Math 2070 Week 7

Polynomials, Rings

7.1 Polynomials with Rational Coefficients

Notation:

$$\begin{aligned}\mathbb{Q} &= \text{Set of rational numbers}\\ \mathbb{Q}[x] &= \text{Set of polynomials with rational coefficients}\\ &= \{a_0 + a_1 x + \cdots + a_n x^n | n \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{Q}\}\end{aligned}$$

Theorem 7.1 (Division Theorem for Polynomials with Rational Coefficients)**.** *For all $f, g \in \mathbb{Q}[x]$, such that $f \neq 0$, there exist unique $q, r \in \mathbb{Q}[x]$, satisfying $\deg r < \deg f$, such that $g = fq + r$.*

Proof. We first prove the existence of q and r, via induction on the degree of g. The base step corresponds to the case $\deg g < \deg f$. In this case, the choice $q = 0$, $r = g$ works, since $g = f \cdot 0 + g$, and $\deg r = \deg g < \deg f$.

Now, we establish the inductive step. Let f be fixed. Given g, suppose for all g' with $\deg g' < \deg g$, there exist $q', r' \in \mathbb{Q}[x]$ such that $g' = fq' + r'$, with $\deg r' < \deg f$. We want to show that there exist q, r such that $g = fq + r$, with $\deg r < \deg f$.

Suppose $g = a_0 + a_1 x + \cdots + a_m x^m$ and $f = b_0 + b_1 x + \cdots + b_n x^n$, where $a_m, b_n \neq 0$. We may assume that $m \geq n$, since the case $m < n$ (i.e. $\deg g < \deg f$) has already been proved.

Consider the polynomial:

$$g' = g - \frac{a_m}{b_n} x^{m-n} f.$$

Then, $\deg g' < \deg g$, and by the induction hypothesis we have:

$$g' = fq' + r'$$

for some $q', r' \in \mathbb{Q}[x]$ such that $\deg r' < \deg f$.

Hence,

$$g - \frac{a_m}{b_n} x^{m-n} f = g' = fq' + r',$$

which implies that:

$$g = f\left(q' + \frac{a_m}{b_n} x^{m-n}\right) + r'$$

This establishes the existence of the quotient $q = q' + \frac{a_m}{b_n} x^{m-n}$ and the remainder $r = r'$.

Now, we prove the uniqueness of q and r. Suppose $g = fq + r = fq' + r'$, where $q, q', r, r' \in \mathbb{Q}[x]$, with $\deg r, \deg r' < \deg f$. We have:

$$fq + r = fq' + r',$$

which implies that:

$$\deg f(q - q') = \deg(r' - r) < \deg f.$$

The above inequality can hold only if $q = q'$, which in turn implies that $r' = r$. It follows that the quotient q and the remainder r are unique. $\square$

Definition 7.2. Given $f, g \in \mathbb{Q}[x]$, a **Greatest Common Divisor** d of f and g is a polynomial in $\mathbb{Q}[x]$ which satisfies the following two properties:

1. d divides both f and g.
2. For any $e \in \mathbb{Q}[x]$ which divides both f and g, we have $\deg e \leq \deg d$.

Claim 7.3. *If $g = fq + r$, and d is a GCD of g and f, then d is a GCD of f and r.*

Proof. See the proof of Lemma 6.2 . $\square$

Corollary 7.4. *The Euclidean Algorithm applies to $\mathbb{Q}[x]$.*

Namely: Suppose $\deg g \geq \deg f$. let $g_0 = g$, $f_0 = f$, and let r_0 be the unique polynomial in $\mathbb{Q}[x]$ such that:

$$g_0 = f_0 q_0 + r_0, \quad \deg r_0 < \deg f_0,$$

for some $q_0 \in \mathbb{Q}[x]$.

For $k > 0$, let:

$$g_k = f_{k-1}, \quad f_k = r_{k-1}.$$

Let r_k be the remainder such that:

$$g_k = f_k q_k + r_k,$$

for some $q_k \in \mathbb{Q}[x]$.

Since $\deg r_k < \deg f_k = \deg r_{k-1}$, *we have:*

$$\deg r_0 > \deg r_1 > \deg r_2 > \cdots \geq 0 \geq -\infty$$

(where by convention we let $\deg 0 = -\infty$*).*

Eventually, $r_n = 0$ *for some* n*, and it follows from the previous claim and arguments similar to those used in the case of* $\mathbb{Z}$ *that* r_{n-1} *is a GCD of* f *and* g*.*

Example 7.5. 1. Find a GCD of $x^5 + 1$ and $x^3 + 1$ in $\mathbb{Q}[x]$.

$$\begin{aligned} x^5 + 1 &= \left(x^3 + 1\right)\left(x^2\right) + \left(-x^2 + 1\right) \\ x^3 + 1 &= \left(-x^2 + 1\right)(-x) + (x + 1) \\ -x^2 + 1 &= (x + 1)(-x + 1) + (0) \end{aligned}$$

So, a GCD is $x + 1$.

2. Find a GCD of $x^3 - x^2 - x + 1$ and $x^3 + 4x^2 + x - 6$ in $\mathbb{Q}[x]$.

$$\begin{aligned} x^3 - x^2 - x + 1 &= \left(x^3 + 4x^2 + x - 6\right)(1) + \left(-5x^2 - 2x + 7\right) \\ x^3 + 4x^2 + x - 6 &= \left(-5x^2 - 2x + 7\right)\left(-\frac{1}{5}x - \frac{18}{25}\right) + \left(\frac{24}{25}x - \frac{24}{25}\right) \\ -5x^2 - 2x + 7 &= \left(\frac{24}{25}x - \frac{24}{25}\right)\left(-\frac{125}{24}x - \frac{175}{24}\right) + (0) \end{aligned}$$

So, a GCD is $\frac{24}{25}x - \frac{24}{25}$, and so is $x - 1$.

Corollary 7.6 (Bézout's Identity for Polynomials)**.** *For any* $f, g \in \mathbb{Q}[x]$ *which are not both zero, and* d *a GCD of* f *and* g*, there exist* $u, v \in \mathbb{Q}[x]$ *such that:*

$$d = fu + gv.$$

Example 7.7. In , we have:

$$\begin{aligned} (x + 1) &= \left(x^3 + 1\right) - \left(-x^2 + 1\right)(-x) \\ &= \left(x^3 + 1\right) - \left(\left(x^5 + 1\right) - \left(x^3 + 1\right)\left(x^2\right)\right)(-x) \\ &= \Big(x\Big)\Big(x^5 + 1\Big) + \Big(-x^3 + 1\Big)\Big(x^3 + 1\Big) \end{aligned}$$

7.2 Factorization of Polynomials

Definition 7.8. A polynomial p in $\mathbb{Q}[x]$ is **irreducible** if it satisfies the following conditions:

1. $\deg p > 0$,
2. if $p = ab$ for some $a, b \in \mathbb{Q}[x]$, then either a or b is a constant.

Claim 7.9. *If $p \in \mathbb{Q}[x]$ is irreducible and $p|f_1f_2$, where $f_1, f_2 \in \mathbb{Q}[x]$, then $p|f_1$ or $p|f_2$.*

Proof. Suppose p does not divide f_2, then the only common divisors of p and f_2 are constant polynomials. In particular, 1 is a GCD of p and f_2. Then, by , there exist $u, v, \mathbb{Q}[x]$ such that $1 = pu + f_2v$. We have:

$$f_1 = puf_1 + f_1f_2v.$$

Since p divides the right-hand side of the above equation, it must divide f_1. □

Theorem 7.10. *A polynomial in $\mathbb{Q}[x]$ of degree greater than zero is either irreducible or a product of irreducibles.*

Proof. Suppose there is a nonempty set of polynomials of degree > 0 which are neither irreducible nor products of irreducibles. Let p be an element of this set which has the least degree. Since p is not irreducible, there are $a, b \in \mathbb{Q}[x]$ of degrees > 0 such that $p = ab$. But, a, b, having degrees strictly less than $\deg p$, must be either irreducible or products of irreducibles. This implies that p is a product of irreducibles, a contradiction. □

Remark: Compare this proof with that of Part 1 of the Fundamental Theorem of Arithmetic (Theorem 6.14 (The Fundamental Theorem of Arithmetic)).

Theorem 7.11 (Unique Factorization for Polynomials)**.** *For any $p \in \mathbb{Q}[x]$ of degree > 0, if:*

$$p = f_1f_2 \cdots f_n = g_1g_2 \cdots g_m,$$

where f_i, g_j are irreducible polynomials in $\mathbb{Q}[x]$, then $n = m$, and the g_j's may be reindexed so that $f_i = \lambda_i g_i$ for some $\lambda_i \in \mathbb{Q}$, for $i = 1, 2, \ldots, n$.

Proof. **Exercise** . See the proof of Part 2 of Theorem 6.14 (The Fundamental Theorem of Arithmetic)). □

7.3 Rings

7.3.1 Definition of a Ring

Definition 7.12. A **ring** R (or $(R, +, \times)$) is a set equipped with two operations:

$$\times, + : R \times R \to R$$

which satisfy the following properties:

1. Properties of $+$:
   (a) Commutativity: $a + b = b + a$, $\forall a, b \in R$.
   (b) Associativity: $a + (b + c) = (a + b) + c$.
   (c) There is an element $0 \in R$ (called the **additive identity element**), such that $a + 0 = a$ for all $a \in R$.
   (d) Every element of R has an additive inverse; namely: For all $a \in R$, there exists an element of R, usually denoted $-a$, such that $a+(-a) = 0$.
2. Properties of $\times$:
   (a) Associativity: $a(bc) = (ab)c$.
   (b) There is an element $1 \in R$ (called the **multiplicative identity element**), such that $1 \times a = a \times 1 = a$ for all $a \in R$.
3. Distributativity:
   (a) $a \times (b + c) = a \times b + a \times c$, for all $a, b, c \in R$.
   (b) $(a + b) \times c = a \times c + b \times c$, for all $a, b, c \in R$.

Note:

1. For convenience's sake, we often write ab for $a \times b$.
2. In the definition, commutativity is required of addition, but not of multiplication.
3. Every element has an additive inverse, but *not necessarily* a multiplicative inverse. That is, there may be an element $a \in R$ such that $ab \neq 1$ for all $b \in R$.

Example 7.13. The following sets, equipped with the usual operations of addition and multiplication, are rings:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

2. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ (Polynomials with integer, rational, real coefficients, respectively.)

3. $$\begin{aligned}\mathbb{Q}[\sqrt{2}] &= \{\sum_{k=0}^{n} a_k(\sqrt{2})^k \mid a_k \in \mathbb{Q}, n \in \mathbb{Z}_{\geq 0}\} \\ &= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.\end{aligned}$$

4. $M_n(\mathbb{R})$, the set of $n \times n$ real matrices, $n \in \mathbb{N}$.

5. For a fixed n, the set of $n \times n$ matrices with integer coefficients.

6. $C[0,1] = \{f : [0,1] \to \mathbb{R} \mid f$ is continuous.$\}$

The following sets, under the usual operations of addition and multiplication, are not rings:

1. $\mathbb{N}$, no additive identity element, i.e. no 0.

2. $\mathbb{N} \cup \{0\}$, nonzero elements have no additive inverses.

3. $\mathrm{GL}(n, \mathbb{R})$, the set of $n \times n$ invertible real matrices, $n \in \mathbb{N}$.

Claim 7.14. *In a ring R, there is a unique additive identity element and a unique multiplicative identity element.*

Proof. Suppose there is an element $0' \in R$ such that $0' + r = r$ for all $r \in R$, then in particular $0' + 0 = 0$.

Since 0 is an additive identity, we have $0' + 0 = 0'$. So, $0' = 0$.
Suppose there is an element $1' \in R$ such that $1'r = r$ or all $r \in R$,
then in particular $1' \cdot 1 = 1$.
But $1' \cdot 1 = 1'$ since 1 is a multiplicative identity element, so $1' = 1$. $\square$

Exercise 7.15. Prove that: For any r in a ring R, its additive inverse $-r$ is unique. That is, if $r + r' = r + r'' = 0$, then $r' = r''$.

7.3.2 WeBWorK

1. **WeBWorK**
2. **WeBWorK**

Claim 7.16. *For all elements r in a ring R, we have $0r = r0 = 0$.*

Proof. By distributativity,

$$0r = (0 + 0)r = 0r + 0r.$$

Adding $-0r$ (additive inverse of $0r$) to both sides, we have:

$$0 = (0r + 0r) + (-0r) = 0r + (0r + (-0r)) = 0r + 0 = 0r.$$

The proof of $r0 = 0$ is similar and we leave it as an **exercise** . □

Claim 7.17. *For all elements r in a ring, we have $(-1)(-r) = (-r)(-1) = r$.*

Proof. We have:

$$0 = 0(-r) = (1 + (-1))(-r) = -r + (-1)(-r).$$

Adding r to both sides, we obtain

$$r = r + (-r + (-1)(-r)) = (r + -r) + (-1)(-r) = (-1)(-r).$$

We leave it as an **exercise** to show that $(-r)(-1) = r$. □

Exercise 7.18. Show that: For all r in a ring R, we have:

$$(-1)r = r(-1) = -r.$$

Exercise 7.19. Show that: If R is a ring in which $1 = 0$, then $R = \{0\}$. That is, it has only one element.

(We call such an R the **zero ring** .)