Math 4030-001/Foundations of Algebra/Fall 2017

Polynomials at the Foundations: Rational Coefficients

The rational numbers are our first **field**, meaning that all the laws of arithmetic hold, every number has an additive inverse and every number except the additive identity (zero) has a multiplicative inverse. We explore here the arithmetic of **polynomials** with coefficients in the field of rational numbers and draw a series of close analogies with the arithmetic of the integers.

Definition 7.1. $\mathbb{Q}[x]$ is the set of polynomials with coefficients in $\mathbb{Q}$.

Each polynomial $f(x) \in \mathbb{Q}[x]$ except for $f(x) = 0$ has the form:

$$f(x) = r_d x^d + r_{d-1} x^{d-1} + \cdots + r_0$$

where the coefficients $r_0, ..., r_d$ are rational numbers and $r_d \neq 0$.

Definition 7.2. The **degree** of $f(x) = r_d x^d + \cdots + r_0$ is d.

Remark. Polynomials of degree 0 are also called (non-zero) constants, polynomials of degrees 1, 2 and 3 are called linear, quadratic and cubic, respectively. The zero polynomial $f(x) = 0$ is the only polynomial not to fit the pattern, and its degree is undefined.

The structure of a polynomial resembles that of a natural number.

Natural Number	Polynomial
Digits	Coefficients
10^ds place	x^d

so, for instance:

$$\frac{1}{3}x^3 + 2x - \frac{1}{2} = \frac{1}{3}x^3 + 0x^2 + 2x - \frac{1}{2}$$

is analogous to a four-digit number with "digits" $1/3, 0, 2$ and $-1/2$.

Remark. We lose the bracket notation and refer to the rational number [1/3] as 1/3, always remembering the naming problem: $1/3 = 2/6 = ...$

Addition of polynomials is completely determined by:

$$r_d x^d + s_d x^d = (r_d + s_d)x^d$$

In other words, addition is done "place" by "place" with no carrying.

Example.

$$\begin{array}{rrrrrrrr} & \frac{1}{2}x^3 & + & 3x^2 & + & 0x & - & \frac{1}{4} \\ + & & & -\frac{1}{3}x^2 & - & 2x & + & 1 \\ \hline & \frac{1}{2}x^3 & + & \frac{8}{3}x^2 & - & 2x & + & \frac{3}{4} \end{array}$$

Proposition 7.3.

(a) Addition of polynomials is associative and commutative.

(b) The zero polynomial $f(z) = 0$ is the additive identity, and

(c) The additive inverse of $f(x)$ is $-f(x)$.

Remark. This all immediately follows from the arithmetic of $\mathbb{Q}$.

Multiplication of polynomials is completely determined by:

$$(r_d x^d)(s_e x^e) = (r_d s_e)x^{d+e}$$

and the distributive law. Once again, this is exactly analogous to the multiplication of many-digit numbers, but with no carrying.

Example.

$$\begin{array}{rrrrrrrr} & & & x^2 & - & x & + & 1 \\ \times & & & & & 2x & - & 1 \\ \hline & & - & x^2 & + & x & - & 1 \\ & 2x^3 & - & 2x^2 & + & 2x & & \\ \hline & 2x^3 & - & 3x^2 & + & 3x & - & 1 \end{array}$$

Proposition 7.4.

(a) Multiplication of polynomials is associative, commutative and distributes with addition.

(b) The constant polynomial $f(x) = 1$ is the multiplicative identity.

(c) The product of two polynomials satisfies:

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$

(d) The non-zero constant polynomials are the only polynomials with multiplicative inverses.

Proof. (a) and (b) follow from the fact that $\mathbb{Q}$ is a field.

For (c), if $f(x) = r_d x^d + \cdots + r_0$ and $g(x) = s_e x^e + \cdots + s_0$, then

$$f(x)g(x) = (r_d s_e)x^{d+e} + \text{terms with lower place values}$$

so the degree of $f(x)g(x)$ is $d + e$ provided that $r_d s_e \neq 0$. But since $r_d \neq 0$ and $s_e \neq 0$, it follows that they both have multiplicative inverses ($\mathbb{Q}$ is a field!) and $(1/r_d)(1/s_e)(r_d s_e) = 1$, so $r_d s_e \neq 0$.

For (d), suppose $g(x)$ is the multiplicative inverse of $f(x)$. Then $f(x) \cdot g(x) = 1$, so by (c), $\deg(f(x)) + \deg(g(x)) = 0$ and then it follows that $\deg(f(x)) = 0$ and $\deg(g(x)) = 0$, since there are no polynomials with negative degrees. $\square$

Remark. In particular, (c) shows that $f(x) \cdot g(x)$ can only be the zero polynomial if $f(x) = 0$ or $g(x) = 0$.

Definition 7.5. (a) A set together with addition and multiplication that satisfies all commutative, associative and distributive laws, has an additive identity (0), a multiplicative identity (1) and additive inverses (but not necessarily multiplicative inverses) to all elements is called a **Commutative Ring**.

(b) The elements of a commutative ring with multiplicative inverses are called the **units** of the ring.

Example. $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{Q}[x]$ are all commutative rings with 1. $\mathbb{N}$ is not.

(a) The units of $\mathbb{Z}$ are 1 and -1.

(b) Every element of $\mathbb{Q}$ except for 0 is a unit.

(c) The units of $\mathbb{Q}[x]$ are the constant (non-zero) polynomials.

Division with Remainders is also a feature of $\mathbb{Q}[x]$. Namely, given $f(x)$ and $g(x)$, of degrees $d > e$, respectively, then there is a quotient polynomial $q(x)$ such that either:

(i) $f(x) = q(x)g(x)$, in which case we say $g(x)$ **divides** $f(x)$, or else

(ii) $f(x) = q(x)g(x) + r(x)$ for a remainder $r(x)$ with $\deg(r(x)) < e$.

Proof. Suppose $f(x) = r_d x^d + \cdots r_0$ and $g(x) = s_e x^e + \cdots s_0$. We prove this with the "long division algorithm."

Initialize. Set $q(x) = (r_d/s_e)x^{d-e}$ and let $r(x) = f(x) - q(x)g(x)$.

Loop. If $\deg(r(x)) < e$ (or $r(x) = 0$), STOP. Otherwise,

$$r(x) = t_f x^f + ... + t_0$$

so add $(t_f/s_e)x^{f-e}$ to $q(x)$ and reset $r(x) = f(x) - q(x)g(x)$. REPEAT.

Remark. This is exactly the long division algorithm for polynomials, and it is a perfect analogue of the (harder!) long division algorithm used for dividing natural numbers with many digits. This one is easier because the terms of the polynomial $q(x)$ are so easy to find.

Examples. (a) $x + 1$ does not divide $x^2 + 1$ since:

$$x^2 + 1 = (x - 1)(x + 1) + 2$$

has a non-zero remainder.

(b) $x + 1$ **does** divide $x^3 + 1$ since:

$$x^3 + 1 = (x^2 - x + 1)(x + 1)$$

has no remainder.

Euclid's Algorithm can now be applied to polynomials in $\mathbb{Q}[x]$.

Definition 7.6. Any polynomial of maximum degree that divides both $f(x)$ and $g(x)$ is called a gcd of $f(x)$ and $g(x)$.

Remark. If $h(x)$ is a gcd of $f(x)$ and $g(x)$, then $u \cdot h(x)$ is another gcd, whenever u is any unit polynomial (non-zero constant) because:

$$h(x) = (1/u)(u \cdot h(x))$$

(so $u \cdot h(x)$ divides $h(x)$, and thus also divides $f(x)$ and $g(x)$). We will see that this is the **only** ambiguity in the gcd.

Example. $x - 1$ is a gcd of $x^2 - 1$ and $x^3 - 1$, but so are:

$$2x - 2, -x + 1, -\frac{1}{2}x + \frac{1}{2}, \text{ etc}$$

Euclid's Algorithm and Extras. The following algorithm produces a gcd $h(x)$ of $f(x)$ and $g(x)$ and **also** solves the equation:

$$a(x)f(x) + b(x)g(x) = h(x)$$

It is *exactly the same* as Euclid's algorithm for natural numbers!

Initialize. Set $f_0(x) = f(x)$ and $g_0(x) = g(x)$ (to be fixed throughout). Initialize two equations:

$$a_1(x)f_0(x) + b_1(x)g_0(x) = f(x)$$

$$a_2(x)f_0(x) + b_2(x)g_0(x) = g(x)$$

by initializing $a_1(x) = 1, b_1(x) = 0, a_2(x) = 0, b_2(x) = 1$.

Loop. Use division with remainders to solve:

$$g(x) = q(x)f(x) + r(x)$$

If $r(x) = 0$, STOP. Return $f(x)$ and $a_2(x)f_0(x) + b_2(x)g_0(x) = f(x)$. OTHERWISE, update the two equations via:

$$\begin{array}{rcrcl} (a_2(x) - q(x)a_1(x))f_0(x) & + & (b_2(x) - q(x)b_1(x))g_0(x) & = & r(x) \\ a_1(x)f_0(x) & + & b_1(x)g_0(x) & = & f(x) \end{array}$$

and reset $g(x) := f(x)$ and $f(x) := r(x)$. REPEAT.

Remark. Since the degrees of the remainder polynomials decrease with each iteration of the loop, Euclid's algorithm eventually terminates. The argument for why it terminates in a gcd is the same as with the integers. But that argument shows more, namely:

Corollary 7.6. Every polynomial that divides both $f(x)$ and $g(x)$ divides the output of Euclid's algorithm.

As a consequence, if $h(x)$ is the output of Euclid's algorithm, and $d(x)$ is another gcd, which is necessarily of the **same** degree, then

$$d(x)k(x) = h(x)$$

and then by Proposition 7.4, $k(x)$ is a constant polynomial, i.e. a unit.

Example. Run Euclid's enhanced algorithm on $x^5 - 1$ and $x^7 - 1$

Initialize: $f_0(x) = x^5 - 1, g_0(x) = x^7 - 1$.

$$(1)(x^5 - 1) + (0)(x^7 - 1) = x^5 - 1$$

$$(0)(x^5 - 1) + (1)(x^7 - 1) = x^7 - 1$$

First Loop.

$$x^7 - 1 = (x^2)(x^5 - 1) + (x^2 - 1)$$

New linear equations:

$$(-x^2)(x^5 - 1) + (1)(x^7 - 1) = x^2 - 1$$

$$(1)(x^5 - 1) + (0)(x^7 - 1) = x^5 - 1$$

New $g(x) = x^5 - 1$. New $f(x) = x^2 - 1$.

Second Loop.

$$x^5 - 1 = (x^3 + x)(x^2 - 1) + (x - 1)$$

New linear equations:

$$(x^5 + x^3 + 1)(x^5 - 1) + (-x^3 - x)(x^7 - 1) = x - 1$$

$$(-x^2)(x^5 - 1) + (1)(x^7 - 1) = x^2 - 1$$

Final Loop.

$$x^2 - 1 = (x + 1)(x - 1)$$

STOP. $x - 1$ is returned by the algorithm, with:

$$(x^5 + x^3 + 1)(x^5 - 1) + (-x^3 - x)(x^7 - 1) = x - 1$$

We may continue the analogy:

Definition 7.7. A polynomial $p(x) \in \mathbb{Q}[x]$ of positive degree is **prime** if every divisor of $p(x)$ is either a unit (degree zero) or $p(x)$ times a unit (same degree as $p(x)$).

Examples. (i) Constant polynomials are by definition not prime.

(ii) All linear polynomials are prime. If $p(x)$ is linear and:

$$f(x) \cdot g(x) = p(x)$$

then $\deg(f(x)) + \deg(g(x)) = \deg(p(x)) = 1$, so either $\deg(f(x)) = 0$ and $f(x)$ is a unit or else $\deg(f(x)) = 1$ and $g(x)$ is a unit.

(iii) A quadratic or cubic is prime if and only if it has no linear factors. We'll see that this is the case if and only if it has **no roots.**

(iv) The polynomial:

$$p(x) = x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$$

is not prime and it also has no linear factors.

Factorization. Each $f(x) \in \mathbb{Q}[x]$ is a finite product of primes $p(x)$.

Proof. Consider the set S of **degrees** of non-constant polynomials that are not finite products of primes. Then S is either empty or else S has a smallest element. The smallest element is not 1, since every linear polynomial is prime. Suppose the smallest element of S is n and $f(x)$ is a polynomial of degree n that is not a finite product of primes. Then $f(x)$ is not prime, so it must be a product of two polynomials:

$$g(x)h(x) = f(x)$$

of degrees smaller than n (and adding to n). But then by assumption the degrees of $g(x)$ and $h(x)$ are not in S, so $g(x)$ and $h(x)$ must be finite products of prime polynomials, and we have a contradiction. $\square$

What about Euler's Theorem? This is a little tricky. Notice that there are infinitely many prime polynomials already in degree one, since each of the polynomials:

$$x - r, \quad r \in \mathbb{Q}$$

is prime. Maybe instead we want primes of arbitrarily large degree. In that case we would use the argument from Euler's theorem to take products of primes and add 1:

$$p_1(x) \cdots p_n(x) + 1$$

to get a new polynomial. But unfortunately, this polynomial might factor as a product of linear polynomials, and deny us any new primes. We will see later, however, that the polynomials:

$$x^{p-1} + x^{p-2} + \cdots + 1$$

are always prime whenever p is a prime number!

We do have:

Unique Factorization. The prime factorization of $f(x)$ is unique up to reordering the primes and multiplying each by a unit.

Example.

$$x^2 + 3x + 2 = (x + 1)(x + 2) = \left(\frac{1}{2}x + \frac{1}{2}\right)(2x + 4)$$

Finally, we can define the **field of rational functions** as the set of equivalence classes of polynomial fractions:

$$\frac{f(x)}{g(x)}$$

where $(f(x)), g(x)) \in \mathbb{Q}[x] \times \mathbb{Q}[x]$ is an ordered pair of polynomials, and $g(x)$ is not the zero polynomial. Then we **define**

$$\frac{f_1(x)}{g_1(x)} \sim \frac{f_2(x)}{g_2(x)} \quad \text{if} \quad f_1(x)g_2(x) = f_2(x)g_1(x)$$

and check by hand that this is an equivalence relation (in the case of integer fractions, this was done for us via the partition of $U \subset \mathbb{Z} \times \mathbb{Z}$).

Proposition 6.2 in this setting gives well-defined operations:

$$\left[\frac{f_1(x)}{g_1(x)}\right] + \left[\frac{f_2(x)}{g_2(x)}\right] = \left[\frac{f_1(x)g_2(x) + f_2(x)g_1(x)}{g_1(x)g_2(x)}\right]$$

and

$$\left[\frac{f_1(x)}{g_1(x)}\right] \cdot \left[\frac{f_2(x)}{g_2(x)}\right] = \left[\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}\right]$$

(we will suppress the brackets from now on).

The set of equivalence classes of such fractions with this arithmetic is the **field of rational functions** (with rational coefficients), written:

$$\mathbb{Q}(x)$$

Notice also that elements of $\mathbb{Q}(x)$ can be chosen in lowest terms, in which $f(x)$ and $g(x)$ share no common prime factors. If the leading coefficient of $g(x)$ is chosen to be 1, then this is uniquely determined.

The inductively-minded reader may observe that we took a field, made polynomials with coefficients in that field to create a commutative ring analogous to the integers, in which unique factorization held, and then took fractions of such polynomials to create a new field. This process could be iterated to produce more and more fields:

$$\mathbb{Q}, \mathbb{Q}(x), \mathbb{Q}(x)(y), \mathbb{Q}(x)(y)(z), \ldots$$

We will not pursue this particular string of fields beyond $\mathbb{Q}(x)$, though we will apply this process to other fields.

Exercises. 8.1. Multiply the following polynomials:

(a) $(x^2 + mx + 1)(x^2 - mx + 1)$

(b) $(x^n + x^{n-1} + \cdots + 1)(x - 1)$

(c) $(x^{2n} - x^{2n-1} + \cdots + 1)(x + 1)$

8.2. Use Euclid's algorithm to find a gcd $h(x)$ of:

$$x^5 + x^2 - x + 1 \text{ and } x^8 - 1$$

and solve the equation:

$$a(x)(x^5 + x^2 - x + 1) + b(x)(x^8 - 1) = h(x)$$

by using Euclid's algorithm with extras.

8.3. Show that a quadratic polynomial:

$$ax^2 + bx + c, \quad a, b, c \in \mathbb{Z}$$

is prime if and only if:

$$b^2 - 4ac$$

fails to have a rational square root.

8.4. Prove Unique Factorization into Prime Polynomials.