MATH 433

Applied Algebra

Lecture 34:
Polynomials in one variable.
Division of polynomials.

Polynomials in one variable

Definition. A **polynomial** in a variable X over a ring R is an expression of the form

$$p(X) = c_0X^0 + c_1X^1 + c_2X^2 + \cdots + c_nX^n,$$

where $c_0, c_1, \dots, c_n$ are elements of the ring R (called **coefficients** of the polynomial). The **degree** $\deg(p)$ of the polynomial $p(X)$ is the largest integer k such that $c_k \neq 0$. The set of all such polynomials is denoted $R[X]$.

Remarks on notation. The polynomial is denoted $p(X)$ or p. The terms c_0X^0 and c_1X^1 are usually written as c_0 and c_1X. Zero terms $0X^k$ are usually omitted. Also, the terms may be rearranged, e.g., $p(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$. This does not change the polynomial.

Remark on formalism. Formally, a polynomial $p(X)$ is determined by an infinite sequence $(c_0, c_1, c_2, \dots)$ of elements of R such that $c_k = 0$ for k large enough.

Arithmetic of polynomials

From now on, we consider polynomials over a field $\mathbb{F}$.

If
$$p(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$
$$q(X) = b_0 + b_1 X + b_2 X^2 + \cdots + b_m X^m,$$

then $(p+q)(X) = (a_0+b_0) + (a_1+b_1)X + \cdots + (a_d+b_d)X^d$,

where $d = \max(n, m)$ and missing coefficients are assumed to be zeroes. Also, $(\lambda p)(X) = (\lambda a_0) + (\lambda a_1)X + \cdots + (\lambda a_n)X^n$ for all $\lambda \in \mathbb{F}$. This makes $\mathbb{F}[X]$ into a vector space over $\mathbb{F}$, with a basis $X^0, X^1, X^2, \ldots, X^n, \ldots$

Further, $(pq)(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{n+m} X^{n+m}$,

where $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0$.
Equivalently, the product pq is a bilinear function defined on elements of the basis by $X^n X^m = X^{n+m}$ for all $n, m \geq 0$.
Now $\mathbb{F}[X]$ is a commutative ring and an associative $\mathbb{F}$-algebra.

Notice that $\deg(p \pm q) \leq \max(\deg(p), \deg(q))$. If $p, q \neq 0$ then $\deg(pq) = \deg(p) + \deg(q)$.

Polynomial expression vs. polynomial function

By definition, a polynomial $p(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0 \in \mathbb{F}[X]$ 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, $\mathbb{F} = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. Then a polynomial $p(X) = (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_k)$ 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 $\mathbb{F}$.

Division of polynomials

Let $f(x), g(x) \in \mathbb{F}[x]$ be polynomials over a field $\mathbb{F}$ and $g \neq 0$. 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 $\deg(r) < \deg(g)$ or $r = 0$. 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

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

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

Zeros 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 $x - \alpha$.

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

Problem. Find the remainder under division of $f(x) = x^{100}$ by $g(x) = x^2 + x - 2$.

We have $x^{100} = (x^2 + x - 2)q(x) + r(x)$, where $r(x) = ax + b$ for some $a, b \in \mathbb{R}$. The polynomial g has zeros 1 and -2. Evaluating both sides at $x = 1$ and $x = -2$, we obtain $f(1) = r(1)$ and $f(-2) = r(-2)$. This gives rise to a system of linear equations $a + b = 1$, $-2a + b = 2^{100}$. Unique solution: $a = (1 - 2^{100})/3$, $b = (2^{100} + 2)/3$.

Integer roots

Theorem Let $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ be a polynomial with integer coefficients and $c_0 \neq 0$. Assume that f has a rational root α. Then α is an integer dividing c_0.

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

By Theorem, possible rational roots of f are ± 1, ± 2, ± 3, ± 6. Moreover, 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 $f(x) = (x+1)(x+2)(x+3)$.