4.5 Polynomial Rings

Let R be a ring, and let x be a "formal variable"

A **polynomial in x over R** is a formal expression of the form

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$ ← the coefficients are ring elements

where $n \geq 0$ (and is finite) and $a_0, a_1, \ldots, a_n \in R$.

Note

Each polynomial p determines a function that maps R to R, but it is important to distinguish between the polynomial p & the function it determines.

Example $\mathbb{Z}_2 = \{0, 1\}$

Let $R = \mathbb{Z}_2$. Consider the polynomials

$$p(x) = x^2 + x + 1 \quad \& \quad q(x) = 1.$$

They are different polynomials. However, the functions they determine are equal, since

$p: \mathbb{Z}_2 \to \mathbb{Z}_2$ $\quad p(0) = 1 = q(0)$

$q: \mathbb{Z}_2 \to \mathbb{Z}_2$ $\quad p(1) = 1 = q(1)$

so $p(k) = q(k)$ for all $k \in \mathbb{Z}_2$.

To be more precise, polynomials

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \qquad a_0, a_1, \ldots, a_n \in R$$

and

$$q(x) = b_0 + b_1 x + \cdots + b_n x^n \qquad b_0, b_1, \ldots, b_n \in R$$

are <u>equal</u> if & only if $a_k = b_k$ for $k = 0, \ldots, n$.

The polynomials p & q also determine functions, that we also call p & q, that map $R \to R$. These functions are equal if

$$p(r) = a_0 + a_1 r + \cdots + a_n r^n$$

equals

$$q(r) = b_0 + b_1 r + \cdots + b_n r^n$$

for all $r \in R$. As we have seen,

p & q are equal polynomials $\Longrightarrow$ $\not\Longleftarrow$ p & q are equal functions.

Definition

The degree of a polynomial p is the integer $n \geq 0$ such that

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \text{ with } a_n \neq 0.$$

We write $\deg(p) = n$.

Note that the zero polynomial has no degree.

We declare that $\deg(0) = -\infty$.

Example: A constant polynomial is $p(x) = a_0$ with $a_0 \in R$
If $a_0 \neq 0$ then $\deg(p) = 0$

Example

If R is a ring with identity, then $k = k \cdot 1 \in R$ for $k = 1 + \cdots + 1$ (k times)

all $k \in \mathbb{Z}$. Then

Example: In $\mathbb{Z}_3$, $3x^2 - 2x + 1 = -2x + 1 = x + 1$ so in this case the degree is 1, not 3

→ $p(x) = 3x^2 - 2x + 1$ has $\deg(p) = 2$ if $3 \neq 0$

$p(x) = 0x^2 + 3x - 4$ has $\deg(p) = 1$ if $3 \neq 0$

Example: In $\mathbb{Z}_8$ we have $8 = 0$, so $p(x)$ is the zero polynomial

→ $p(x) = 8$ has $\deg(p) = 0$ if $8 \neq 0$

$p(x) = 0$ has $\deg(p) = -\infty$

Note

If
$$p(x) = a_0 + a_1 x + \cdots + a_m x^m$$
and
$$q(x) = b_0 + b_1 x + \cdots + b_n x^n$$
are two polynomials with $m < n$. Note that when we write this, we don't know that $a_m \neq 0$ or $b_n \neq 0$. Further, by setting $a_{m+1} = \cdots = a_n = 0$, we can write

Pad p with extra zero terms so that is has the same number of coefficients as q

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

Thus given two polynomials we can always write them using the same number of coefficients, although some of these coefficients may be zero.

Exercise

If $r \in R$, then there is a polynomial that we also call r, defined by

$$r(x) = r.$$

If $r \neq 0$ then this polynomial has degree 0

This is really another abuse of notation, since there are two different r's here: one is an element of R, and one is a "constant polynomial" taking the value r. We use the same letter for both & distinguish between the two by context.

Accepting this abuse of notation, we have

~~Let~~ that every element of R is also a polynomial.

Definition

If R is a ring then

$$R[x] = \{p : p \text{ is a polynomial in } x \text{ over } R\}$$

$$= \{p(x) = a_0 + a_1 x + \cdots + a_n x^n : n \geq 0,\ a_i \in R\}$$

Accepting the abuse of notation discussed above, we have

$$R \subseteq R[x].$$

Every ring element r determines a constant polynomial that we also call r.

Example

$3 \in \mathbb{Z}$ but also 3 determines a constant polynomial

$$3(x) = 3 = 3 + 0x + 0x^2 + \cdots + 0x^n$$

In this sense $3 \in \mathbb{Z}[x]$ and $\mathbb{Z} \subseteq \mathbb{Z}[x]$

Operations on $R[x]$

Suppose that R is a commutative ring. Then we define addition & multiplication on $R[x]$ as follows.

Addition

Given

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

and

$$q(x) = b_0 + b_1 x + \cdots + b_m x^m$$

pad with zero terms so both have the same number of terms →

Set $a_i = 0$ for $i > n$ & $b_i = 0$ for $i > m$. Then

$$(p+q)(x) = (a_0+b_0) + (a_1+b_1)x + \cdots + (a_k+b_k)x^k$$

add corresponding terms

where $k = \max\{m, n\}$.

In other words, we just add corresponding terms together.

Multiplication is a little more complicated to write down, but is exactly what it should be using the formal definition of the distributive laws, and collecting terms together.

Multiplication: Assume R is a commutative ring

Given

$$p(x) = a_0 + a_1 X + \cdots + a_m X^m$$

and

$$q(x) = b_0 + b_1 X + \cdots + b_n X^n,$$

we define $p(x)q(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots$

$$(pq)(x) = c_0 + c_1 X + \cdots + c_{m+n} X^{m+n}$$

where

$$c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_{k-i} b_i$$

Remark

The type of formula appearing in the definition of c_k is called a convolution of the a_i with b_j coefficients.

Try some examples to see how this works.

Exercise: Let R be a commutative ring.

a. $R[x]$ is a commutative ring.

b. If R has an identity, then so does $R[x]$.

Properties of the degree of a polynomial

Recall: If $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $a_n \neq 0$ then $\deg(p) = n$

Lemma
Let R be a commutative ring, and let p, q be nonzero polynomials.

a. $\deg(pq) \leq \deg(p) + \deg(q)$

b. If R is an integral domain, then

$$\deg(pq) = \deg(p) + \deg(q).$$

Proof:

Let $m = \deg(p)$ & $n = \deg(q)$. Then we can write

$$p(x) = a_0 + a_1 X + \cdots + a_m X^m \qquad a_m \neq 0$$

$$q(x) = b_0 + b_1 X + \cdots + b_n X^n \qquad a_n \neq 0$$

where $a_m \neq 0$ & $b_n \neq 0$. Then by definition

First and last coefficients

$c_0 = a_0 b_0$

$c_{m+n} = a_m b_n$

$$(pq)(x) = c_0 + c_1 X + \cdots + c_{m+n} X^{m+n}$$

could possibly have $c_{m+n} = a_m b_n = 0$!

The other coefficients aren't so easy

so $\deg(pq) \leq m+n$, and equality holds if $c_{m+n} \neq 0$. Now,

$$c_{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i} = a_m b_n \quad \text{(why?)}.$$

no zero divisors in an integral domain!
$ab = 0 \Rightarrow a = 0$ or $b = 0$

If R is an integral domain, then the fact that $a_m \neq 0$, $b_n \neq 0$ implies $c_{m+n} = a_m b_n \neq 0$, so $\deg(pq) = m + n$. ▨

Example
Let $R = \mathbb{Z}_6$. Then

$$p(x) = 2x + 1 \quad \text{and} \quad q(x) = 3x + 2$$

are nonzero polynomials in $\mathbb{Z}_6[x]$. We have

$$\deg(p) = 1 \quad \text{and} \quad \deg(q) = 1$$

but

$$(pq)(x) = (2x+1)(3x+2) = 0x^2 + 1x + 2$$

satisfies

$$\deg(pq) = 1 < 2 = \deg(p) + \deg(q).$$

Exercise
Show that in $\mathbb{Z}_{12}[x]$, $(1+6x)(1-6x) = 1$
and $(4x)(3x^3) = 0$
Thus $\mathbb{Z}_{12}[x]$ has zero divisors.

As a consequence, we have the following.

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

integral domain = commutative ring with no zero divisors

Proof:
We already know that $R[x]$ is a commutative ring, so we just have to show that it has no zero divisors. But if p, q are nonzero polynomials, then they each have $\deg(p) \geq 0$ & $\deg(q) \geq 0$, so pq is a polynomial with $\deg(pq) = \deg(p) + \deg(q) \geq 0$.

↑ because R is an integral domain

Hence pq is not the zero polynomial, so p, q are not zero divisors. ∎

the degree of the zero polynomial is $-\infty$

Note that $\deg(p) = 0$ says that p is a nonzero constant polynomial, i.e., $p(x) = a_0$ with $a_0 \neq 0$.

Since all fields are integral domains, we have the following consequence.

Corollary

If F is a field, then $F[x]$ is an integral domain with identity.

However $F[x]$ will not itself be a field! For example, the polynomial $p(x) = x$ has no multiplicative identity, because if $q(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$, then $\deg(q) = n$ and

$$(pq)(x) = xq(x) = a_0 x + a_1 x^2 + \cdots + a_n x^{n+1}$$

($a_n \neq 0$)

so $\deg(pq) = n+1 \geq 1$. Since the multiplicative identity is the constant polynomial $1(x) = 1$, which has degree zero, $pq \neq 1$.

Exercise Let F be a field. Find all elements that have multiplicative inverses in $F[x]$.

For addition, we have the following.

Exercise
Let R be a commutative ring. If $p, q \in R[x]$, then $\deg(p+q) \leq \max\{\deg(p), \deg(q)\}$

Note: If $p+q=0$, then $\deg(p+q) = -\infty$, so the inequality is still satisfied.

Example: If $\deg(p) = n$ then $\deg(-p) = n$, but
$$\deg(p + (-p)) = \deg(0) = -\infty$$

Example: In $\mathbb{Z}[x]$, $p(x) = 1 + x + 2x^2$ and $q(x) = 1 + 2x - 2x^2$ both have degree 2, but
$$(p+q)(x) = 2 + 3x$$
has degree 1.

Long Division for Polynomials

If F is a field, then long division for polynomials works just like long division of integers.

Theorem (Division Algorithm)

Let F be a field. If g is a nonzero polynomial in $F[x]$, then for any $f \in F[x]$ there exist $q, r \in F[x]$ s.t.

$$f = qg + r$$

Every polynomial f is a polynomial multiple of g plus a polynomial remainder

where either $r = 0$ or $0 \leq \deg(r) < \deg(g)$.

Proof is by induction on $\deg(g)$.

Example

In $\mathbb{R}[x]$:

$$\begin{array}{r} x \\ x+1 \overline{)\, x^2+x+1} \\ \underline{x^2+x} \\ 1 \end{array}$$

Given $g(x) = x+1$, write $f(x) = x^2+x+1$ as a multiple of g plus a remainder

$$\underbrace{x^2+x+1}_{f(x)} = \underbrace{x}_{q(x)}\underbrace{(x+1)}_{g(x)} + \underbrace{1}_{r(x)}$$

$\deg(g) = 1$

$\deg(r) = 0$ or $r = 0$

Example in $\mathbb{Z}_5[x]$

$$
\begin{array}{rl}
 & 4x+2 \\
3x+4 \;\big|\; & 2x^2+2x+1 \\
 & \underline{2x^2+x} \qquad (3x+4)(4x) = 2x^2+x \\
 & x+1 \\
 & \underline{x+3} \qquad (3x+4)(2) = x+3 \\
 & 3 \qquad 1-3=3 \text{ in } \mathbb{Z}_5
\end{array}
$$

So

$$2x^2+2x+1 = (4x+2)(3x+4)+3 \quad \text{in } \mathbb{Z}_5[x]$$

Verify directly by multiplying out the right side!

As a consequence, we can prove that every ideal in $F[x]$ is a principal ideal, generated by a monic polynomial.

Definition

A polynomial p is monic if we can write it as

$x^n = 1x^n$

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

i.e., the coefficient of the highest power is 1.

Recall that we create principal ideals as follows. Given a polynomial $p \in F[x]$, since $F[x]$ is commutative the principal ideal generated by p is

$$(p) = pF[x] = \{pq : q \in F[x]\}.$$

For example, the principal ideal generated by the polynomial X is

(x) is an ideal. Any polynomial in (x) has the form $xq(x)$, which is a multiple of x. If you multiply any one of those by another polynomial $f(x)$, you get another multiple of x, $xq(x)f(x)$

$$(x) = xF(x) = \{xq(x) : q \in F[x]\}$$

$$= \left\{ a_0 X + a_1 X^2 + \cdots + a_n X^{n+1} : \begin{array}{l} n \geq 0 \\ a_i \in F \end{array} \right\}$$

i.e., (x) is the set of all polynomials whose constant term is zero.

Exercise

Show that if F is a field & $c \in F$ with $c \neq 0$, then for any polynomial $p \in F[x]$, we have

$$(p) = (cp).$$

Since $c \neq 0$, it has a multiplicative inverse c^{-1}

However, also show that this is not true for polynomial rings over integral domains. In particular, for $R = \mathbb{Z}$, show that the principal ideals generated by x & $2x$ are not equal, i.e.,

$$(x) \neq (2x) \quad \text{in } \mathbb{Z}[x].$$

Show that $x \neq (2x)q(x)$ for any $q(x) \in \mathbb{Z}[x]$

Exercise

Verify directly that

$$I = (x) = \{a_0 x + \cdots + a_n x^{n+1} : n \geq 0,\ a_i \in F\}$$

is an ideal in $F[x]$.

Theorem

If F is a field, then every ideal in $F[x]$ is a principal ideal. Moreover, if $I \neq 0$ then $\exists$ monic polynomial $p(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$ such that

$$I = (p) = \{pq : q \in F[x]\}$$

A principal ideal is the set of all multiples of a fixed element p, and is denoted by (p)

Proof:

If $I = \{0\}$ then I is the principal ideal $I = (0)$, so we are done.

Therefore, consider the case that $I \neq \{0\}$.

Consider all the nonzero polynomials

$p(x) = a_0 + a_1 x + \cdots + a_n x^n$ that belong to I.

Each of these has a degree that is an integer ≥ 0.

If we consider all the degrees of the nonzero polynomials in I, then there's a smallest possible degree. There might be many polynomials with that degree, but there has to be a smallest possible degree.

Example: If there are no polynomials of degree 0 or 1 in I, but there is a polynomial of degree 2, then the smallest degree of the nonzero polynomials in I is 2.

For example, $I = (x^2)$ is the set of all polynomial multiples of x^2. There are no polynomials of degree 0 or 1 in (x^2).

Choose any one of these nonzero polynomials in I with smallest degree, say

$$g(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + b_n x^n.$$

By definition of degree, we have $b_n \neq 0$. Since F is a field, $\exists\, b_n^{-1} \in F$. But I is an ideal, so if we multiply g by the

constant polynomial b_n^{-1}, we get a monic polynomial that still belongs to I:

degree n

$$b_n^{-1} g(x) = b_n^{-1} b_0 + b_n^{-1} b_1 X + \cdots + b_n^{-1} b_{n-1} X^{n-1} + X^n$$

Call this polynomial p & set $a_i = b_n^{-1} b_i$, so

$$p(x) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in I.$$

Summary: $I \neq \{0\}$ is an ideal. Choose a monic polynomial $p \in I$ with smallest degree. We'll show that $I = (p)$

Now consider the principal ideal (p) generated by p. If q is any polynomial in $F[x]$, then $pq \in I$ since I is an ideal. Therefore

$$(p) = \{pq : q \in F[x]\} \subseteq I.$$

↑ definition: (p) is the set of all polynomial multiples of p.

Now we prove the converse inclusion. Suppose that f is any polynomial in I. Then we can write

Must show $I \subseteq (p)$

$$f = pq + r$$

$f \in I$ by hypothesis
$p \in I$ by definition
$pq \in I$ since I is an ideal

$$f = pq + r$$

for some polynomials $q, r \in F[x]$ where either $r = 0$ or $0 \leq \deg(r) < \deg(p)$.

But $f \in I$ and $pq \in I$ since I is an ideal, so this implies

$$r = f - pq \in I.$$

But either $r = 0$ or r has smaller degree than p, and p has the smallest possible degree among the nonzero polynomials in I. Hence we must have

$$r = 0.$$

Therefore

$$f = pq \in (p),$$

which shows $I \subseteq (p)$. Thus we conclude that $I = (p)$. ∎

Exercise: Show p is the unique monic polynomial that generates I.

Remark

You should compare this proof to the proof of the fact that $\mathbb{Z}$ has only principal ideals.

Example

What about ideals in $R[x]$ where R is an integral domain but not a field? The following example shows that ideals need not be principal in this case.

Consider $R = \mathbb{Z}$. Set

$$I = \{2k_0 + k_1 x + \cdots + k_n x^n : n \geq 0,\ k_i \in \mathbb{Z}\}.$$

the constant term is even

Exercise: Show directly that I is an ideal in $\mathbb{Z}[x]$.

Is I a principal ideal? Suppose that it was, i.e., $I = (p)$ for some polynomial $p \in I$. Since the constant polynomial 2 belongs to I, we must therefore have

$$2 \in I = (p) = \{pq : q \in \mathbb{Z}[x]\}.$$

Hence, $\exists q \in \mathbb{Z}[x]$ such that

$$2 = pq.$$

Since $\mathbb{Z}$ is an integral domain, we therefore have

degrees add

$$0 = \deg(2) = \deg(pq) = \deg(p) + \deg(q).$$

Therefore $\deg(p) = \deg(q) = 0$, so p & q are constant polynomials. Thus $\exists a \in \mathbb{Z}$ s.t.

$$p(x) = a.$$

But $p \in I$, so we must have $a = 2k$ for some $k \in \mathbb{Z}$.

all polynomials in I have an even constant term

Now, the polynomial x belongs to $I = (p)$, so we must have $x = p(x)q(x)$ for some $q \in \mathbb{Z}[x]$.

Hence

$$\begin{aligned} x &= p(x)\,q(x) \\ &= (2k)(b_0 + b_1 x + \cdots + b_n x^n) \\ &= 2kb_0 + 2kb_1 x + \cdots + 2kb_n x^n. \end{aligned}$$

But this implies (look at the coefficients of the x terms):

$$1 = 2k b_0.$$

But there are no $k, b_0 \in \mathbb{Z}$ for which this is true, so we have a contradiction. Hence I is NOT a principal ideal. ▨

GCDs & Factorization in Rings of Polynomials

Motivation: The Integers.

Many facts that hold for the ring of integers also hold for polynomial rings over fields. To motivate some of these, let us review the connection between ideals, factors, greatest common divisors, etc., in the integers.

Recall that if $n \in \mathbb{Z}$ then the principal ideal generated by n is simply the set of all multiples of n:

$$(n) = n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}.$$

Exercises

Let $m, n \in \mathbb{Z}$ be given. For simplicity, assume $m, n > 0$.

a. Show $m|n \iff (n) \subseteq (m)$

b. Let $\ell = \text{l.c.m.}(m, n)$. Show that

$$(m) \cap (n) = (\ell)$$

c. Show that $(m) \cup (n)$ need not be an ideal in $\mathbb{Z}$.

d. Show that $I = \{jm + kn : j, k \in \mathbb{Z}\}$

is an ideal in $\mathbb{Z}$ that contains both m & n.

e. Show that I is the smallest ideal in $\mathbb{Z}$ that contains both m & n. That is, show that if J is an ideal in $\mathbb{Z}$ that contains both m & n, then $I \subseteq J$.

For this reason, we call I the <u>ideal generated by m & n</u> & write $I = (m, n)$.

f. Since every ideal in $\mathbb{Z}$ is a principal ideal, we must have

$$I = (d)$$

for some integer d. Identify d & prove your statement, ie., prove that

$(m, n) = (d)$ where $d =$ _____.

Divisors

Just as for integers, we can talk about divisors or factors of polynomials.

Definition
Let F be a field. If $g, f \in F[x]$ with $g \neq 0$, then we say g divides f, written $g \mid f$ or $g(x) \mid f(x)$, if

$$f = qg \quad \text{for some } q \in F[x].$$

Exercise Assume $f \neq 0$.
Show that if $g \mid f$ then $\deg(g) \leq \deg(f)$.

Exercise (Important!)
Suppose g, f are nonzero polynomials in $F[x]$. Show that

$$g \mid f \iff (f) \subseteq (g)$$

Exercise

Show that $g|f$ and $f|g$ does not imply $f=g$. What does it imply? Show that if $f, g \neq 0$ then:

$$g|f \ \& \ f|g \iff \_\_\_\_\_$$

Next we define the greatest common divisor of two polynomials. While the following definition is somewhat cumbersome, we will prove some equivalent formulations (and also show that a greatest common divisor actually exists!)

Definition

Let f, g be polynomials in $F[x]$, not both zero. Then their greatest common divisor is the monic polynomial $d \in F[x]$ that satisfies:

a. $d|f$ & $d|g$,

b. if $h|f$ & $h|g$, then $h|d$

Note that a says that d is a common divisor of both f & g, while b says that d is the greatest common divisor.

We need an exercise for ideals in $F[x]$ similar to one we did for ideals in $\mathbb{Z}$.

Exercise

Let $f, g \in F[x]$ with $f, g \neq 0$ be given. Define

$$(f,g) = \{af + bg : a, b \in F[x]\}.$$

a. Show that (f,g) is an ideal in $F[x]$.

b. Show that (f,g) is the smallest ideal in $F[x]$ that contains both f & g. That is, show that:

$$I \text{ is an ideal } \& \ f, g \in I \implies (f,g) \subseteq I.$$

Theorem

Let F be a field, & let $f, g \in F[x]$ with $f, g \neq 0$ be given.

a. A greatest common divisor d of f & g exists.

b. d is the monic polynomial s.t. $(d) = (f,g)$.

c. $d = af + bg$ for some $a, b \in F[x]$.

Proof:
By the exercise, we know that (f,g) is an ideal. But every ideal in $F[x]$ is principal, so since (f,g) is a nonzero ideal, there exists a unique monic polynomial $d \in F[x]$ s.t.

$$(d) = (f,g) = \{af+bg : a,b \in F[x]\}.$$

Now, $(f) \subseteq (f,g) = (d)$ (why?) so $d|f$, & likewise $d|g$. Thus d is a divisor of both f & g.

To show d is the greatest common divisor of f & g, suppose that $h|f$ & $h|g$. Then

$$f \in (f) \subseteq (h) \quad \& \quad g \in (g) \subseteq (h).$$

Exercise: Show that this implies that

$$(f,g) \subseteq (h).$$

Hence $(d) = (f,g) \subseteq (h)$, which implies $h|d$.

Thus d is the greatest common divisor, and we have also shown statements b & c. ∎

Definition

Nonzero polynomials f & g are relatively prime if their greatest common divisor is 1.

Exercise

Let f, g be nonzero polynomials in $F[x]$. Then

f, g are relatively prime $\iff \exists a, b \in F[x]$ s.t.
$af + bg = 1$

Theorem

If q & f are relatively prime polynomials and

$q \mid fg$, then $q \mid g$.

Proof:

Since q & f are relatively prime, the preceding exercise implies that

$$aq + bf = 1$$

for some $a, b \in F[x]$. Therefore

$$aqg + bfg = g.$$

But $q \mid fg$, so $fg = qh$ for some polynomial h.

Therefore

$$aqg + bqh = g$$

or

$$q(ag + bh) = g.$$

Therefore $q \mid g$. ▨

As we have seen, a polynomial ring $F[x]$ over a field F has many properties analogous to properties of the ring of integers. Next we see that $F[x]$ has elements that behave much like the prime numbers do in $\mathbb{Z}$.

Definition
A polynomial p is irreducible if:

a. $\deg(p) \geq 1$ (p is not a constant polynomial)

b. $\forall f \in F[x]$, either $p \mid f$ or p & f are relatively prime.

Theorem
Let F be a field, & suppose $p \in F[x]$ satisfies $\deg(p) \geq 1$. Show that TFAE:

a. p is irreducible.

b. There are no polynomials q, m with degree ≥ 1 such that $p = qm$.

Proof:
a $\Rightarrow$ b. Suppose that p is irreducible. Suppose

$p = qm$ where $\deg(q) \geq 1$ & $\deg(m) \geq 1$.

Then q is a nonconstant polynomial that divides both q and p, so q & p are not relatively prime. The definition of irreducible therefore implies that $p|q$. But we also have $q|p$ since $p=qm$, so by an earlier exercise we have $p=cq$ where $c \in F$. But then $qm = p = cq$, which is a contradiction (why? What are the degrees of qm & cq?). Hence no such q, m exist, so statement b holds.

b $\Rightarrow$ a.

Exercise.

Hint: Suppose statement b holds. Suppose f is any polynomial such that p & f are not relatively prime. Show that we must have $p|f$.

Examples

Irreducibility depends on the field F! For example

X^2+1 is irreducible in $\mathbb{R}[x]$

$X^2+1 = (x+i)(x-i)$ is not irreducible in $\mathbb{C}[x]$

$X^2+1 = (x+1)(x+1)$ is not irreducible in $\mathbb{Z}_2[x]$

Exercise

Show that if F is a field & $a, b \in F$ with $a \neq 0$ are given, then $p(x) = ax+b$ is irreducible.

Irreducibility & Maximal Ideals

Next we show that the question of whether a polynomial p is irreducible is related to the question of whether the principal ideal (p) is a maximal ideal in $F[x]$. Furthermore, we saw in the section on maximal ideals that this is related to the question of whether the quotient ring $F[x]/(p)$ is a field.

Theorem

Let F be a field, and let $p \in F[x]$ satisfy $\deg(p) \geq 1$. Then TFAE.

a. p is irreducible in $F[x]$.

b. (p) is a maximal ideal in $F[x]$.

c. $F[x]/(p)$ is a field.

Proof:

a $\Rightarrow$ b. Suppose that p is irreducible. We must show that

$$(p) = pF[x] = \{pq : q \in F[x]\}$$

is maximal in $F[x]$. To do this, suppose

that I is an ideal such that $(p) \subseteq I \subseteq F[x]$.

We must show that I must either equal (p) or $F[x]$.

Now, we proved earlier that every ideal in $F[x]$ is a principal ideal, so we must have $I = (f)$ for some $f \in F[x]$. Therefore

$$p \in (p) \subseteq I = (f) = \{fq : q \in F[x]\}.$$

Therefore $p = fq$ for some $q \in F[x]$.

However, p is irreducible, so $p = fq$ implies that either f must be constant or q must be constant.

If $f(x) = a_0$ is a constant polynomial then we must have $a_0 \neq 0$ (why?), so a_0 is a unit in F and therefore f is a unit in $F[x]$ (why?)

Here, unit means an element that has a multiplicative inverse

But since f is a unit, we have $I = (f) = F[x]$ (why?)

On the other hand, if $q(x) = a_0$ is constant, then

again $a_0 \neq 0$ (why?), so a_0 is a unit in F

and Therefore an earlier exercise implies

$$I = (f) = (pq) = (a_0 p) = (p).$$

Thus, the only possibilities are $I = F[x]$ or $I = (p)$. Therefore (p) is maximal.

b $\Rightarrow$ a. Suppose that $M = (p)$ is a maximal ideal in $F[x]$. Suppose that p was not irreducible. Then there would exist polynomials a, b with $\deg(a) \geq 1$ & $\deg(b) \geq 1$, such that $p = ab$.

Now, since $a \mid p$, we have $M = (p) \subseteq (a) \subseteq F[x]$. Since $\deg(a) \geq 1$, there are no nonzero constant polynomials in (a) (why?), so we have $(a) \neq F[x]$. Since M is maximal, this implies $(a) = (p)$. But then we have both $a \mid p$ & $p \mid a$, so $p = ca$ where

$c \in F$, $c \neq 0$. Hence $\deg(p) = \deg(a)$. But $p = ab$, so this implies $\deg(b) = 0$, which is a contradiction. Therefore p must indeed be irreducible.

$b \Leftrightarrow c$. We proved this equivalence in the section on maximal ideals. ∎

Thus, if p is irreducible, then $F[x]/(p)$ is a field. Now, $F[x]/(p)$ is the set of all cosets of (p);

$$F[x]/(p) = \{ q + (p) : q \in F[x] \}$$

But what are these cosets? Is it possible to give a better description of $F[x]/(p)$?

Exercise

Let F be a field, & let p be an irreducible polynomial in $F[x]$.

a. Let f be any polynomial in $F[x]$. Use the Division Algorithm to write

$$f = pq + r, \qquad r = 0 \text{ or } 0 \le \deg(r) < \deg(p)$$

Show that f & r determine the same coset, i.e.,

$$f + (p) = r + (p).$$

b. Show that

$$F[x]/(p) = \{ r + (p) : r = 0 \text{ or } 0 \le \deg(r) < \deg(p) \}$$

Is this a listing <u>without</u> duplication? That is, does each polynomial r with $\deg(r) < \deg(p)$ determine a unique coset $r + (p)$?

c. If F is finite, how many cosets are there in $F[x]/(p)$? In particular, is $F[x]/(p)$ a finite field?

<u>Remark</u>

If writing (p) is notationally confusing, let $I = (p)$ and use that instead, e.g., write

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

Factorization of Polynomials

As we know, every positive integer has a unique factorization as a product of powers of primes. The next result is the analogous Theorem for polynomials over a field.

Theorem

Let F be a field, & choose $f \in F[x]$ with $\deg(f) \geq 1$.

Then either f is itself irreducible, or it can be written as a product of irreducible polynomials.

In fact,

$$f = a\, p_1^{m_1} \cdots p_k^{m_k} \qquad (*)$$

where: $k \geq 1$,

$a \in F$ is the leading coefficient of f,

$p_1, \ldots, p_k$ are monic & irreducible,

$m_1 > 0, \ldots, m_k > 0$.

The factorization in $(*)$ is unique up to the ordering of the factors p_k

Proof:

We first show that f is either irreducible or is a product of irreducible polynomials. We proceed by induction on the degree of f.

Base step: $\deg(f) = 1$.

In this case $f(x) = ax + b$ with $a, b \in F$, $a \neq 0$.

Exercise: Show f is irreducible.

Inductive step: Suppose the result is true for all polynomials of degree $1, \ldots, \deg(f) - 1$.

Now, if f is irreducible, then the result is true for f. So, we need to examine the case where f is not irreducible. In this case, we can write

$f = ab$ where $1 \leq \deg(a), \deg(b) < \deg(f)$.

But then by the inductive hypothesis,

[redacted]

$$a = c\,p_1^{m_1} \cdots p_k^{m_k} \quad \text{and} \quad b = d\,q_1^{n_1} \cdots q_\ell^{n_\ell}$$

where $c, d \in F$ and p_i, q_i are irreducible. Hence

$$f = (cd)\,p_1^{m_1} \cdots p_k^{m_k} q_1^{n_1} \cdots q_\ell^{n_\ell}$$

is a product of irreducible polynomials - some p_i may equal some q_j, but this is not a problem.

The proof of uniqueness is similar, by induction on the degree of f - see the text for proof. ∎

Why are the integers & polynomial rings over fields so similar? The important fact in each is that it is possible to compare the "size" of elements of the ring: in the integers we have the usual ordering $1 \leq 2 \leq 3 \leq \cdots$, while in the ring $F[x]$ we have the degree of the polynomial to tell us its "size." Size is no longer an injective function on $F[x]$ (two different polynomials may have the same degree), but we have the Division Algorithm & the behavior of the degree under multiplication. Any ring that has analogues of these properties will share the properties of $\mathbb{Z}$ & $F[x]$. Such a ring is called a Euclidean ring, defined precisely as follows.

Definition

An integral domain R is a *Euclidean ring* or a *Euclidean domain* if there is a *Euclidean function* $f: R^* = R \setminus \{0\} \longrightarrow \mathbb{N}$ that satisfies:

a. $\forall\, a \neq 0, b \neq 0, \quad d(a) \leq d(ab)$

b. If $a \neq 0$ then for every $b \neq 0$ we can write

$$b = aq + r$$

where $q, r \in R$ and either $r = 0$ or $d(r) < d(a)$.

It can be shown that:

Euclidean domain $\Rightarrow$ Principal Ideal Domain (PID) $\Rightarrow$ Unique Factorization Domain (UFD) $\Rightarrow$ Integral Domain