MATH 433

Applied Algebra

Lecture 35:
Zeros of polynomials (continued).
Greatest common divisor of polynomials.

Zeros of polynomials

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

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

Idea of the proof: The remainder after division of $f(x)$ by $x - \alpha$ is $f(\alpha)$.

Corollary A polynomial $f \in \mathbb{F}[x]$ has distinct elements $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{F}$ as zeros if and only if it is divisible by $(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_k)$.

Rational roots

Theorem Let $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ be a polynomial with integer coefficients and $c_n, c_0 \neq 0$. Assume that f has a rational root $\alpha = p/q$, where the fraction is in lowest terms. Then p divides c_0 and q divides c_n.

Proof: By assumption,

$$c_n\left(\frac{p}{q}\right)^n + c_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + c_1\,\frac{p}{q} + c_0 = 0.$$

Multiplying both sides of this equality by q^n, we obtain

$$c_n p^n + c_{n-1}p^{n-1}q + \cdots + c_1 pq^{n-1} + c_0 q^n = 0.$$

It follows that $c_0 q^n$ is divisible by p while $c_n p^n$ is divisible by q. Since the fraction p/q is in lowest terms, we have $\gcd(p, q) = 1$. This implies that, in fact, c_0 is divisible by p and c_n is divisible by q.

Corollary If $c_n = 1$ then any rational root of the polynomial f is, in fact, an integer.

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

Since all coefficients are integers and the leading coefficient is 1, all rational roots of f (if any) are integers. Moreover, the only possible integer roots of f are divisors of the constant term: ±1, ±2, ±3, ±6. Notice that there are no positive roots 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 $f(x) = (x + 1)(x + 2)(x + 3)$.

Alternatively, once we know that $f(x)$ has roots -1, -2 and -3, it follows that it is divisible by $(x + 1)(x + 2)(x + 3)$. Since $\deg(f) = 3$, we obtain $f(x) = a(x + 1)(x + 2)(x + 3)$, where a is a constant. Comparing the leading coefficients of the left-hand side and the right-hand side, we obtain $a = 1$.

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

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