MATH 433

Applied Algebra

Lecture 35:
Greatest common divisor of polynomials.
Factorisation of polynomials.

Greatest common divisor

Definition. Given non-zero polynomials $f, g \in \mathbb{F}[x]$, a **greatest common divisor** $\gcd(f, g)$ is a polynomial over the field $\mathbb{F}$ such that **(i)** $\gcd(f, g)$ divides f and g, and **(ii)** if any $p \in \mathbb{F}[x]$ divides both f and g, then it divides $\gcd(f, g)$ as well.

Theorem The polynomial $\gcd(f, g)$ exists and is unique up to a scalar multiple. Moreover, it is a non-zero polynomial of the least degree that can be represented as $uf + vg$, where $u, v \in \mathbb{F}[x]$.

Theorem The polynomial $\gcd(f, g)$ exists and is unique up to a scalar multiple. Moreover, it is a non-zero polynomial of the least degree that can be represented as $uf + vg$, where $u, v \in \mathbb{F}[x]$.

Proof: Let S denote the set of all polynomials of the form $uf + vg$, where $u, v \in \mathbb{F}[x]$. The set S contains non-zero polynomials, say, f and g. Let $d(x)$ be any such polynomial of the least possible degree. It is easy to show that the remainder under division of any polynomial $h \in S$ by d belongs to S as well. By the choice of d, that remainder must be zero. Hence d divides every polynomial in S. In particular, d is a common divisor of f and g. Further, if any $p(x) \in \mathbb{F}[x]$ divides both f and g, then it also divides every element of S. In particular, it divides d. Thus $d = \gcd(f, g)$.

Now assume d_1 is another greatest common divisor of f and g. By definition, d_1 divides d and d divides d_1. This is only possible if d and d_1 are scalar multiples of each other.

Euclidean algorithm

Lemma 1 If a polynomial g divides a polynomial f then $\gcd(f, g) = g$.

Lemma 2 If g does not divide f and r is the remainder of f by g, then $\gcd(f, g) = \gcd(g, r)$.

Theorem For any non-zero polynomials $f, g \in \mathbb{F}[x]$ there exists a sequence of polynomials $r_1, r_2, \ldots, r_k \in \mathbb{F}[x]$ such that $r_1 = f$, $r_2 = g$, r_i is the remainder of r_{i-2} by r_{i-1} for $3 \leq i \leq k$, and r_k divides r_{k-1}. Then $\gcd(f, g) = r_k$.

Irreducible polynomials

Definition. A polynomial $f \in \mathbb{F}[x]$ is said to be **irreducible** over $\mathbb{F}$ if it cannot be written as $f = gh$, where $g, h \in \mathbb{F}[x]$, and $\deg(g), \deg(h) < \deg(f)$.

Irreducible polynomials are for multiplication of polynomials what prime numbers are for multiplication of integers.

Proposition 1 Let f be an irreducible polynomial and suppose that f divides a product $f_1 f_2$. Then f divides at least one of the polynomials f_1 and f_2.

Proposition 2 Let f be an irreducible polynomial and suppose that f divides a product of polynomials $f_1 f_2 \dots f_r$. Then f divides at least one of the factors $f_1, f_2, \dots, f_r$.

Proposition 3 Let f be an irreducible polynomial that divides a product $f_1 f_2 \dots f_r$ of other irreducible polynomials. Then one of the factors $f_1, f_2, \dots, f_r$ is a scalar multiple of f.

Unique factorisation

Theorem Any polynomial $f \in \mathbb{F}[x]$ of positive degree admits a factorisation $f = p_1 p_2 \dots p_k$ into irreducible factors over $\mathbb{F}$. This factorisation is unique up to rearranging the factors and multiplying them by non-zero scalars.

Ideas of the proof: The **existence** is proved by strong induction on $\deg(f)$. It is based on a simple fact: if $p_1 p_2 \dots p_s$ is an irreducible factorisation of f and $q_1 q_2 \dots q_t$ is an irreducible factorisation of g, then $p_1 p_2 \dots p_s q_1 q_2 \dots q_t$ is an irreducible factorisation of fg.

The **uniqueness** is proved by (normal) induction on the number of irreducible factors. It is based on a (not so simple) fact: if an irreducible polynomial p divides a product of irreducible polynomials $q_1 q_2 \dots q_t$ then one of the factors $q_1, \dots, q_t$ is a scalar multiple of p.

Factorisation over $\mathbb{C}$ and $\mathbb{R}$

Clearly, any polynomial $f \in \mathbb{F}[x]$ of degree 1 is irreducible over $\mathbb{F}$. Depending on the field $\mathbb{F}$, there may exist other irreducible polynomials as well.

Fundamental Theorem of Algebra Any nonconstant polynomial over the field $\mathbb{C}$ has a root.

Corollary 1 The only irreducible polynomials over the field $\mathbb{C}$ of complex numbers are linear polynomials. Equivalently, any polynomial $f \in \mathbb{C}[x]$ of a positive degree n can be factorised as $f(x) = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$, where $c, \alpha_1, \dots, \alpha_n \in \mathbb{C}$ and $c \neq 0$.

Corollary 2 The only irreducible polynomials over the field $\mathbb{R}$ of real numbers are linear polynomials and quadratic polynomials without real roots.

Examples of factorisation

- $f(x) = x^4 - 1$ over $\mathbb{R}$.

$f(x) = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$.
The polynomial $x^2 + 1$ is irreducible over $\mathbb{R}$.

- $f(x) = x^4 - 1$ over $\mathbb{C}$.

$f(x) = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$
$= (x - 1)(x + 1)(x - i)(x + i)$.

- $f(x) = x^4 - 1$ over $\mathbb{Z}_5$.

It follows from Fermat's Little Theorem that any non-zero element of the field $\mathbb{Z}_5$ is a root of the polynomial f. Hence f has 4 distinct roots. By the Unique Factorisation Theorem,

$$\begin{aligned} f(x) &= (x - 1)(x - 2)(x - 3)(x - 4) \\ &= (x - 1)(x + 1)(x - 2)(x + 2). \end{aligned}$$

- $f(x) = x^4 - 1$ over $\mathbb{Z}_7$.

Note that the polynomial $x^4 - 1$ can be considered over any field. Moreover, the expansion $x^4 - 1 = (x^2 - 1)(x^2 + 1)$ $= (x - 1)(x + 1)(x^2 + 1)$ holds over any field. It depends on the field whether the polynomial $g(x) = x^2 + 1$ is irreducible. Over the field $\mathbb{Z}_7$, we have $g(0) = 1$, $g(\pm 1) = 2$, $g(\pm 2) = 5$ and $g(\pm 3) = 10 = 3$. Hence g has no roots. For polynomials of degree 2 or 3, this implies irreducibility.

- $f(x) = x^4 - 1$ over $\mathbb{Z}_{17}$.

The polynomial $x^2 + 1$ has roots ± 4. It follows that $f(x) = (x - 1)(x + 1)(x^2 + 1) = (x - 1)(x + 1)(x - 4)(x + 4)$.

- $f(x) = x^4 - 1$ over $\mathbb{Z}_2$.

For this field, we have $1 + 1 = 0$ so that $-1 = 1$. Hence $x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x^2 - 1)^2 = (x - 1)^2(x + 1)^2$ $= (x - 1)^4$.