Kris Harper
MATH 16300
Miklós Abért
April 15, 2008

Sheet 19: Polynomials

Definition 1 *A real polynomial of degree n is a function of the form*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_i \in \mathbb{R}$ $(0 \leq i \leq n)$ and $a_n \neq 0$. If $p(x) = 0$ then we define the degree $\deg p = -\infty$. The set of real polynomials is denoted by $\mathbb{R}[x]$.

Theorem 2 *For all $p, q \in \mathbb{R}[x]$ we have*

$$\deg(p+q) \leq \max(\deg(p), \deg(q))$$

and

$$\deg(pq) = \deg(p) + \deg(q)$$

Proof. Let $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{i=0}^{m} b_i x^i$. Then

$$p + q(x) = p(x) + q(x) = \left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{m} b_i x^i\right)$$

and so $\deg(p+q) = \max(n, m) = \max(\deg(p), \deg(q))$. Also

$$pq(x) = p(x)q(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right)$$

and so using the product of powers $\deg pq = n + m = \deg(p) + \deg(q)$. $\square$

Theorem 3 (Division Remainder) *Let $a, b \in \mathbb{R}[x]$ be polynomials with $b \neq 0$. Then there exists unique $q, r \in \mathbb{R}[x]$ such that*

$$a = bq + r$$

and

$$\deg r < \deg b.$$

Proof. To show existence consider the set $S = \{a - bc \mid c \in \mathbb{R}[x]\}$. Suppose that for all $r \in S$, $\deg(r) \geq \deg(b)$. Choose $p \in S$ such that $\deg(p)$ is the minimum degree of all elements of S using the Well Ordering Principle. Note that $p = a - bc$ for some $c \in \mathbb{R}[x]$. Now let $q = p - bd$ for some $d \in \mathbb{R}[x]$. Then $q = a - bc - bd = a - b(c + d)$ and so $q \in S$. Thus $\deg(q) \geq \deg(p)$. But then if $p(x) = \sum_{i=0}^{n} a_i x^i$ and $b(x) = \sum_{i=0}^{m} b_i x^i$ then consider $d = (a_n/b_m)x^{(n-m)}$. Then $\deg(bd) = n$ and so $\deg(q) < \deg(p)$ since $q = p - bd$. This is a contradiction and so there exists $r \in S$ such that $\deg(r) < \deg(b)$.

For uniqueness suppose that there exists q, q', r, r' with $q \neq q'$ and $r \neq r'$ such that $a = bq + r$, $a = bq' + r'$, $\deg(r) < b$ and $\deg(r') < b$. Then $bq + r = bq' + r'$ and $b(q - q') = r' - r$. Note that since $q \neq q'$ and $r \neq r'$, $\deg(q - q') \geq 0$ and $\deg(r - r') \geq 0$. But then using Theorem 2 we have $\deg(r - r') < b$ and $\deg(b(q - q')) = \deg(b) + \deg(q - q') \geq \deg(b)$ (19.2). This is a contradiction and so $q = q'$ and $r = r'$ which means q and r are unique. $\square$

Definition 4 *We call r the remainder of a divided by b.*

Exercise 5 *Divide x^3+4 by $2x^2-1$ with remainder. Also x^4-1 by x^2-1.*

x^3+4 divided by $2x^2-1$ is $x/2$ with $x/2+4$ as a remainder because $x^3+4 = x^3+x/2-x/2+4 = (2x^2-1)(x/2)+x/2+4$. Also $(x^2-1)(x^2+1) = x^4-1$ so x^4-1 divided by x^2-1 is x^2+1 with no remainder.

Definition 6 *A real number α is a root of $p(x) \in \mathbb{R}[x]$ if $p(\alpha) = 0$.*

Theorem 7 *Let $p, q \in \mathbb{R}[x]$. Then α is a root of pq if and only if α is a root of p or q.*

Proof. Let $p(x) = \sum_{i=0}^n a_i x^i$ and $q(x) = \sum_{i=0}^m b_i x^i$ and suppose that α is a root of p or q. Without loss of generality suppose that α is a root of p. Then $\sum_{i=0}^n a_i \alpha^i = 0$ and so

$$pq(\alpha) = p(\alpha)q(\alpha) = \left(\sum_{i=0}^n a_i \alpha^i\right)\left(\sum_{i=1}^m b_i \alpha^i\right) = 0 \cdot \left(\sum_{i=1}^m b_i \alpha^i\right) = 0$$

which means α is a root of pq. For the converse we use the contrapositive. Suppose that α is not a root of p and q. Then $p(\alpha) \neq 0$ and $q(\alpha) \neq 0$. But then $pq(\alpha) = p(\alpha)q(\alpha) \neq 0$. □

Theorem 8 *Let $p \in \mathbb{R}[x]$. Then α is a root of p if and only if $p = (x-\alpha)q$ for some $q \in \mathbb{R}[x]$.*

Proof. Suppose that $p = (x-\alpha)q$ for some $q \in \mathbb{R}[x]$. Then $p(\alpha) = (\alpha-\alpha)q = 0$ and so α is a root of p. Conversely suppose that α is a root of p. From Theorem 3 we know that $p = (x-\alpha)q + r$ for $q, r \in \mathbb{R}[x]$ and $\deg(r) = 0$ (19.3). Thus r is a constant and since α is a root of p we have $p(\alpha) = (\alpha-\alpha)q + r = r = 0$. Thus $p = (x-\alpha)q$ for some $q \in \mathbb{R}[x]$. □

Theorem 9 *Let $p \in \mathbb{R}[x]$ be a nonzero polynomial of degree n. Then p has at most n roots.*

Proof. Suppose that $\deg(p) = n$ and p has m distinct roots with $m > n$. Let the m roots be $\alpha_1, \alpha_2, \ldots, \alpha_m$. From Theorem 8 we know that $p = (x-\alpha_1)q_1$ for some $q \in \mathbb{R}[x]$ (19.8). From Theorem 7 we know that since α_2 is a root of p it is a root of $(x-\alpha_1)$ or q (19.7). Since $\alpha_2 - \alpha_1 \neq 0$, α_2 is a root of q_1. This $q_1 = (x-\alpha_2)q_2$ and $p = (x-\alpha_1)(x-\alpha_2)q_2$ (19.8). We can continue in this process m times until we have

$$p = \prod_{i=1}^m (x-\alpha_i) q_m.$$

But then $\deg(p) = m \neq n$ which is a contradiction. □

Theorem 10 *For every even n there exists a real polynomial of degree n with no roots. Every real polynomial of odd degree has a root.*

Proof. Let n be even. Consider the polynomial $p(x) = x^n + 1$. Since n is even, $n = 2k$ for some $k \in \mathbb{N}$. Then $p(x) = x^{2k} + 1 = (x^k)^2 + 1$. But then $p(x) > 0$ for all $x \in \mathbb{R}$ and so $p(x)$ has no roots.

Now let p be a polynomial of degree n with n odd such that $p(x) = \sum_{i=0}^n a_i x^i$. Suppose that $a_n > 0$. We know $\lim_{x\to\infty} p(x)/(a_n x^n) = 1$. Let $\varepsilon = 1/2$. Then there exists $m \in \mathbb{R}$ such that for all $x > m$ we have $|p(x)/(a_n x^n) - 1| < 1/2$. Thus there exists $x_1 > 0$ such that $1/2 < p(x_1)/(a_n x_1^n)$. Since $x_1, a_n > 0$ and n is odd we have $0 < (a_n x_1^n)/2 < p(x_1)$. Thus $p(x_1)$ is positive. Similarly take $\lim_{x\to-\infty} p(x)/(a_n x^n) = 1$ and let $\varepsilon = 1/2$. Then there exists $m \in \mathbb{R}$ such that for all $x < m$ we have $|p(x)/(a_n x^n) - 1| < 1/2$. Then there exists $x_2 < 0$ such that $1/2 < p(x)/(a_n x^n)$. But since $x_2 < 0$ and $a_n > 0$ we have $a_n x^n < 0$ so then $p(x) < (a_n x^n)/2 < 0$. Thus $p(x_2) < 0$. Therefore there exist $x_1, x_2 \in \mathbb{R}$ with $p(x_2) < 0$ and $p(x_1) > 0$ so there must exist $c \in (x_2; x_1)$ with $p(c) = 0$ by the Intermediate Value Theorem. A very similar proof holds if $a_n < 0$ where the limits give values of opposite signs as in this proof. □

Theorem 11 (Lagrange Interpolation) *Let $a_1 < a_2 < \cdots < a_n$ and $b_1, b_2, \ldots, b_n$ be real numbers. Then there exists a polynomial $p(x)$ of degree at most $n-1$ such that*

$$p(a_i) = b_i \ (1 \le i \le n).$$

Proof. Consider the polynomial

$$p(x) = \sum_{i=1}^{n} b_i \prod_{j=1, j\neq i}^{n} \frac{(x-a_j)}{(a_i - a_j)}.$$

Note that

$$p(a_k) = \sum_{i=1}^{n} b_i \prod_{j=1, j\neq i}^{n} \frac{(a_k-a_j)}{(a_i - a_j)} = b_k \prod_{j=1, j\neq k}^{n} \frac{(a_k-a_j)}{(a_k - a_j)} = b_k.$$

□

Exercise 12 *Is this polynomial unique?*

Yes.

Proof. Let $a_1 < a_2 < \cdots < a_n$ and $b_1, b_2, \ldots, b_n$ be real numbers. Consider two polynomials $f(x)$ and $g(x)$ such that $f(a_i) = b_i$ and $g(a_i) = b_i$ $(1 \le i \le n)$. Then consider $h(x) = f(x) - g(x)$. We see $h(x) = 0$ for each a_i and so h has n roots. But then $n \le \deg(h) \le \max(\deg(p), \deg(q))$ (19.2, 19.9). Thus $\deg(p)$ or $\deg(q)$ is greater than or equal to n which means there exists only one such polynomial with degree less than n. □

Theorem 13 *Let p be a real polynomial which maps rationals to rationals. Then all the coefficients of p are rational.*

Proof. Take $n+1$ rational points $a_1 < a_2 < \cdots < a_{n+1}$ and their images $p(a_1) = b_1, p_(a_2) = b_2, \ldots, p(a_{n+1}) = b_{n+1}$. From Theorem 11 we know that there exists a polynomial of degree n

$$p'(x) = \sum_{i=1}^{n} b_i \prod_{j=1, j\neq i}^{n} \frac{(x-a_j)}{(a_i - a_j)}$$

such that $p'(a_i) = b_i$ $(1 \le i \le n+1)$ (19.11). Note that the coefficients of p' are all rational because $a_i, b_i \in \mathbb{Q}$ $(1 \le i \le n)$. From Exercise 12 we know that this polynomial is unique and so $p = p'$ (19.12). Thus p has all rational coefficients. □