



Exercises on Polynomial Division

(Handout February 12, 2007)

The set of all polynomials in X with rational coefficients is denoted $\mathbb{Q}[X]$. The **degree** of a polynomial $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m \in \mathbb{Q}[X]$ is m , assuming that $a_m \neq 0$. Here we call a_mX^m the **leading term** of $f(X)$; and we call a_m the **leading coefficient**. We say $f(X)$ is **monic** if its leading coefficient is 1. Observe that every polynomial, *except* the zero polynomial, has a leading term. We also define the degree of the zero polynomial to be $-\infty$, so that the rule $\deg(f(X)g(X)) = \deg f(X) + \deg g(X)$ holds in all cases (and is easily verified by comparing terms of highest degree in $f(X)$, $g(X)$, and $f(X)g(X)$). Given two polynomials $f(X), g(X) \in \mathbb{Q}[X]$, we say that $f(X)$ **divides** $g(X)$ (denoted $f(X) \mid g(X)$) if $g(X) = a(X)f(X)$ for some $a(X) \in \mathbb{Q}[X]$.

Theorem 1 (Division Algorithm). *Let $f(X), d(X) \in \mathbb{Q}[X]$ where $d(X) \neq 0$. Then there exist unique polynomials $q(X), r(X) \in \mathbb{Q}[X]$ satisfying*

$$f(X) = q(X)d(X) + r(X), \quad \deg r(X) < \deg d(X).$$

In the latter relation, we call $d(X)$ the **divisor**; $q(X)$ the **quotient**; and $r(X)$ the **remainder** upon dividing $f(X)$ by $d(X)$. Note that $d(X)$ divides $f(X)$ if and only if the remainder $r(X) = 0$. Several straightforward facts about divisibility of polynomials are evident (as their proofs are the same as the proofs of corresponding facts about divisibility of integers) and may be freely used. For example we have

Theorem 2. *Let $f(X), g(X), d(X) \in \mathbb{Q}[X]$, and suppose that $d(X)$ divides both $f(X)$ and $g(X)$. Then $d(X)$ divides both $f(X)+g(X)$ and $f(X)-g(X)$. Moreover $d(X)$ divides every multiple of $f(X)$.*

Let $f(X), g(X) \in \mathbb{Q}[X]$ and suppose that $f(X)$ and $g(X)$ are *not both* zero. The **greatest common divisor** of $f(X)$ and $g(X)$, denoted $\gcd(f(X), g(X))$, is the unique monic polynomial of maximum possible degree, which divides both $f(X)$ and $g(X)$. In particular if $\gcd(f(X), g(X)) = 1$, we say that $f(X)$ and $g(X)$ are **relatively prime**. On the previous handout we gave a computational example of the following important result, which directly parallels the Euclidean algorithm for \mathbb{Z} .

Theorem 3 (Euclid's Algorithm). Let $a(X), b(X) \in \mathbb{Q}[X]$ be polynomials, not both zero; and let $g(X) = \gcd(a(X), b(X))$. Then there exist $m(X), n(X) \in \mathbb{Q}[X]$ such that $g(X) = m(X)a(X) + n(X)b(X)$.

HOMEWORK #3 Due Mon Feb 19

1. Let $a(X) = 4X^2 - 3X - 1$ and $b(X) = X^3 + 5X^2 + 2X + 7$. Determine $g(X) = \gcd(a(X), b(X))$, and find polynomials $m(X), n(X)$ such that $g(X) = m(X)a(X) + n(X)b(X)$.
2. Let $f(X), g(X), d(X) \in \mathbb{Q}(X)$ where $d(X) \neq 0$, and suppose $d(X) \mid f(X)g(X)$. If $d(X)$ and $f(X)$ are relatively prime, show that $d(X)$ divides $g(X)$.
(*Hint:* Imitate the steps used in class to prove Euclid's Lemma.)