MATH 415

Modern Algebra I

Lecture 28:
Factorization of polynomials.

Polynomial expression vs. polynomial function

Let us consider the polynomial ring $\mathbb{F}[X]$ over a field $\mathbb{F}$. By definition, $p(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0 \in \mathbb{F}[X]$ is just an expression. However we can evaluate it at any $\alpha \in \mathbb{F}$ to $p(\alpha) = c_n \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0$, which is an element of $\mathbb{F}$. Hence each polynomial $p(X) \in \mathbb{F}[X]$ gives rise to a **polynomial function** $p : \mathbb{F} \to \mathbb{F}$. One can check that $(p+q)(\alpha) = p(\alpha) + q(\alpha)$ and $(pq)(\alpha) = p(\alpha)q(\alpha)$ for all $p(X), q(X) \in \mathbb{F}[X]$ and $\alpha \in \mathbb{F}$.

Theorem All polynomials in $\mathbb{F}[X]$ are uniquely determined by the induced polynomial functions if and only if $\mathbb{F}$ is infinite.

Idea of the proof: Suppose $\mathbb{F}$ is finite, $\mathbb{F} = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$. Then a polynomial $p(X) = (X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_k)$ gives rise to the same function as the zero polynomial.

If $\mathbb{F}$ is infinite, then any polynomial of degree at most n is uniquely determined by its values at $n+1$ distinct points of $\mathbb{F}$.

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 $x - \alpha$.

Proof: We have $f(x) = (x - \alpha)q(x) + r(x)$, where q is the quotient and r is the remainder when f is divided by $x - \alpha$. Note that r has only the constant term. Evaluating both sides of the above equality at $x = \alpha$, we obtain $f(\alpha) = r(\alpha)$. Thus $r = 0$ if and only if α is a zero of f.

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.

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: $\pm 1, \pm 2, \pm 3, \pm 6$. 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 $f(x) = (x + 1)(x + 2)(x + 3)$.

Factorization of polynomials over a field

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.

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

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.

Factorization 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 might exist other irreducible polynomials as well.

Fundamental Theorem of Algebra Any non-constant 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 factorized 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.