Lecture 16: Polynomials

Today we will start (adn finish) Chapter 6. I will assume that you know how to add $(+)$ and multiply $(\cdot)$ polynomials and know about the complex numbers $\mathbb{C}$.

Polynomials

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

$(F, +, \bullet)$ *is a commutative algebra.*

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

Degree of Polynomials

First recall the degree of a polynomials. If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, the degree of the polynomiasl 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 $F[x]$. Then $f(x) \cdot g(x) \neq 0$ and

$$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

Proof. Let

$$\begin{aligned} f(x) &= a_m x^m \ldots + a_0 \text{ with } a_m \neq 0 \\ g(x) &= b_n x^n \ldots + b_0 \text{ with } b_n \neq 0 \end{aligned}$$

Degree of Polynomials

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

$$(a_m x^m \ldots + a_0)(b_n x^n \ldots + b_0) = a_m b_n x^{m+n} + \text{stricly lower order terms}$$

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

Corollary

$(F, +, \bullet)$ is an integral domain. That is,

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

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/n.

The division Algorithm for Integers: Let m and n with $m \neq 0$. Then there exit integers q and r such that

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

GCD and LCM

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/m and d/n.

(3) If d'/m and d'/n then d'/d.

There is an analagous 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 is m/k and n/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 analagous 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*

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

Definition

An integer p is said to be prime if

(1) $p > 1$.

(2) if d/p and $d > 0$, the either $d = 1$ or $d = p$.

The Fundamental Theorem of Arithmetic

Theorem (The Fundamental Theorem of Arithmetic)

Every non-zero integer m has unique prime factorization

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

Lemma (Basic)

If $p/a \cdot b$, and p is prime then either p/a or p/b.

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

(1) $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$

(2) $n = q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}$

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

lcm: Take the product of the primes that occur either both (1) or (2) to the power in (1) or (2). If f_i appears in both (1) and (2), raise it to the larger of e_i, f_i.

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

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

$$0 = \deg(f \cdot g) = \deg(f) + \deg(g) \implies \deg(f) = \deg(g) = 0. \quad \square$$

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 the leading term is 1.

Note: Given a non-zero $f \in F[x]$ there is an unique unit c such that cf is monic.

Definition

A polynomial g dovedes a polynomial f is there exists a polynomial ℓ such that

$$f(x) = g(x)\ell(x)$$

We write $g|f$.

Example:

$$(x^2 + 1)|(x^4 - 1)$$

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

The Division Algortithm for Polynomials

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

$$f = Qg + R$$

with $\deg(R) < \deg(g)$.

Definition

Let f and g be polynomials. A greatest common divisor, written $\gcd f, g$ is a polynomial

(1) d is monic.

(2) $d|f$ and $d|g$.

(3) If $d'|f$ and $d'|g$ then $d'|d$.

Theorem (Text, 20.15)

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

(2) *There exist polynomials* $\ell_1, \ell_2, \ldots, \ell_n$ *such that*

$$d(x) = \ell_1(x) f_1(x) + \ell_2(x) f_2(x) + \ldots + \ell_n(x) f_n(x)$$

The Unique Factorization Theorem

Definition

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

(1) p is monic

(2) If $d|p$ and d is monic then either $d = 1$ or $d = p$.

Theorem (The Unique Factorization Theorem)

Let $f(x) \in F[x]$ and $f = 0$. Then $f(x)$ has a unique factorization

$$f(x) = cp_1(x)^{e_1} p_2(x)^{e_2} \dots p_n(x)^{e_n}$$

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

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

First, we note the answer depends of 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 $x^2 - 2$ does not 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

Theorem

$(x - a)|f(x) \iff f(a) = 0.$

Proof.

($\Longrightarrow$) Is obvious. $(x-a)|f(x) \Longleftrightarrow f(x) = (x-a)q(x)$ for some $q(x) \in F[x]$. Then

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

($\Longleftarrow$) Is not clear.

If fact there is a more general result. Apply the Division Algorithm to obtain

$$f(x) = (x-a)Q + R \quad (*)$$

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

In fact,

Theorem (Text, 20.13)

$R = f(a)$.

Proof. Subsitute 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 $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

Prime Polynomials in $\mathbb{R}[x]$ and $\mathbb{C}[x]$

Theorem (1)

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* $b^2 - 4ac < 0$.

Theorem (2)

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

Primes in $\mathbb{C}[x]$

We will first prove Theorem 2 assuming

Theorem (The Fundamental Theorem of Algebra)

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

Corollary

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

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

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

First, factor in $\mathbb{C}[x]$:

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

Non-real roots need occur in complex conjugate pairs.

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

So,

$$f(x) = (x - a_1) \ldots (x - a_r)(x - \beta_1)(x - \overline{\beta_1}) \ldots (x - \beta_m)(x - \overline{\beta_m})$$

Define

$$\begin{aligned} q_i(x) &= (x - \beta_i)(x - \overline{\beta_i}) \\ &= x^2 - (\beta_i + \overline{\beta_i})x + \beta_i\overline{\beta_i} \\ &= x^2 - 2\mathrm{Re}(\beta_i)x + |\beta_i|^2 \end{aligned}$$

Then $q_i(x)$ is prime in $\mathbb{R}[x]$ because it was not 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 $\overline{\beta_i}$.