Math 2070 Week 11

Quotient Rings, Polynomials over a Field

11.1 Quotient Rings - continued

Example 11.1. *Let m be a natural number. Consider the map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ defined by:*

$$\phi(n) = n_m, \quad \forall\, n \in \mathbb{Z},$$

where n_m is the remainder of the division of n by m.

Exercise: *ϕ is a homomorphism.*

It is clear that ϕ is surjective, and that $\ker \phi = m\mathbb{Z}$. So, it follows from the First Isomorphism Theorem that:

$$\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}.$$

Definition 11.2 (Gaussian Integers)**.** *Let:*

$$\mathbb{Z}[i] = \{z \in \mathbb{C} : z = a + bi \textit{ for some } a, b \in \mathbb{Z}\},$$

where $i = \sqrt{-1}$.

Exercise 11.3. *Show that the set $\mathbb{Z}[i]$ is a ring under the usual addition $+$ and multiplication $\times$ operations on $\mathbb{C}$.*

Moreover, we have $0_{\mathbb{Z}[i]} = 0$, $1_{\mathbb{Z}[i]} = 1$, and:

$$-(a + bi) = (-a) + (-b)i$$

for any $a, b \in \mathbb{Z}$.

Example 11.4. *The ring $\mathbb{Z}[i]/(1 + 3i)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.*

Proof. Define a map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}[i]/(1+3i)$ as follows:

$$\phi(n) = \overline{n}, \quad \forall\, n \in \mathbb{Z},$$

where $\overline{n}$ is the residue of $n \in \mathbb{Z}[i]$ modulo $(1+3i)$.

It is clear that ϕ is a homomorphism (**Exercise**).

Observe that in $\mathbb{Z}[i]$, we have:

$$1 + 3i \equiv 0 \mod (1+3i),$$

which implies that:

$$\begin{aligned} 1 &\equiv -3i \mod (1+3i) \\ i \cdot 1 &\equiv i \cdot (-3i) \mod (1+3i) \\ i &\equiv 3 \mod (1+3i). \end{aligned}$$

Hence, for all $a, b \in \mathbb{Z}$,

$$\overline{a+bi} = \overline{a+3b} = \phi(a+3b)$$

in $\mathbb{Z}[i]/(1+3i)$. Hence, ϕ is surjective.

Suppose n is an element of $\mathbb{Z}$ such that $\phi(n) = \overline{n} = 0$. Then, by the definition of the quotient ring we have:

$$n \in (1+3i).$$

This means that there exist $a, b \in \mathbb{Z}$ such that:

$$n = (a+bi)(1+3i) = (a-3b) + (3a+b)i,$$

which implies that $3a + b = 0$, or equivalently, $b = -3a$. Hence:

$$n = a - 3b = a - 3(-3a) = 10a,$$

which implies that $\ker\phi \subseteq 10\mathbb{Z}$. Conversely, for all $m \in \mathbb{Z}$, we have:

$$\phi(10m) = \overline{10m} = \overline{(1+3i)(1-3i)m} = 0$$

in $\mathbb{Z}[i]/(1+3i)$.

This shows that $10\mathbb{Z} \subseteq \ker\phi$. Hence, $\ker\phi = 10\mathbb{Z}$.

It now follows from the First Isomorphism Theorem that:

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}[i]/(1+3i).$$

$\square$

11.2 Polynomials over a Field

Let k be a field. For $f \in k[x]$ and $a \in k$, let:

$$f(a) = \phi_a(f),$$

where ϕ_a is the **evaluation homomorphism** defined in Example 9.5. That is:

$$\phi_a\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} c_i a^i.$$

Definition 11.5. *Let $f = \sum_{i=0}^{n} c_i x^i$ be a polynomial in $k[x]$. An element $a \in k$ is a* **root** *of f if:*

$$f(a) = 0$$

in k.

Lemma 11.6. *For all $f \in k[x]$, $a \in k$, there exists $q \in k[x]$ such that:*

$$f = q(x-a) + f(a)$$

Proof. By the Division Theorem for Polynomials with Unit Leading Coefficients, there exist $q, r \in k[x]$ such that:

$$f = q(x-a) + r, \quad \deg r < \deg(x-a) = 1.$$

This implies that r is a constant polynomial.

Applying the evaluation homomorphism ϕ_a to both sides of the above equation, we have:

$$\begin{aligned} f(a) &= \phi_a(q(x-a) + r) \\ &= \phi_a(q) \cdot \phi_a(x-a) + \phi_a(r) \\ &= q(a)(a-a) + r \\ &= r. \end{aligned}$$

□

Claim 11.7 (Root Theorem)**.** *Let k be a field, f a polynomial in $k[x]$. Then, $a \in k$ is a root of f if and only if $(x-a)$ divides f in $k[x]$.*

Proof. If $a \in k$ is a root of f, then by the previous lemma there exists $q \in k[x]$ such that:

$$f = q(x-a) + \underbrace{f(a)}_{=0} = q(x-a),$$

so $(x-a)$ divides f in $k[x]$.

Conversely, if $f = q(x-a)$ for some $q \in k[x]$, then $f(a) = q(a)(a-a) = 0$. Hence, a is a root of f. □

Theorem 11.8. *Let k be a field, f a nonzero polynomial in $k[x]$.*

1. *If f has degree n, then it has at most n roots in k.*
2. *If f has degree $n > 0$ and $a_1, a_2, \ldots, a_n \in k$ are distinct roots of f, then:*

$$f = c \cdot \Pi_{i=1}^{n}(x - a_i) := c(x - a_1)(x - a_2) \cdots (x - a_n)$$

for some $c \in k$.

Proof. 1. We prove Part 1 of the claim by induction. If f has degree 0, then f is a nonzero constant, which implies that it has no roots. So, in this case the claim holds.

Let f be a polynomial with degree $n > 0$. Suppose the claim holds for all nonzero polynomials with degrees strictly less than n. We want to show that the claim also holds for f. If f has no roots in k, then the claim holds for f since $0 < n$. If f has a root $a \in k$, then by the previous claim there exists $q \in k[x]$ such that:

$$f = q(x - a).$$

For any other root $b \in k$ of f which is different from a, we have:

$$0 = f(b) = q(b)(b - a).$$

Since k is a field, it has no zero divisors; so, it follows from $b - a \neq 0$ that $q(b) = 0$. In other words, b is a root of q. Since $\deg q < n$, by the induction hypothesis q has at most $n - 1$ roots. So, f has at most $n - 1$ roots different from a. This shows that f has at most n roots.

---

2. Let f be a polynomial in $k[x]$ which has $n = \deg f$ distinct roots $a_1, a_2, \ldots, a_n \in k$.

If $n = 1$, then $f = c_0 + c_1 x$ for some $c_i \in k$, with $c_1 \neq 0$. We have:

$$0 = f(a_1) = c_0 + c_1 a_1,$$

which implies that: $c_0 = -c_1 a_1$. Hence,

$$f = -c_1 a_1 + c_1 x = c_1(x - a_1).$$

Suppose $n > 1$. Suppose for all $n' \in \mathbb{N}$, such that $1 \leq n' < n$, the claim holds for any polynomial of degree n' which has n' distinct roots in k. By the previous claim, there exists $q \in k[x]$ such that:

$$f = q(x - a_n).$$

Note that $\deg q = n - 1$.

For $1 \le i < n$, we have

$$0 = f(a_i) = q(a_i)\underbrace{(a_i - a_n)}_{\neq 0}.$$

Since k is a field, this implies that $q(a_i) = 0$ for $1 \le i < n$. So, $a_1, a_2, \ldots, a_{n-1}$ are $n-1$ distinct roots of q. By the induction hypothesis there exists $c \in k$ such that:

$$q = c(x - a_1)(x - a_2)\cdots(x - a_{n-1}).$$

Hence, $f = q(x - a_n) = c(x - a_1)(x - a_2)\cdots(x - a_{n-1})(x - a_n)$.

$\square$

Corollary 11.9. *Let k be a field. Let f, g be nonzero polynomials in $k[x]$. Let $n = \max\{\deg f, \deg g\}$. If $f(a) = g(a)$ for $n+1$ distinct $a \in k$. Then, $f = g$.*

Proof. Let $h = f - g$, then $\deg h \le n$. By hypothesis, there are $n+1$ distinct elements $a \in k$ such that $h(a) = f(a) - g(a) = 0$. If $h \neq 0$, then it is a nonzero polynomial with degree $\le n$ which has $n+1$ distinct roots, which contradicts the previous theorem. Hence, h must necessarily be the zero polynomial, which implies that $f = g$. $\square$

Definition 11.10. *A polynomial in $k[x]$ is called a* **monic polynomial** *if its leading coefficient is* 1.

Corollary 11.11. *Let k be a field. Let f, g be nonzero polynomials in $k[x]$. There exists a unique monic polynomial $d \in k[x]$ with the following property:*

1. $(f, g) = (d)$

   Moreover, this d also satisfies the following properties:

2. *d divides both f and g, i.e., there exists $a, b \in k[x]$ such that $f = ad$, $g = bd$.*

3. *There are polynomials $p, q \in k[x]$ such that $d = pf + qg$.*

4. *If $h \in k[x]$ is a divisor of f and g, then h divides d.*

Terminology.

- The unique monic $d \in k[x]$ which satisfies property 1 is called the **Greatest Common Divisor** (*abbrev.* **GCD**) of f and g.

- We say that f and g are **relatively prime** if their GCD is 1.

Proof. 1. By Theorem 10.18 , there exists $d = \sum_{i=0}^{n} a_i x^i \in k[x]$ such that $(d) = (f, g)$. Replacing d by $a_n^{-1} d$ if necessary, we may assume that d is a monic polynomial. It remains to show that d is unique.

Suppose $(d) = (d')$, where both d and d' are monic polynomials. Then, there exist nonzero $p, q \in k[x]$ such that:

$$d' = pd, \quad d = qd'.$$

Examining the degrees of the polynomials, we have:

$$\deg d' = \deg d + \deg p,$$

and:

$$\deg d = \deg q + \deg d' = \deg p + \deg q + \deg d.$$

This implies that $\deg p + \deg q = 0$. Hence, p and q must both have degree 0; in other words, they are constant polynomials. Moreover, we have $\deg d = \deg d'$. Comparing the leading coefficients of d' and pd, we have $p = 1$. Hence, $d = d'$.

2. Clear.

3. Clear.

4. By Part 3 of the corollary, there are $p, q \in k[x]$ such that $d = pf + qg$. It is then clear that if h divides both f and g, then h must divide d.

$\square$

Definition 11.12. *Let R be a commutative ring. A nonzero element $p \in R$ which is not a unit is said to be* **irreducible** *if $p = ab$ implies that either a or b is a unit.*

Example 11.13. *The set of irreducible elements in the ring $\mathbb{Z}$ is $\{\pm p : p \text{ a prime number}\}$.*

Let k be a field.

Lemma 11.14. *A polynomial $f \in k[x]$ is a unit if and only if it is a nonzero constant polynomial.*

Proof. **Exercise.** $\square$

Claim 11.15. *A nonzero nonconstant polynomial $p \in k[x]$ is irreducible if and only if there is no $f, g \in k[x]$, with $\deg f, \deg g < \deg p$, such that $fg = p$.*

Proof. Suppose p is irreducible, and $p = fg$ for some $f, g \in k[x]$ such that $\deg f, \deg g < \deg p$. Then $p = fg$ implies that $\deg f$ and $\deg g$ are both positive. By the previous lemma, both f and g are non-units, which is a contradiction, since the irreducibility of p implies that either f or g must be a unit.

Conversely, suppose p is a nonzero non-unit in $k[x]$, which is not equal to fg for any $f, g \in k[x]$ with $\deg f, \deg g < \deg p$. Then, $p = ab$, a, $b \in k[x]$, implies that either a or b must have the same degree as p, and the other factor must be a nonzero constant, in other words a unit in $k[x]$. Hence, p is irreducible. □

Lemma 11.16 (Euclid's Lemma)**.** *Let k be a field. Let f, g be polynomials in $k[x]$. Let p be an irreducible polynomial in $k[x]$. If $p|fg$ in $k[x]$, then $p|f$ or $p|g$.*

Proof. Suppose $p \nmid f$. Then, any common divisor of p and f must have degree strictly less than $\deg p$. Since p is irreducible, this implies that any common divisor of p and f is a nonzero constant. Hence, the GCD of p and f is 1. By Corollary 11.11 , there exist $a, b \in k[x]$ such that:

$$ap + bf = 1.$$

Multiplying both sides of the above equation by g, we have:

$$apg + bfg = g.$$

Since p divides the left-hand side of the above equation, it must also divide the right-hand side, which is the polynomial g. □

Claim 11.17. *If $f, g \in k[x]$ are relatively prime, and both divide $h \in k[x]$, then $fg|h$.*

Proof. **Exercise.** □

Theorem 11.18 (Unique Factorization)**.** *Let k be a field. Every nonconstant polynomial $f \in k[x]$ may be written as:*

$$f = cp_1 \cdots p_n,$$

where c is a nonzero constant, and each p_i is a monic irreducible polynomial in $k[x]$. The factorization is unique up to the ordering of the factors.

Proof. **Exercise.** One possible approach is very similar to the proof of unique factorization for $\mathbb{Z}$. See: The Fundamental Theorem of Arithmetic . □

Exercise 11.19. *1.* **WeBWorK**

Theorem 11.20. *Let k be a field. Let p be a polynomial in $k[x]$. The following statements are equivalent:*

1. *$k[x]/(p)$ is a field.*
2. *$k[x]/(p)$ is an integral domain.*
3. *p is irreducible in $k[x]$.*

Remark. *Compare this result with Exercise 8.11 and Corollary 8.16 .*

Proof.

1. $1 \Rightarrow 2$: Clear, since every field is an integral domain.
2. $2 \Rightarrow 3$: If p is not irreducible, there exist $f, g \in k[x]$, with degrees strictly less than that of p, such that $p = fg$. Since $\deg f, \deg g < \deg p$, the polynomial p does not divide f or g in $k[x]$. Consequently, the congruence classes $\overline{f}$ and $\overline{g}$ of f and g, respectively, modulo (p) is not equal to zero in $k[x]/(p)$. On the other hand, $\overline{f} \cdot \overline{g} = \overline{fg} = \overline{p} = 0$ in $k[x]/(p)$. This implies that $k[x]/(p)$ is not an integral domain, a contradiction. Hence, p is irreducible if $k[x]/(p)$ is an integral domain.
3. $3 \Rightarrow 1$: By definition, the multiplicative identity element 1 of a field is different from the additive identity element 0. So we need to check that the congruence class of $1 \in k[x]$ in $k[x]/(p)$ is not 0. Since p is irreducible, by definition we have $\deg p > 0$. Hence, $1 \notin (p)$, for a polynomial of degree > 0 cannot divide a polynomial of degree 0 in $k[x]$. We conclude that $1 + (p) \neq 0 + (p)$ in $k[x]/(p)$.

   Next, we need to prove the existence of the multiplicative inverse of any nonzero element in $k[x]/(p)$. Given any $f \in k[x]$ whose congruence class $\overline{f}$ modulo (p) is nonzero in $k[x]/(p)$, we want to find its multiplicative inverse $\overline{f}^{-1}$. If $\overline{f} \neq 0$ in $k[x]/(p)$, then by definition $f - 0 \notin (p)$, which means that p does not divide f. Since p is irreducible, this implies that $GCD(p, f) = 1$. By Corollary 11.11 there exist $g, h \in k[x]$ such that $fg + hp = 1$. It is then clear that $\overline{g} = \overline{f}^{-1}$, since $fg - 1 = -hp$ implies that $fg - 1 \in (p)$, which by definition means that $\overline{f} \cdot \overline{g} = \overline{fg} = 1$ in $k[x]/(p)$.

□

Example 11.21. *The rings $\mathbb{R}[x]/(x^2 + 1)$ and $\mathbb{C}$ are isomorphic.*

Proof. Define a map $\phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ as follows:

$$\phi(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} a_k i^k.$$

Exercise: ϕ is a homomorphism.

For all $a + bi$ ($a, b \in \mathbb{R}$) in $\mathbb{C}$, we have:

$$\phi(a + bx) = a + bi.$$

Hence, ϕ is surjective.

We now find $\ker \phi$. Since $\mathbb{R}[x]$ is a PID (see Definition 10.15). There exists $p \in \mathbb{R}[x]$ such that $\ker \phi = (p)$.

Observe that $\phi(x^2 + 1) = 0$. So, $x^2 + 1 \in \ker \phi$, which implies that there exists $q \in \mathbb{R}[x]$ such that $x^2 + 1 = pq$. Since $x^2 + 1$ has no real roots, neither p or q can be of degree 1.

So, one of p or q must be a nonzero constant polynomial. p cannot be a nonzero constant polynomial, for that would imply that $\ker \phi = \mathbb{R}[x]$. So, q is a constant, which implies that $p = q^{-1}(x^2 + 1)$. We conclude that $\ker \phi = (x^2 + 1)$.

It now follows from the First Isomorphism Theorem that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. $\square$