MATH 433
Applied Algebra

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

Division of polynomials

Let $f(x), g(x) \in \mathbb{F}[x]$ be polynomials over a field $\mathbb{F}$ and $g(x) \neq 0$. We say that $g(x)$ **divides** $f(x)$ if $f = qg$ for some polynomial $q(x) \in \mathbb{F}[x]$. Then q is called the **quotient** of f by g.

Let $f(x)$ and $g(x)$ be polynomials and $\deg(g) > 0$. Suppose that $f = qg + r$ for some polynomials q and r such that $\deg(r) < \deg(g)$. Then r is the **remainder** and q is the (partial) **quotient** of f by g.

Note that $g(x)$ divides $f(x)$ if the remainder is 0.

Theorem Let $f(x)$ and $g(x)$ be polynomials and $\deg(g) > 0$. Then the remainder and the quotient of f by g are well-defined. Moreover, they are unique.

Long division of polynomials

Problem. Divide $x^4 + 2x^3 - 3x^2 - 9x - 7$ by $x^2 - 2x - 3$.

$$
\begin{array}{r|rrrrrrrrr}
 & x^2 & + & 4x & + & 8 & & & & \\
\cline{2-10}
x^2 - 2x - 3 & x^4 & + & 2x^3 & - & 3x^2 & - & 9x & - & 7 \\
 & x^4 & - & 2x^3 & - & 3x^2 & & & & \\
\cline{2-10}
 & & & 4x^3 & & & - & 9x & - & 7 \\
 & & & 4x^3 & - & 8x^2 & - & 12x & & \\
\cline{4-10}
 & & & & & 8x^2 & + & 3x & - & 7 \\
 & & & & & 8x^2 & - & 16x & - & 24 \\
\cline{6-10}
 & & & & & & & 19x & + & 17
\end{array}
$$

We have obtained that

$x^4 + 2x^3 - 3x^2 - 9x - 7 = x^2(x^2 - 2x - 3) + 4x^3 - 9x - 7,$
$4x^3 - 9x - 7 = 4x(x^2 - 2x - 3) + 8x^2 + 3x - 7,$
$8x^2 + 3x - 7 = 8(x^2 - 2x - 3) + 19x + 17.$ Therefore

$x^4 + 2x^3 - 3x^2 - 9x - 7 = (x^2 + 4x + 8)(x^2 - 2x - 3) + 19x + 17.$

Zeroes of polynomials

Definition. An element $\alpha \in \mathbb{F}$ is called a **zero** (or a **root**) of a polynomial $f \in \mathbb{F}[x]$ if $f(\alpha) = 0$.

Theorem $\alpha \in \mathbb{F}$ is a zero of $f \in \mathbb{F}[x]$ if and only if the polynomial $f(x)$ is divisible by $x - \alpha$.

Proposition Suppose $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ is a polynomial with integer coefficients and $c_0 \neq 0$. Then any rational zero of f is an integer dividing c_0.

Example. $f(x) = x^3 + 6x^2 + 11x + 6$.

By Proposition, possible rational zeroes of f are ± 1, ± 2, ± 3. Moreover, there are no positive zeroes as all coefficients are positive. We obtain that $f(-1) = 0$, $f(-2) = 0$, and $f(-3) = 0$. First we divide $f(x)$ by $x + 1$: $x^3 + 6x^2 + 11x + 6 = (x+1)(x^2 + 5x + 6)$. Then we divide $x^2 + 5x + 6$ by $x + 2$: $x^2 + 5x + 6 = (x+2)(x+3)$. Thus $f(x) = (x+1)(x+2)(x+3)$.

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 $\mathbb{F}$ 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 also divides $\gcd(f, g)$.

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. Let $d(x)$ be any such polynomial of the least possible degree. It is easy to show that remainders under division of f and of g by d belong to S. By the choice of d, both remainders must be zeroes. Hence d divides both 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 $r_1, r_2, \dots, r_k \in \mathbb{F}[x]$ 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 $\gcd(f, g) = r_k$.

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 $f = p_1 p_2 \ldots p_k$ 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 $p_1 p_2 \ldots p_s$ is an irreducible factorisation of f and $q_1 q_2 \ldots q_t$ is an irreducible factorisation of g, then $p_1 p_2 \ldots p_s q_1 q_2 \ldots q_t$ 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 $q_1 q_2 \ldots q_t$ then one of the factors $q_1, \ldots, q_t$ 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 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 The only irreducible polynomials over the field $\mathbb{R}$ of real numbers are linear polynomials and quadratic polynomials without real roots.

Remark. If $f(x) = x^2 + ax + b$ is an irreducible polynomial over $\mathbb{R}$, then $f(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$, where α and $\overline{\alpha}$ are complex conjugate roots of f.

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 $\mathbb{C}$.

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

- $f(x) = x^6 - 1$ over $\mathbb{Z}_7$.

It follows from Fermat's Little Theorem that any non-zero element of the field $\mathbb{Z}_7$ is a root of the polynomial f. Hence f has 6 distinct roots. Now it follows from the Unique Factorisation Theorem that

$$f(x) = (x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6).$$