The Division Algorithm for Polynomials

Let $F$ be a field (such as $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, or $\mathbb{F}_p$ for some prime $p$). This will allow us to divide by any nonzero scalar. (For some of the following, it is sufficient to choose a ring of constants; but in order for the Division Algorithm for Polynomials to hold, we need to be able to divide constants.) For much of the following, you can pretend that $F = \mathbb{Q}$.

Recall that a polynomial in $x$ is an expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $x$ is a symbol and $a_0, a_1, \ldots, a_n \in F$. We say that $a_k$ is the coefficient of $x^k$, for $k = 0, 1, 2, \ldots, n$. Let $F[x]$ denote the set of all polynomials in $x$, with coefficients in $F$. (Thus, for example, $\mathbb{R}[x]$ is the set of polynomials in $x$ with real coefficients.) The zero polynomial, denoted by $0$, is the polynomial whose coefficients are all zero. Two polynomials $f(x)$ and $g(x)$ are the same, denoted $f(x) = g(x)$, if their corresponding coefficients are the same; for example,

$$1 - 2x + 5x^3 = 5x^3 - 2x + 1 = 1 - 2x + 0x^2 + 5x^3 = 0x^4 + 5x^3 + 0x^2 - 2x + 1.$$ 

In particular, we write $f(x) = 0$ if and only if all coefficients of $f(x)$ are zero, thus for example, $x^2 - 1 \neq 0$. If $h(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \neq 0$, the degree of $h(x)$, denoted by $\deg h(x)$, is the largest $k$ such that $a_k \neq 0$. For example, $\deg (1 - 2x + 5x^3) = 3$, $\deg (2x - 0x^2) = 1$, $\deg (-8) = 0$. We define $\deg 0 = -\infty$ so that the following proposition holds universally for all polynomials $f(x), g(x)$, with the obvious conventions for adding $-\infty$.

**Proposition 1.** If $f(x), g(x) \in F[x]$ then $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

**Proof.** If either of the two polynomials $f(x), g(x)$ is zero, then $f(x)g(x) = 0$ and the desired equality holds, with both sides equal to $-\infty$ by convention. We may therefore assume $f(x)$ and $g(x)$ are nonzero polynomials. Now

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n; \quad g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$$

where $n = \deg f(x)$ and $m = \deg g(x)$; in particular, $a_n \neq 0$ and $b_m \neq 0$. Thus

$$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{n+m}$$
where the last term is the unique term of highest degree in \( f(x)g(x) \), with coefficient \( a_nb_m \neq 0 \); thus
\[
\deg (f(x)g(x)) = n + m = \deg f(x) + \deg g(x).
\]

We say that \( f(x) \) divides \( g(x) \) in \( F[x] \), denoted \( f(x) \mid g(x) \), if \( g(x) = m(x)f(x) \) for some \( m(x) \in F[x] \). The following is obviously analogous to the Division Algorithm for Integers. We omit the proof, which we take to be evident from the usual algorithm of long division.

**Theorem 2 (Division Algorithm for Polynomials).** Let \( f(x), d(x) \in F[x] \) such that \( d(x) \neq 0 \). Then there exist unique polynomials \( q(x), r(x) \in F[x] \) such that
\[
f(x) = q(x)d(x) + r(x), \quad \deg r(x) < \deg d(x).
\]

As usual ‘unique’ means that there is only one pair of polynomials \((q(x), r(x))\) satisfying the conclusions of the theorem. We call \( q(x) \) and \( r(x) \) the quotient and remainder, respectively. Note that \( a(x) \mid b(x) \) if and only if \( r(x) = 0 \). Note that the Division Algorithm holds in \( F[x] \) for any field \( F \); it does not hold in \( \mathbb{Z}[x] \), the set of polynomials in \( x \) with integer coefficients.

**Proof of Theorem 2.** Consider the set of polynomials \( S = \{ f(x) - q(x)d(x) : q(x) \in F[x] \} \subseteq F[x] \). Since \( S \) is nonempty, it contains an element of minimal degree (the smallest degree of any element in \( S \)). Let \( k \) be the minimal degree of elements of \( S \), and let \( q(x) \in F[x] \) such that the polynomial \( r(x) = f(x) - q(x)d(x) \in S \) has this minimal degree \( k \).

We may assume \( d(x) = d_0 + d_1x + \cdots + d_nx^n \) where \( n \geq 0 \) and \( d_n \neq 0 \). If \( k \geq n \) then \( r(x) \) has leading term \( r_kx^k \) and the polynomial
\[
r(x) - \frac{cr_k}{d_n}x^{k-n}d(x) = f(x) - [q(x) - \frac{cr_k}{d_n}x^{k-n}]d(x) \in S
\]
has degree less than \( k \) due to cancellation of the degree \( k \) terms. However this is contrary to the choice of \( r(x) \in S \) as the element of smallest degree. So we must in fact have \( k < n \), i.e. \( \deg r(x) < \deg d(x) \).

Finally, to show uniqueness of the solution \((q(x), r(x))\) above, observe that for every nonzero polynomial \( h(x) \),
\[
f(x) - [q(x) + h(x)]d(x) = r(x) - h(x)d(x)
\]
has degree at least \( n \) since \( \deg (h(x)d(x)) \geq \deg d(x) = n > k = \deg r(x) \). This completes the proof.

\[ \Box \]
A zero or root of \( f(x) \) is a number \( a \) such that \( f(a) = 0 \). An important consequence of the Division Algorithm is the fact (made explicit by the following theorem) that roots of polynomials correspond to linear factors.

**Theorem 3.** Let \( f(x) \in F[x] \) and \( a \in F \). Then \( f(a) = 0 \) if and only if \( (x - a) \mid f(x) \).

**Proof.** If \( (x - a) \mid f(x) \) then \( f(x) = (x - a)m(x) \) for some \( m(x) \in F[x] \), and so \( f(a) = 0 \).

Conversely, suppose \( f(a) = 0 \). By the Division Algorithm, we may write \( f(x) = (x - a)q(x) + r(x) \) for some \( q(x), r(x) \in F[x] \) where \( r(x) \) has degree less than 1 (the degree of \( x - a \)). If \( r(x) = 0 \) then we would have \( (x - a) \mid f(x) \), and so we would be done. So let’s assume instead that \( r(x) \neq 0 \), in which case \( \deg r(x) = 0 \), so \( r = r(x) \) is a nonzero constant. Substituting \( a \) for \( x \) gives \( 0 = f(a) = 0m(a) + r \), so \( r = 0 \). This contradiction proves that in fact \( (x - a) \mid f(x) \).

This argument extends to multiple roots:

**Theorem 4.** If \( f(x) \in F[x] \) has distinct roots \( a_1, a_2, \ldots, a_n \), then \( f(x) \) is divisible by \( (x - a_1)(x - a_2) \cdots (x - a_n) \). In particular, either \( f(x) \neq 0 \) or \( \deg f(x) \geq n \).

**Proof.** Suppose \( f(x) \) has at least \( n \) distinct roots \( a_1, a_2, \ldots, a_n \). By Theorem 3, we have \( f(x) = (x - a_1)g(x) \) for some \( g(x) \in F[x] \). Substituting \( a_2 \) for \( x \) gives \( 0 = f(a_2) = (a_2 - a_1)g(a_2) \) where \( a_2 - a_1 \neq 0 \) since the \( n \) roots are distinct. Therefore \( g(a_2) = 0 \), and by Theorem 3 we have \( g(x) = (x - a_2)h(x) \) for some \( h(x) \in F[x] \). Thus \( f(x) = (x - a_1)(x - a_2)h(x) \). Continuing in this way, we eventually obtain \( f(x) = (x - a_1)(x - a_2)(x - a_3) \cdots (x - a_n)m(x) \) for some \( m(x) \in F[x] \).

**Corollary 5.** A nonzero polynomial \( f(x) \in F[x] \) of degree \( n \) cannot have more than \( n \) distinct roots.

From Proposition 1 it follows easily that the units of the ring \( F[x] \) are the nonzero constant polynomials, i.e. \( F[x]^\times = F^\times \). A polynomial \( f(x) \in F[x] \) is monic if its leading coefficient is 1. Every nonzero polynomial in \( F[x] \) is uniquely expressible as \( cf(x) \) where \( c \in F^\times \) and \( f(x) \) is monic. Thus every nonzero polynomial in \( F[x] \) has a unique monic associate.

The notion of gcd for integers, generalizes to polynomials as follows. Given two polynomials \( f(x), g(x) \in F[x] \), not both zero, we define the greatest common divisor (denoted
$\gcd(f(x), g(x))$ to be the unique monic polynomial of highest degree dividing both $f(x)$ and $g(x)$. Consider the following example:

The divisors of $f(x) = 2x^2 - \frac{1}{2} = 2(x + \frac{1}{2})(x - \frac{1}{2}) \in \mathbb{Q}[x]$ are all polynomials of the form

$$c; \ c(x + \frac{1}{2}); \ c(x - \frac{1}{2}); \ c(x + \frac{1}{2})(x - \frac{1}{2})$$

where $c$ is an arbitrary nonzero constant. The divisors of $g(x) = 2x^2 - 3x + 1 = (2x - 1)(x - 1) = 2(x - \frac{1}{2})(x - 1)$ are

$$c; \ c(x - \frac{1}{2}); \ c(x - 1); \ c(x - \frac{1}{2})(x - 1)$$

where $c$ is an arbitrary nonzero constant. The common divisors of $f(x)$ and $g(x)$ have the form

$$c; \ c(x - \frac{1}{2})$$

where $c$ is an arbitrary nonzero constant. The polynomials of highest degree dividing both $f(x)$ and $g(x)$ have the form $c(x - \frac{1}{2})$ where $c$ is a nonzero constant. In order that the greatest common divisor of $f(x)$ and $g(x)$ be well-defined, we choose $c = 1$ so that the answer is monic; thus

$$\gcd(f(x), g(x)) = \gcd(2x^2 - \frac{1}{2}, 2x^2 - 3x + 1) = x - \frac{1}{2}.$$

The computation of $\gcd(f(x), g(x))$ does not require knowing how to factorize polynomials; instead, we use Euclid’s Algorithm, just as we did with integers. This algorithm, in its extended form, also expresses $\gcd(f(x), g(x))$ as a ‘polynomial-linear combination’ of $f(x)$ and $g(x)$:

**Theorem 6 (Euclid’s Algorithm for Polynomials).** Let $f(x), g(x) \in F[x]$ be polynomials, not both zero. Then there exist polynomials $r(x), s(x) \in F[x]$ such that

$$r(x)f(x) + s(x)g(x) = \gcd(f(x), g(x)).$$

For example, we compute the gcd of the polynomials $f(x) = 5x^3 + 2x^2 + 3x - 10$, $g(x) = x^3 + 2x^2 - 5x + 2 \in \mathbb{Q}[x]$. The steps are almost the same as when computing the gcd of two integers. We proceed to repeatedly apply the Division Algorithm:

$$f(x) = 5g(x) + (-8x^2 + 28x - 20)$$

$$g(x) = (-\frac{1}{5}x - \frac{11}{10})(-8x^2 + 28x - 20) + (\frac{47}{4}x - \frac{47}{4})$$

$$-8x^2 + 28x - 20 = \frac{4}{47}(-8x + 20)(\frac{47}{4}x - \frac{47}{4}) + 0$$
Here the last nonzero remainder is $\gcd(f(x), g(x)) = \frac{47}{4}x - \frac{47}{4} = \frac{47}{4}(x - 1)$. Any common divisor of $f(x)$ and $g(x)$ has degree at most 1; and in order that the gcd be well-defined, we scale it to obtain the monic polynomial $\gcd(f(x), g(x)) = x - 1$. The extended form of the algorithm allows us to write this as a polynomial-linear combination of $f(x)$ and $g(x)$:

$$\frac{47}{4}x - \frac{47}{4} = g(x) - (-\frac{1}{8}x - \frac{11}{16})(-8x^2 + 28x - 20);$$

$$x - 1 = \frac{47}{4}g(x) + (\frac{94}{91}x + \frac{11}{188})(-8x^2 + 28x - 20)$$

$$= \frac{47}{4}g(x) + (\frac{94}{91}x + \frac{11}{188})(f(x) - 5g(x))$$

$$= (\frac{1}{94}x + \frac{11}{188})f(x) + (-\frac{5}{94}x - \frac{39}{188})g(x).$$

Ugly fractions like this are to be expected when working over $\mathbb{Q}$. Life is much easier working over $\mathbb{F}_p$, when coefficients are more simply expressed as elements of $\{0,1,2,\ldots,p-1\}$. Consider what happens to the preceding example over $\mathbb{F}_7$:

$$f(x) = 5x^3 + 2x^2 + 3x + 4,$$

$$g(x) = x^3 + 2x^2 + 2x + 2;$$

$$f(x) = 5g(x) + (6x^2 + 1)$$

$$g(x) = (6x + 5)(6x^2 + 1) + (3x + 4)$$

$$6x^2 + 1 = 5(6x + 1)(3x + 4) + 0$$

so from $3x + 4 = 3(x + 6)$ we obtain $\gcd(f(x), g(x)) = x + 6$ over $\mathbb{F}_7$. The extended version of Euclid’s Algorithm over $\mathbb{F}_7$ is also not hard:

$$3x + 4 = 3(x + 6) = g(x) - (6x + 5)(6x^2 + 1);$$

$$x + 6 = 5g(x) + (5x + 3)(6x^2 + 1)$$

$$= 5g(x) + (5x + 3)(f(x) - 5g(x))$$

$$= (5x + 3)f(x) + (3x + 4)g(x).$$

Alternatively, we use coefficient matrices as we did in $\mathbb{Z}$ to reduce the amount of writing involved:

<table>
<thead>
<tr>
<th>$f(x)$</th>
<th>$g(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>$5x^3 + 2x^2 + 3x + 4$</td>
</tr>
<tr>
<td>1</td>
<td>$x^3 + 2x^2 + 2x + 2$</td>
</tr>
<tr>
<td>$x + 2$</td>
<td>$2x + 5$</td>
</tr>
<tr>
<td>$5x^2 + x + 4$</td>
<td>$3x + 4$</td>
</tr>
<tr>
<td>$3x^2 + 6$</td>
<td>0</td>
</tr>
</tbody>
</table>

where the last nonzero entry in the third column is $3x + 4 = (x + 2)f(x) + (2x + 5)g(x)$; and after multiplying by 5 we obtain

$$\gcd(f(x), g(x)) = x + 6 = (5x + 3)f(x) + (3x + 4)g(x).$$
It is important to understand how this works (and to be prepared to perform simple versions of this on a test) in the same way that we expect you to be able (in principle) to perform arithmetic (including multiplication and division of large integers). However, there is little point in repeatedly performing such operations by hand once the principles are mastered. For this we may use a symbolic computational software such as Maple:

```
It is important to understand how this works (and to be prepared to perform simple versions of this on a test) in the same way that we expect you to be able (in principle) to perform arithmetic (including multiplication and division of large integers). However, there is little point in repeatedly performing such operations by hand once the principles are mastered. For this we may use a symbolic computational software such as Maple:

```

According to the general definition of irreducibility in rings, we note that an irreducible polynomial in $F[x]$ is a polynomial of degree $k \geq 1$ all of whose divisors have degree 0 or $k$. The property of irreducibility is relative to the choice of field $F$; for example, $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, but not in $\mathbb{R}[x]$ where it factors as $(x + \sqrt{2})(x - \sqrt{2})$. The polynomial $x^2 + 1$ is irreducible in both $\mathbb{Q}[x]$ and $\mathbb{R}[x]$, but not in $\mathbb{C}[x]$ where it factors as $(x + i)(x - i)$, $i = \sqrt{-1}$. Recall Euclid’s Lemma for Integers, which states that a prime $p$ divides a product of two integers $ab$, iff $p \mid a$ or $p \mid b$. (As usual, this is an inclusive ‘or’: we allow the possibility that both $a$ and $b$ are divisible by $p$.) This fact extends to polynomials, with the same proof.
**Theorem 7 (Euclid’s Lemma).** Let \( p(x) \in F[x] \) be irreducible, and consider two polynomials \( f(x), g(x) \in F[x] \). If \( f(x)g(x) \) is divisible by \( p(x) \), then \( p(x) \mid f(x) \) or \( p(x) \mid g(x) \).

*Proof.* Suppose that \( p(x) \nmid f(x) \); we must prove that \( p(x) \mid g(x) \). Since \( p(x) \nmid f(x) \) where \( p(x) \) is irreducible, we have \( \gcd(p(x), f(x)) = 1 \). By Euclid’s Algorithm, there exist \( r(x), s(x) \in F[x] \) such that

\[
1 = r(x)p(x) + s(x)f(x).
\]

Then

\[
g(x) = [g(x)r(x)]p(x) + s(x)[f(x)g(x)]
\]

is divisible by \( p(x) \) as required.

A consequence of Euclid’s Lemma is the fact that every polynomial has an essentially unique factorization into irreducible factors. By ‘essentially unique’, we mean the factorization is unique except for constant scalar multiples. If we factor out the coefficient of the leading term, and then use only monic irreducible factors, then the factorization is unique. This is the analogue (for polynomials) of the Fundamental Theorem of Arithmetic (the fact that every positive integer has a unique factorization as a product of primes).

As a further example of the Extended Euclidean Algorithm, in class we considered

\[
f(x) = 5x^3 + 2x^2 + 3x + 4, \quad g(x) = x^3 + 2x^2 + 2x + 2
\]

in \( \mathbb{Q}[x] \). This example, while very similar to the example above, is more typical in that \( f(x) \) and \( g(x) \) are relatively prime. We compute

<table>
<thead>
<tr>
<th>( f(x) )</th>
<th>( g(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>-5</td>
</tr>
<tr>
<td>( \frac{1}{8}x + \frac{9}{64} )</td>
<td>( -\frac{5}{8}x + \frac{19}{64} )</td>
</tr>
<tr>
<td>( \frac{64}{17}x^2 - \frac{2560}{289}x - \frac{3968}{289} )</td>
<td>( -\frac{320}{17}x^2 + \frac{21504}{289}x - \frac{10432}{289} )</td>
</tr>
<tr>
<td>(-\frac{17}{574}x^2 + \frac{20}{287}x + \frac{31}{287} )</td>
<td>( \frac{85}{574}x^2 - \frac{24}{41}x + \frac{163}{574} )</td>
</tr>
</tbody>
</table>

which says that

\[
\gcd(f(x), g(x)) = 1 = \left(-\frac{17}{574}x^2 + \frac{20}{287}x + \frac{31}{287}\right)f(x) + \left(\frac{85}{574}x^2 - \frac{24}{41}x + \frac{163}{574}\right)g(x).
\]