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 coeficients 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.

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 $p(X)$ and $s(X)$ be polynomials and $s(X) \neq 0$. We say that $s(X)$ **divides** $p(X)$ if $p = qs$ for some polynomial $q(X)$. Then q is called the **quotient** of p by s.

Let $p(X)$ and $s(X)$ be polynomials and $s(X)$ be of positive degree. Suppose that $p = qs + r$ for some polynomials q and r such that the degree of r is less than the degree of s. Then r is the **remainder** and q is the (partial) **quotient** of p by s.

Note that $s(X)$ divides $p(X)$ if the remainder is 0.

Theorem Let $p(X)$ and $s(X)$ be polynomials and $s(X)$ be of positive degree. Then the remainder and the quotient of p by s are well-defined. Moreover, they are unique.

Long division of polynomials

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

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

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

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