MATH 433

Applied Algebra

Lecture 35:
Euclidean algorithm for polynomials.
Factorisation of polynomials.

Greatest common divisor of polynomials

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 (Bezout) 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 $u, v \in \mathbb{F}[x]$.

Euclidean algorithm for polynomials

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 $3 \le i \le k$, and r_k divides r_{k-1}. Then $\gcd(f, g) = r_k$.

Problem. Find all common roots of real polynomials $p(x) = x^4 + 2x^3 - x^2 - 2x + 1$ and $q(x) = x^4 + x^3 + x - 1$.

Common roots of p and q are exactly roots of their greatest common divisor $\gcd(p, q)$. We can find $\gcd(p, q)$ using the Euclidean algorithm.

First we divide p by q: $x^4 + 2x^3 - x^2 - 2x + 1 =$
$= (x^4 + x^3 + x - 1)(1) + x^3 - x^2 - 3x + 2$.

Next we divide q by the remainder $r_1(x) = x^3 - x^2 - 3x + 2$:
$x^4 + x^3 + x - 1 = (x^3 - x^2 - 3x + 2)(x + 2) + 5x^2 + 5x - 5$.

Next we divide r_1 by the remainder $r_2(x) = 5x^2 + 5x - 5$:
$x^3 - x^2 - 3x + 2 = (5x^2 + 5x - 5)(\frac{1}{5}x - \frac{2}{5})$.

Since r_2 divides r_1, it follows that

$$\gcd(p, q) = \gcd(q, r_1) = \gcd(r_1, r_2) = r_2.$$

The polynomial $r_2(x) = 5x^2 + 5x - 5$ has roots $(-1 - \sqrt{5})/2$ and $(-1 + \sqrt{5})/2$.

Irreducible polynomials

Definition. A non-constant polynomial $f \in \mathbb{F}[x]$ over a field $\mathbb{F}$ 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.

If an irreducible polynomial f is divisible by another polynomial g, then g is either of degree zero or a scalar multiple of f.

Unique Factorisation Theorem

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.

Some facts and examples

- Any polynomial of degree 1 is irreducible.

- A polynomial $p(x) \in \mathbb{F}[x]$ is divisible by a polynomial of degree 1 if and only if it has a root.

Indeed, if $p(\alpha) = 0$ for some $\alpha \in \mathbb{F}$, then $p(x)$ is divisible by $x - \alpha$. Conversely, if $p(x)$ is divisible by $ax + b$ for some $a, b \in \mathbb{F}$, $a \neq 0$, then p has a root $-b/a$.

- A polynomial of degree 2 or 3 is irreducible if and only if it has no roots.

If such a polynomial splits into a product of two non-constant polynomials, then at least one of the factors is of degree 1.

- Polynomial $p(x) = (x^2 + 1)^2$ has no real roots, yet it is not irreducible over $\mathbb{R}$.

- Polynomial $p(x) = x^3 + x^2 - 5x + 2$ is irreducible over $\mathbb{Q}$.

We only need to check that $p(x)$ has no rational roots. Since all coefficients are integers and the leading coefficient is 1, possible rational roots are integer divisors of the constant term: ± 1 and ± 2. We check that $p(1) = -1$, $p(-1) = 7$, $p(2) = 4$ and $p(-2) = 8$.

- If a polynomial $p(x) \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$, then $\deg(p) = 1$ or 2.

Assume $\deg(p) > 1$. Then p has a complex root $\alpha = a + bi$ that is not real: $b \neq 0$. Complex conjugacy $\overline{r + si} = r - si$ commutes with arithmetic operations and preserves real numbers. Therefore $p(\overline{\alpha}) = \overline{p(\alpha)} = 0$ so that $\overline{\alpha}$ is another root of p. It follows that $p(x)$ is divisible by $(x - \alpha)(x - \overline{\alpha})$ $= x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2ax + a^2 + b^2$, which is a real polynomial. Then $p(x)$ must be a scalar multiple of it.

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