M7210 Lecture 2. Polynomials August 22, 2012

Let $\mathbb{F}$ be a field (e.g., $\mathbb{Q}$, $\mathbb{R}$ of $\mathbb{C}$). An *polynomial in the variable x with coefficients from* $\mathbb{F}$ is an expression of the form $A = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, written as a sum of elements $a_i \in \mathbb{F}$ times powers of x of increasing degree. $\mathbb{F}[x]$ denotes the set of all such polynomials. We will use capital letters A, B denote elements of $\mathbb{F}[x]$.

The exponent of the highest power of x with non-zero coefficient is called the degree of A. A polynomial of degree 0 is called a constant. $0 \in \mathbb{F}[x]$ is also called a constant, but 0 does not have a degree.

We say A is *monic* if $a_n = 1$. Thus, 1 is the unique monic polynomial of degree 0. Any polynomial of the form $x + a_0$ is monic of degree 1. Etc.

Given a polynomial A and an element $s \in \mathbb{F}$, we may obtain an element of $\mathbb{F}$ by substituting s for x in A and simplifying. This is called *evaluating A at $x = s$.* When we need to evaluate and we want to emphasize the variable and the constant put in its place, we will refer to $A(x)$ and $A(s)$.

The Polynomial Remainder Theorem, Part 1. *Suppose $A, B \in \mathbb{F}[x]$, $B \neq 0$. Then, there are unique $Q, R \in \mathbb{F}[x]$ such that:*

$$A = Q\,B + R \quad \textit{and:} \quad R = 0 \quad \textit{or} \quad \deg R < \deg B. \tag{$*$}$$

Proof of existence. If $A = 0$, we get $(*)$ by letting $R = Q = 0$. If $\deg B > \deg A$, then regardless of the degree of A we can take $Q = 0$ and $R = B$. We are left to prove the theorem under the assumption that $A \neq 0$ and $\deg B \leq \deg A$. We use induction on $n = \deg A$. If $\deg A = 0$ and $\deg B = 0$ we take $Q = A/B$ and $R = 0$. Assume the theorem is true for all A' with $\deg A' < n$. Suppose $A = a_nx^n + \cdots + a_0$ and $B = b_m\,x^m + \cdots + a_0$, with $m \leq n$. Let $Q_0 = (a_n/b_m)x^{n-m}$. Then $A - Q_0B$ has degree $< n$, so

$$A - Q_0B = Q_1B + R \quad \text{ with } R = 0 \text{ or } \deg R < \deg B.$$

It follows that $A = (Q_0 + Q_1)B + R$.

Proof of uniqueness. Suppose Q' and R' also satisfy $(*)$. Then $Q\,B + R = Q'\,B + R'$, so $(Q - Q')\,B = R - R'$. Now, $\deg(R - R') < \deg B$, and this implies $Q - Q' = 0$. It follows that $R = R'$. /////

Definition. Suppose $A, B \in \mathbb{F}[x]$.
- *A divides B*—in symbols, $A|B$—means: there is $K \in \mathbb{F}[x]$ such that $K\,A = B$.
- We say *D is a common divisor of A and B* if $D|A$ and $D|B$.

The Polynomial Remainder Theorem, Part 2. *Suppose $0 \neq A(x) \in \mathbb{F}[x]$, and $s \in \mathbb{F}$. Then $(x - s)|A(x)$ iff $A(s) = 0$.*

Proof. By Part 1, $A(x) = Q(x)(x - s) + r$, where $r \in \mathbb{F}$. If we substitute s for x, we get $A(s) = r$. /////

The Euclidean Algorithm for $\mathbb{F}[x]$ is exactly parallel to the Euclidean Algorithm for integers, with the condition on degree in place of the condition on absolute value. Given polynomials R_{-1} and $R_0 \neq 0$, we can get a sequence of remainders R_i as follows:

$$\begin{aligned}
R_{-1} &= Q_1 R_0 + R_1 \quad \text{and} \quad \deg R_1 < \deg R_0 \\
R_0 &= Q_2\, R_1 + R_2 \quad \text{and} \quad \deg R_2 < \deg R_1 \\
&\vdots \\
R_{i-1} &= Q_{i+1}\, R_i + R_{i+1} \quad \text{and} \quad \deg R_{i+1} < \deg R_i
\end{aligned}$$

The process leads to a sequence $R_0, R_1, \dots, R_{n+1}$ with $\deg R_0 > \deg R_1 > \cdots > \deg R_n$ and $R_{n+1} = 0$. /////

Lemma 1. *There are $U, V \in \mathbb{F}[x]$ with the property that*

$$U\,R_{-1} + V\,R_0 = R_n. \qquad /////$$

Lemma 2. *There are $U, V \in \mathbb{F}[x]$ such that*

$$U\,R_n = R_{-1} \quad \text{and} \quad V\,R_n = R_0. \qquad /////$$

Lemma 3. *R_n is a common divisor of R_{-1} and R_0, and every common divisor of R_{-1} and R_0 divides R_n.*

Definition. Suppose R_n has degree k and leading coefficient r_k. Then we call R_n/r_k the *greatest common divisor* of R_{-1} and R_0 and denote it $\gcd(R_{-1}, R_0)$.

Theorem. *Let h be the highest degree of any common divisor of $A, B \in \mathbb{F}[x]$. Then, $h = \deg \gcd(A, B)$, and any common divisor of A and B of degree h is a constant multiple of $\gcd(A, B)$.*

Corollary 1. *Suppose $C, M, N \in \mathbb{F}[x]$. If $C|MN$ and $\gcd(C, M) = 1$, then $C|M$*

Corollary 2. *Suppose $A, B, M \in \mathbb{F}[x]$. If $\gcd(A, B) = 1$, $A|M$ and $B|M$, then $AB|M$.*

Definition. $P \in \mathbb{F}[x]$ is called *prime* if $P \neq 0$ and $\deg P > 0$ and $P = A\,B$ for some $A, B \in \mathbb{F}[x]$ implies either A or B is a constant.

Lemma 4. *If P is prime and $P|A\,B$, then $P|A$ or $P|B$.*

Lemma 5. *For all non-constant $K \in \mathbb{F}[x]$:*

either K is prime or K is a product of (finitely many) primes. $(\dagger_K)$

Lemma 6. *Suppose P_i, $i = 1, \dots, m$ and Q_j, $j = 1, \dots, n$ are monic prime elements of $\mathbb{F}[x]$. If $\prod_{i=1}^m P_i = \prod_{j=1}^n Q_j$, then $m = n$ and after renumbering, $P_i = Q_i$ for $i = 1, \dots, m$.*

Homework.

1) Prove the lemmas, theorem and corollaries above.
2) Find $\gcd(-9 - 6x - 3x^2 + 9x^3 + 6x^4 + 3x^5, -3 + 13x + 15x^2 + 15x^3 + 7x^5 + 4x^6 + 3x^7)$.