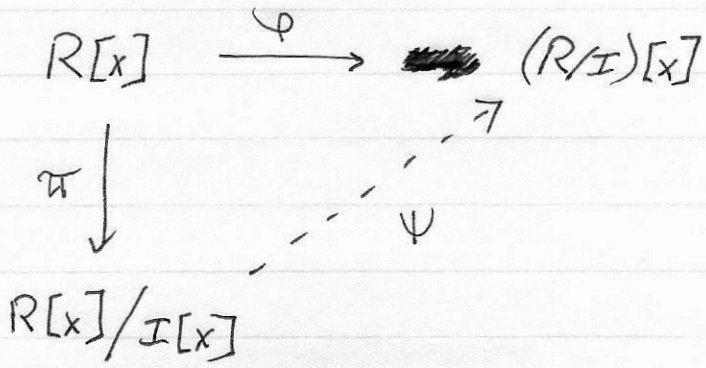
$$a_0 + a_1x + \cdots + a_nx^n + I[x] \qquad (**)$$

where $a_0, \ldots, a_n \in R$.

Clearly (didn't I tell you to never use this word?) there is a relationship between the polynomials appearing in (*) & (**): Each choice of $a_0, \ldots, a_n \in R$ determines a polynomial in $(R/I)[x]$ of the form given in (*), and also determines a polynomial in $R[x]/I[x]$ of the form given in (**).

However, because there are quotients involved, we do <u>not</u> know that each choice of $a_0, \ldots, a_n \in R$ gives a <u>unique</u> polynomial in either (*) or (**). For example, in (*), the constant polynomials $a_0 + I$ & $b_0 + I$ will be equal if $a_0 - b_0 \in I$.

Still, this does suggest a relationship between $(R/I)[x]$ & $R[x]/I[x]$. How do we prove this? The first ring, $(R/I)[x]$ is not a quotient ring (it is a ring of polynomials <u>over</u> a quotient ring), but the second ring, $R[x]/I[x]$ <u>is</u> a quotient ring. This suggests trying to use the First Homomorphism Theorem:



And, we already have a candidate for φ: we've said that each choice of $a_0, \dots, a_n \in R$, i.e., each choice of polynomial $a_0 + \cdots + a_n x^n \in R[x]$ determines an element $(a_0+I) + \cdots + (a_n+I)x^n \in (R/I)[x]$. So, we know what φ is, and therefore we just have to show that φ is a surjective homomorphism with kernel $I[x]$. Well, and one more thing: we do have to show first that $I[x]$ is actually an ideal in $R[x]$. This can either be done directly, or as a consequence of implementing the First Homomorphism Theorem: if we show $I[x]$ is the kernel of a homomorphism, then we know it is an ideal.

Exercise

Show directly that if I is an ideal in a ring R, then

$$I[x] = \{ a_0 + a_1 x + \cdots + a_n x^n : n \geq 0,\ a_0, \dots, a_n \in I \}$$

is an ideal in $R[x]$.

Theorem

If I is an ideal in a ring R then $I[x]$ is an ideal in $R[x]$, and

$$R[x]/I[x] \cong (R/I)[x].$$

Proof:

Define

$$\varphi: R[x] \longrightarrow (R/I)[x]$$

$$\varphi(a_0 + a_1x + \cdots + a_nx^n) = (a_0+I) + (a_1+I)x + \cdots + (a_n+I)x^n.$$

Exercise: Show that φ is a surjective homomorphism.

So, we just have to show that $\ker(\varphi) = I[x]$.

Note that the zero element of R/I is the coset $0+I = I$, so the zero polynomial in $(R/I)[x]$ is the constant polynomial $0+I = I$.

Suppose that $p(x) = a_0 + a_1x + \cdots + a_nx^n \in I[x]$.

Then, by definition, $a_0, \ldots, a_n \in I$. Hence each $a_i + I = I$, so

$$\varphi(p) = (a_0+I) + (a_1+I)x + \cdots + (a_n+I)x^n$$

$$= (0+I) + (0+I)x + \cdots + (0+I)x^n$$

$$= 0+I.$$

Thus $p \in \ker(\varphi)$, so $I[x] \subseteq \ker(\varphi)$.

On the other hand, if $p \in \ker(\varphi)$ and $p(x) = a_0 + a_1x + \cdots + a_nx^n$ where $a_0, \ldots, a_n \in R$, then

$$0+I = \varphi(p)$$

$$= (a_0+I) + (a_1+I)x + \cdots + (a_n+I)x^n$$

Therefore each a_i+I is the zero element in R/I, i.e., $a_i + I = 0+I$ for $i = 0, \ldots, n$. Hence each $a_i \in I$, so $p \in I[x]$. Thus $\ker(\varphi) \subseteq I[x]$.

The First Homomorphism Theorem therefore implies that $R[x]/I[x] \cong (R/I)[x]$. ∎

One use of this theorem is the following result.

Corollary
Let $p \in \mathbb{N}$ be prime. Then

$$\mathbb{Z}[x]/(p\mathbb{Z})[x] \cong \mathbb{Z}_p[x]$$

Note that $p\mathbb{Z}[x]$ is the ring of polynomials over $p\mathbb{Z}$, ie., it contains all polynomials whose coefficients are integer multiples of p.

Proof:
$p\mathbb{Z} = (p) = I$ is the principal ideal in $\mathbb{Z}$ generated by p. Since $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$, we therefore have by the preceding theorem that

$$\mathbb{Z}[x]/p\mathbb{Z}[x] \cong (\mathbb{Z}/p\mathbb{Z})[x] \cong \mathbb{Z}_p[x]. \quad \blacksquare$$

Exercise: What is the isomorphism here? (see next page)

Exercise

Prove the Corollary directly, by using the First Homomorphism Theorem.

Write

$$\mathbb{Z}_p = \{[0], [1], \dots, [p-1]\}$$

where $[a] = p\mathbb{Z} + a = \{pk + a : k \in \mathbb{Z}\}$

is the coset determined by a. Note that

$[a] = [a \bmod p]$, and that addition & multiplicatio in $\mathbb{Z}_p$ obey the rules

$$[a] + [b] = [a+b] = [(a+b) \bmod p]$$

$$[a][b] = [ab] = [ab \bmod p].$$

Define

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$

by

$$\varphi(a_0 + a_1 x + \cdots + a_n x^n) = [a_0] + [a_1]x + \cdots + [a_n]x^n$$

Show that φ is a surjective homomorphism whose kernel is $(p\mathbb{Z})[x]$. Conclude that

$$\mathbb{Z}[x] / p\mathbb{Z}[x] \cong \mathbb{Z}_p[x].$$

Example

Suppose $p = 7$ and let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ be the map constructed in the previous exercise. Then, for example,

$$\varphi(14 - 3x + 25x^2 - 49x^3)$$

$$= [14] + [-3]x + [25]x^2 + [-49]x^3$$

$$= [0] + [4]x + [4]x^2 + [0]x^3$$

$$= [4]x + [4]x^2.$$

The next result says that if a monic polynomial has integer coefficients, and if it can be factored as a product of two polynomials having rational coefficients, then it can be factored as a product of two polynomials having integer coefficients.

Theorem (Gauss' Lemma)

Let $f \in \mathbb{Z}[x]$ be a monic polynomial.

If f can be factored as $f = ab$ for some polynomials $a, b \in \mathbb{Q}[x]$, then

$$f = a_1 b_1$$

for some monic polynomials $a_1, b_1 \in \mathbb{Z}[x]$ with $\deg(a_1) = \deg(a)$ & $\deg(b_1) = \deg(b)$.

Proof:

Suppose $f \in \mathbb{Z}[x]$ is monic and $f = ab$ for some $a, b \in \mathbb{Q}[x]$. By an earlier result, we can write

$$a(x) = \frac{u_1}{v_1}(a_0 + a_1 X + \cdots + a_m X^m) = \frac{u_1}{v_1}\tilde{a}(x)$$

$$b(x) = \frac{u_2}{v_2}(b_0 + b_1 X + \cdots + b_n X^n) = \frac{u_2}{v_2}\tilde{b}(x)$$

where $a_0, \ldots, a_m$ are relatively prime

$b_0, \ldots, b_n$ are relatively prime

$a_m, b_n \neq 0$.

By changing the signs of u_1 & the a_i if necessary, we may assume $a_m > 0$. Likewise, we may assume $b_n > 0$.

Now write

$$f = ab = \frac{u_1 u_2}{v_1 v_2}\tilde{a}\tilde{b} = \frac{u}{v}\tilde{a}\tilde{b}$$

where u, v are relatively prime integers. Then

$$vf = u\tilde{a}\tilde{b}$$

where u, v are integers & $\tilde{a}, \tilde{b} \in \mathbb{Z}[x]$ satisfy

$\deg(a) = \deg(\tilde{a})$ & $\deg(b) = \deg(\tilde{b})$.

By replacing u, v with $-u, -V$ if necessary, we may assume $V > 0$.

Case 1: $V = 1$

In this case, since f is monic, the coefficient of X^{m+n} in Vf is 1. Looking at the same term in $u\tilde{a}\tilde{b}$, we see that

$$u a_m b_n = 1.$$

But u, a_m, b_n are integers & $a_m, b_n > 0$, so this implies $u = a_m = b_n = 1$. Hence $f = \tilde{a}\tilde{b}$ where $\tilde{a}, \tilde{b}$ are monic & have the required properties.

Case 2: $V > 1$

In this case, $\exists$ prime p s.t. $p \mid V$. Since u, v are relatively prime, $p \nmid u$. Also, since $a_0, \ldots, a_n$ are relatively prime they have no common prime factor. Hence p cannot divide all of $a_0, \ldots, a_n$, which means there is at least

one i such that $p \nmid a_i$. Likewise, there is at least one j s.t. $p \nmid b_j$.

Now consider the map

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$

$$\varphi(c_0 + c_1 x + \cdots + c_k x^k) = [c_0] + [c_1]x + \cdots + [c_k]x^k.$$

By an earlier exercise, φ is a surjective homomorphism with kernel $p\mathbb{Z}[x]$.

Now,

$$\begin{aligned} \varphi(vf) &= \varphi(v)\varphi(f) \\ &= [v]\,\varphi(f) \\ &= [0]\,\varphi(f) \quad \text{since } p \mid v \\ &= [0], \end{aligned}$$

i.e., $\varphi(vf)$ is the zero polynomial in $\mathbb{Z}_p[x]$.

On the other hand,

$$\varphi(u\tilde{a}\tilde{b}) = \varphi(u)\varphi(\tilde{a})\varphi(\tilde{b}).$$

Now, $p \nmid u$, so

$$\varphi(u) = [u] \neq [0].$$

Also, $p \nmid a_i$ so $\tilde{a} \notin p\mathbb{Z}[x]$, and ~~therefore~~

$$\varphi(\tilde{a}) = [a_0] + [a_1]x + \cdots + [a_m]x^m \neq [0]$$

Similarly, $p \nmid b_j$ so

$$\varphi(\tilde{b}) = [b_0] + [b_1]x + \cdots + [b_n]x^n \neq [0].$$

Hence $\varphi(u), \varphi(\tilde{a}), \varphi(\tilde{b}) \neq [0]$, the zero element of $\mathbb{Z}_p[x]$. Since $\mathbb{Z}_p$ is a field, we know that $\mathbb{Z}_p[x]$ is an integral domain, so this implies

$$\varphi(u\tilde{a}\tilde{b}) = \varphi(u)\varphi(\tilde{a})\varphi(\tilde{b}) \neq [0].$$

But this contradicts the fact that

$$\varphi(u\tilde{a}\tilde{b}) = \varphi(vf) = [0].$$

Hence this case cannot occur. ▨

For general fields F, it can be very difficult to construct polynomials in $F[x]$ of degree n that we know are irreducible. This is the case even for $\mathbb{Z}_p[x]$. However, in $\mathbb{Q}[x]$, the next result tells us there are irreducible polynomials of arbitrarily high degree.

Theorem (Eisenstein Criteria)

Let [redacted]

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

is a monic polynomial in $\mathbb{Z}[x]$. If $\exists$ prime p s.t.

$$p \mid a_0, \ldots, a_{n-1} \quad \text{but} \quad p^2 \nmid a_0$$

then f is irreducible in $\mathbb{Q}[x]$.

Proof:

Suppose that $f = uv$ where $u, v \in \mathbb{Q}[x]$ satisfy $\deg(u), \deg(v) \geq 1$. By Gauss' Lemma, we can assume that u, v are monic polynomials in $\mathbb{Z}[x]$.

By an earlier result,

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$

$$\varphi(c_0 + c_1 x + \cdots + c_m x^m) = [c_0] + [c_1]x + \cdots + [c_m]x^m$$

is a surjective homomorphism with kernel $p\mathbb{Z}[x]$.

Since $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ and $p \mid a_0, \ldots, a_{n-1}$, we have

$$\varphi(f) = [a_0] + [a_1]x + \cdots + [a_{n-1}]x^{n-1} + [1]x^n$$

$$= x^n$$

On the other hand, $\varphi(uv) = \varphi(u)\varphi(v)$, so we have

$$x^n = \varphi(u)\varphi(v).$$

Exercise: Show that this implies that

$\varphi(u) = x^s$ and $\varphi(v) = x^t$ where $1 \le s, t \le n-1$ & $s+t = n$.

Abusing notation, since $\varphi(x^s) = x^s$, we have

$\varphi(u - x^s) = \varphi(u) - \varphi(x^s) = x^s - x^s = 0$, so

$u - x^s \in \ker(\varphi) = p\mathbb{Z}[x]$. Hence $u(x) - x^s$ is a polynomial each of whose coefficients is divisible by p, or in other words $u(x) - x^s = pg(x)$ for some $g \in \mathbb{Z}[x]$. Thus

$$u(x) = x^s + pg(x)$$

and similarly

$$v(x) = x^t + ph(x)$$

for some $g, h \in \mathbb{Z}[x]$. Write

$$g(x) = g_0 + g_1 x + \cdots + g_j x^j$$

$$h(x) = h_0 + h_1 x + \cdots + h_k x^k$$

Then

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

$$= f(x)$$

$$= u(x)\, v(x)$$

$$= \left(x^s + p\,g(x)\right)\left(x^t + p\,h(x)\right)$$

$$= x^{s+t} + p x^t g(x) + p x^s h(x) + p^2 g(x) h(x)$$

Now, none of x^{s+t}, $p x^t g(x)$, $p x^s h(x)$ has any constant terms (since $s, t \geq 1$). The constant term in $p^2 g(x) h(x)$ is $p^2 g_0 h_0$. Therefore

$$a_0 = p^2 g_0 h_0.$$

But g_0, h_0 are integers, so we have $p^2 \mid a_0$, which contradicts the hypotheses on f. Hence f must be irreducible. ∎

Examples

a. Let $k_1, \ldots, k_{n-1}$ be any integers & let p be a prime. Then

$$f(x) = p + k_1 p x + \cdots + k_{n-1} p x^{n-1} + x^n$$

is irreducible in $\mathbb{Q}[x]$

b. Sometimes we can make some changes of variable that allow us to apply the Eisenstein criterion. For example, consider

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

The Eisenstein criterion does not apply. Consider, however, the polynomial

$$g(x) = f(x+1) = (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1$$

$$= x^4 + 5x^3 + 10x^2 + 10x + 5$$

The Eisenstein criterion applied to g using $p=5$ implies that g is irreducible.

Exercise: Show this implies that f is irreducible.

Exercise: Generalize this. Show that if p is prime

Then $$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible in $\mathbb{Q}[x]$ (use the same trick & apply the binomial theorem to $(x+1)^k$).

c. Here is another change of variables example. Consider

$$f(x) = 5x^4 - 7x^3 + 7.$$

f is not monic, but consider

$$5^3 f(x) = 5^4 x^4 - 7 \cdot 5^3 x^3 + 7 \cdot 5^2 \cdot 5$$

$$= (5x)^4 - 7(5x)^3 + 875$$

$$= y^4 - 7y^3 + 875$$

$$= h(y)$$

where $y = 5x$. Using $p = 7$, show that Eisenstein implies that h is irreducible. Then show that this implies that f itself is irreducible.