Lecture 17

Polynomials

Today we will start (and finish) Chapter 6.

I will assume you know how to add (+) and multiply (·) polynomials and know about the complex numbers $\mathbb{C}$.

We let $\mathbb{R}[x]$ denote the set of polynomials with real coefficients and $\mathbb{C}[x]$ denote the set of polynomials with complex coefficients. More generally, if F is a field we let $F[x]$ denote the set of polynomials with F coefficients.

Theorem

$(F[x], +, \cdot)$ is a commutative F-algebra.

But more is true. There is a theory of factoring polynomials into primes analogous to factoring integers into primes.

First recall the degree of a polynomial.

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, the degree of $f(x)$ denoted $\deg(f(x))$, is the greatest integer m so that $a_m \neq 0$.

Proposition:

Let $f(x) \neq 0$ and $g(x) \neq 0$ be in $F[x]$.
Then $f(x) \cdot g(x) \neq 0$ and $\deg(f(x)\, g(x)) = \deg(f(x)) + \deg(g(x))$

proof: Let $f(x) = a_m x^m + \dots + a_0$ with $a_m \neq 0$

$g(x) = b_n x^n + \dots + b_0$ with $b_n \neq 0$

To calculate the degree of the product, we must only keep track of the highest degree terms in each of $f(x)$ and $g(x)$. That is,

$$(a_m x^m + \dots + a_0)(b_n x^n + \dots + b_0) = a_m b_n x^{m+n} + \text{strictly lower terms.}$$

Since $a_m b_n \neq 0$, $\deg(f(x) \cdot g(x)) = m + n = \deg(f(x)) + \deg(g(x))$

$\square$

Corollary:

$(F[x], +, \cdot)$ is an integral domain. That is,

$$f \cdot g = 0 \iff f = 0 \text{ or } g = 0.$$

Prime Factorization of Integers

Units: The only integers that are invertible are +1 and −1.

Definition:
An integer m divides an integer n if there is some integer q so that $n = mq$. We write $m \mid n$.

The Division Algorithm for Integers

Let m and n be integers with $m \neq 0$. Then there exist integers q and r such that

$$n = mq + r \text{ and } |r| < |m|$$

Definition

Let m and n be integers. The greatest common divisor, written $\gcd(m,n)$, is the integer d such that

(1) $d > 0$

(2) $d \mid m$ and $d \mid n$

(3) If $d' \mid m$ and $d' \mid n$ then $d' \mid d$.

There is an analogous definition for $n_1, \ldots, n_k$, written $\gcd(n_1, \ldots, n_k)$.

Definition

K is said to be a common multiple of m and n if $m \mid K$ and $n \mid K$.

The least common multiple of m and n, written $\operatorname{lcm}(m,n)$ is the smallest positive common multiple of m and n.

There is an analogous definition for $n_1, \ldots n_k$, written $\operatorname{lcm}(n_1, \ldots, n_k)$.

Theorem

(1) $n_1, n_2, \ldots, n_k$ have a unique gcd d.

(2) There exist integers $m_1, m_2, \ldots, m_k$ such that

$$d = m_1 n_1 + m_2 n_2 + \cdots + m_k n_k.$$

Definition

An integer p is said to be prime if

(1) $p > 1$

(2) if $d \mid p$ and $d > 0$ then either $d = 1$ or $d = p$.

The Fundamental Theorem of Arithmetic

Every non-zero integer m has a unique prime factorization.

$$m = \pm\, p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

Basic Lemma:

If $p \mid a \cdot b$ and p is prime then either

$p \mid a$ or $p \mid b$

Given m and n you can read off the gcd and lcm from their prime factorizations

(1) $m = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$

(2) $n = q_1^{f_1} q_2^{f_2} \cdots q_s^{e_s}$

gcd: Take the product of the primes that occur in both (1) and (2), each to the power of the smaller of e_i, f_i.

lcm: Take the product of all primes occurring in either (1) or (2) to the power in (1) or (2). If p_i appears in both (1) and (2), raise it to the lager of e_i, f_i.

Prime Factorization of Polonomials

Units: $f \in F[x]$ is invertible for $\cdot$ $\iff$ f is a constant.

proof: Suppose $f \cdot g = 1$. Then

$$0 = \deg(f \cdot g) = \deg(f) + \deg(g) \Rightarrow \deg(f) = \deg(g) = 0.$$

$\square$

Remark:

There are a lot more units in $F[x]$ than for the integers. We need the analogue of positive integers to get rid of units.

Definition

A polynomial is monic if the coefficient of its leading term is $+1$.

note: given a non-zero $f \in F[x]$ there is a unique unit c so that cf is monic.

Definition

A polynomial g divides a polynomial f if there exists a polynomial l so that

$$f(x) = g(x)\, l(x).$$

We write $g \mid f$.

ex: $(x^2+1) \mid (x^4-1)$

$$x^4 - 1 = (x^2+1)(x^2-1).$$

The Division Algorithm for Polynomials (20.8)

Let $f, g \in F[x]$ with $g \neq 0$. Then there exist uniquely determined polynomials Q, R called the quotient and remainder such that

$$f = Qg + R \quad \text{with} \quad \deg R < \deg g .$$

gcd and lcm

Def Let f and g be polynomials.

A greatest common divisor, written $\gcd(f,g)$ is a polynomial d such that

(1) d is monic

(2) $d \mid f$ and $d \mid g$

(3) If $d' \mid f$ and $d' \mid g$ then $d' \mid d$

Theorem (20.15)

(1) $f_1, f_2, \ldots, f_k$ have a unique gcd d.

(2) There exist polynomials $l_1, l_2, \ldots, l_k$ such that

$$d(x) = l_1(x) f_1(x) + \cdots + l_k(x) f_k(x).$$

Definition

A polynomial P is said to be prime if $P \neq 1$ and

(1) P is monic

(2) If $d \mid P$ and d is monic then either

$$d = 1 \text{ or } d = P$$

The Unique Factorization Theorem for Polynomials

Let $f(x) \in F[x]$ and $f \neq 0$.

Then $f(x)$ has a unique factorization

$$f(x) = c\, p_1(x)^{e_1}\, p_2(x)^{e_2} \cdots p_n(x)^{e_n}$$

for some $c \in F$, $p_i(x)$ prime $1 \leq i \leq n$.

The \$64,000 Question: What are the primes in $F[x]$

First we note the answer depends on F.

$x^2 - 2$ is prime in $\mathbb{Q}[x]$, but factors as

$(x - \sqrt{2})(x + \sqrt{2})$ in $\mathbb{R}[x]$.

$x^2 + 1$ is prime in $\mathbb{R}[x]$, but factors as

$(x + i)(x - i)$ in $\mathbb{C}[x]$

Of course to justify this we need to know that X^2-2 doesn't have some other factorization.

That is, $(X^2-2)=(X-a)(X-b) \iff a=\pm\sqrt{2}$.

This follows from the easy direction of

<u>Theorem</u>

$(X-a) \mid f(x) \iff f(a)=0$

$(\Rightarrow)$ is obvious. $(X-a) \mid f(x) \Rightarrow f(x)=(x-a)q(x)$

for some $q(x) \in F[x]$. Then

$$f(a) = ((a)-a)\,q(a) = 0 \cdot q(a) = 0.$$

$(\Leftarrow)$ is not clear.

In fact there is a more general result.

Apply the Division Algorithm to obtain

$$f(x) = (X-a)\,Q + R \qquad (*)$$

Note $\deg R < 1$ so R is a constant.

In fact

<u>Theorem</u> (20.13)

$$R = f(a)$$

<u>proof</u>

Substitute a into both sides of $(*)$.

$$f(a) = (a-a)Q(a) + R(a) = 0 \cdot Q(a) + R(a) = R(a) = R.$$

$\square$

Describing the prime polynomials over $\mathbb{Q}[x]$ is too hard. However we can solve the problem over $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

<u>Theorem 1</u>

The prime polynomials in $\mathbb{R}[x]$ are the linear polynomials $x-a$, $a \in \mathbb{R}$ and the quadratic polynomials x^2+bx+c where $b^2-4c<0$.

<u>Theorem 2</u>

The prime polynomials in $\mathbb{C}[x]$ are the linear polynomials $x-\alpha$, $\alpha \in \mathbb{C}$.

<u>Primes in $\mathbb{C}[x]$</u>

We will first prove Theorem 2 assuming

<u>The Fundamental Theorem of Algebra</u>

Let $f(x) \in \mathbb{C}[x]$. Then if f is non-constant f has a root. (In fact, it will have $\deg f$ roots if we count with multiplicity).

<u>Corollary</u>

If $f(x) \in \mathbb{C}[x]$ and f is prime then f has degree 1.

Primes in $\mathbb{R}[X]$

Every polynomial in $\mathbb{R}[X]$ can be factored into the product of linears and quadratics.

First, factor in $\mathbb{C}[X]$.

$$f(x) = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n).$$

Non-real roots need occur in complex conjugate pairs.

$$f(\alpha)=0 \iff \overline{f(\alpha)}=0 \iff f(\bar{\alpha})=0.$$

So $f(x) = (X-a_1)\cdots(X-a_r)(X-\beta_1)(X-\overline{\beta_1})\cdots(X-\beta_m)(X-\overline{\beta_m})$

Define

$$q_i(X) = (X-\beta_i)(X-\overline{\beta_i}) = X^2-(\beta_i+\overline{\beta_i})X+\beta_i\overline{\beta_i}$$

$$= X^2 - 2\,\mathrm{Re}(\beta_i)\,X + |\beta_i|^2$$

Then $q_i(X)$ is prime in $\mathbb{R}[X]$ because if it wasn't it would be divisible by $X-a$, $a\in\mathbb{R}$, so a would be a root of $q_i(X)$. But the only roots of $q_i(X)$ are β_i and $\overline{\beta_i}$.