Math 110A Running Notes

Brendan Connelly

January to March 2025

Chapter 1: Integer Arithmetic

Definition (Division Algorithm)**.** Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist unique integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

Existence Sketch: We can set $q = \left\lfloor \frac{a}{b} \right\rfloor$ (the floor of a/b), and then define $r = a - bq$. One checks that $0 \leq r < b$.
Uniqueness Sketch: If there were two representations

$$a \;=\; bq_1 + r_1 \;=\; bq_2 + r_2 \quad \text{with} \quad 0 \leq r_1, r_2 < b,$$

then subtracting them gives $b(q_1 - q_2) = r_2 - r_1$. Since $|r_2 - r_1| < b$, the only way $b \mid (r_2 - r_1)$ is if $r_2 = r_1$ and hence $q_1 = q_2$.

Definition (Well-Ordering Property of $\mathbb{N}$)**.** The Well-Ordering Principle states that every non-empty subset of $\mathbb{N}$ has a least element.

Definition (Greatest Common Divisor (gcd))**.** Let a and b be integers, not both 0. The *greatest common divisor (gcd)* of a and b is the largest integer d that divides both a and b. In other words, d is the gcd of a and b provided that:

1. $d \mid a$ and $d \mid b$;
2. if $c \mid a$ and $c \mid b$, then $c \leq d$.

The greatest common divisor of a and b is usually denoted (a, b).

Theorem (Theorem 1.2)**.** Let a and b be integers, not both 0, and let d be their greatest common divisor. Then there exist (not necessarily unique) integers u and v such that

$$d = au + bv.$$

Corollary (Corollary 1.3)**.** Let a and b be integers, not both 0, and let d be a positive integer. Then d is the greatest common divisor of a and b if and only if d satisfies these conditions:

1. $d \mid a$ and $d \mid b$;
2. if $c \mid a$ and $c \mid b$, then $c \mid d$.

Theorem (Theorem 1.4)**.** If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Proof. Since $(a, b) = 1$, Theorem 1.2 shows that $au + bv = 1$ for some integers u and v. Multiplying this equation by c shows that

$$acu + bcv = c.$$

But $a \mid bc$, so that $bc = ar$ for some r. Therefore,

$$c = acu + bcv = acu + (ar)v = a(cu + rv).$$

The first and last parts of this equation show that $a \mid c$. □

Definition (Prime Integer)**.** An integer p is said to be prime if $p \neq 0, \pm 1$ and the only divisors of p are ± 1 and $\pm p$.

Theorem (Theorem 1.5)**.** Let p be an integer with $p \neq 0, \pm 1$. Then p is prime if and only if p has this property:

$$\text{whenever } p \mid bc, \text{ then } p \mid b \text{ or } p \mid c.$$

Corollary (Corollary 1.6)**.** If p is prime and $p \mid a_1 a_2 \cdots a_n$, then p divides at least one of the a_i.

Proof. If $p \mid a_1(a_2 a_3 \cdots a_n)$, then $p \mid a_1$ or $p \mid a_2 a_3 \cdots a_n$ by Theorem 1.5. If $p \mid a_1$, we are finished. If $p \mid a_2(a_3 a_4 \cdots a_n)$, then $p \mid a_2$ or $p \mid a_3 a_4 \cdots a_n$ by Theorem 1.5 again. If $p \mid a_2$, we are finished; if not, continue this process, using Theorem 1.5 repeatedly. After at most n steps, there must be an a_i that is divisible by p. □

Theorem (The Fundamental Theorem of Arithmetic)**.** Every integer n except $0, \pm 1$ is a product of primes. This prime factorization is unique in the following sense:

If

$$n = p_1 p_2 \cdots p_r \quad \text{and} \quad n = q_1 q_2 \cdots q_s,$$

with each p_i, q_j prime, then $r = s$ (that is, the number of factors is the same) and after reordering and relabeling the q_j's,

$$p_1 = \pm q_1, \quad p_2 = \pm q_2, \quad \ldots, \quad p_r = \pm q_r.$$

Corollary (Corollary 1.9)**.** Every integer $n > 1$ can be written in one and only one way in the form

$$n = p_1 p_2 p_3 \cdots p_r,$$

where the p_i are positive primes such that

$$p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_r.$$

Theorem (Theorem 1.10)**.** Let $n > 1$. If n has no positive prime factor less than or equal to $\sqrt{n}$, then n is prime.

Chapter 2: Modular Arithmetic

Definition (Modular Congruence Classes)**.** Let a and n be integers with $n > 0$. The **congruence class** of a modulo n (denoted $[a]$) is the set of all those integers that are congruent to a modulo n, that is,

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}.$$

Definition (Modular Equivalence)**.** Let a, b, n be integers with $n > 0$. Then a is **congruent** to b modulo n (written $a \equiv b \pmod{n}$) provided that n divides $a - b$.

Theorem (2.1)**.** Let n be a positive integer. For all $a, b, c \in \mathbb{Z}$:

1. $a \equiv a \pmod{n}$;
2. if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
3. if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Theorem (2.2)**.** If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

1. $a + c \equiv b + d \pmod{n}$;
2. $ac \equiv bd \pmod{n}$.

Theorem (Theorem 2.3)**.** $a \equiv c \pmod{n}$ if and only if $[a] = [c]$.

Corollary (Corollary 2.4)**.** Two congruence classes modulo n are either disjoint or identical.

Corollary (Corollary 2.5)**.** Let $n > 1$ be an integer and consider congruence modulo n.

1. If a is any integer and r is the remainder when a is divided by n, then $[a] = [r]$.
2. There are exactly n distinct congruence classes, namely, $[0], [1], [2], \ldots, [n-1]$.

Theorem (Theorem 2.8)**.** If $p > 1$ is an integer, then the following conditions are equivalent:

1. p is prime.
2. For any $a \neq 0$ in $\mathbb{Z}_p$, the equation $ax = 1$ has a solution in $\mathbb{Z}_p$.
3. Whenever $bc = 0$ in $\mathbb{Z}_p$, then $b = 0$ or $c = 0$.

1 Chapter 3: Rings

Definition (Ring)**.** A *ring* is a nonempty set R equipped with two operations (usually written as addition and multiplication) that satisfy the following axioms. For all $a, b, c \in R$:

1. $a + b \in R$ [Closure for addition]
2. $a + (b + c) = (a + b) + c$ [Associative addition]
3. $a + b = b + a$ [Commutative addition]
4. There exists an element $0_R \in R$ such that $a + 0_R = a = 0_R + a$ for every $a \in R$. [Additive identity or zero element]
5. For each $a \in R$, the equation $a + x = 0_R$ has a solution in R. [Additive inverse]
6. $a \cdot b \in R$ [Closure for multiplication]
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ [Associative multiplication]
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$. [Distributive laws]

Definition (Commutative Ring)**.** A *commutative ring* is a ring R that satisfies the additional axiom:

(9) $a \cdot b = b \cdot a$ for all $a, b \in R$. [Commutative multiplication]

Definition (Ring with Identity)**.** A *ring with identity* is a ring R that contains an element 1_R satisfying the additional axiom:

(10) $a \cdot 1_R = a = 1_R \cdot a$ for all $a \in R$. [Multiplicative identity]

Definition (Integral Domain)**.** An *integral domain* is a commutative ring R with identity $1_R \neq 0_R$ that satisfies the additional axiom:

(11) Whenever $a, b \in R$ and $a \cdot b = 0_R$, then $a = 0_R$ or $b = 0_R$. [Zero-product property]

Definition (Field)**.** A *field* is a commutative ring R with identity $1_R \neq 0_R$ that satisfies the additional axiom:

(12) For each $a \neq 0_R$ in R, the equation $a \cdot x = 1_R$ has a solution in R. [Multiplicative inverses]

Theorem (Cartesian Product of Rings)**.** Let R and S be rings. Define addition and multiplication on the Cartesian product $R \times S$ by

$$(r, s) + (r', s') = (r + r', s + s') \quad \text{and} \quad (r, s)(r', s') = (rr', ss').$$

Then $R \times S$ is a ring. If R and S are both commutative, then so is $R \times S$. If both R and S have an identity, then so does $R \times S$.

Theorem (Subring Criterion)**.** Suppose that R is a ring and that S is a subset of R such that

1. S is closed under addition (if $a, b \in S$, then $a + b \in S$);

2. S is closed under multiplication (if $a, b \in S$, then $ab \in S$);
3. $0_R \in S$;
4. If $a \in S$, then the solution of the equation $a + x = 0_R$ is in S.

Then S is a subring of R.

Theorem (Subrings of $\mathbb{Z}/n\mathbb{Z}$)**.** The number of subrings of the ring $\mathbb{Z}/n\mathbb{Z}$ is equal to the number of positive divisors of n.

Theorem (Properties of Ring Homomorphisms)**.** Let $f : R \to S$ be a ring homomorphism. Then:

1. $f(0_R) = 0$,
2. $f(-a) = -f(a)$ for all $a \in R$,
3. $f(a - b) = f(a) - f(b)$ for all $a, b \in R$.

If R has a multiplicative identity 1_R and f is surjective, then:

4. S has a multiplicative identity 1_S and $f(1_R) = 1_S$,
5. If u is a unit in R, then $f(u)$ is a unit in S and $f(u^{-1}) = f(u)^{-1}$.

Proof.

1. $f(0_R) = 0$**:** Since f is a homomorphism, we have:
$$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R).$$
Subtract $f(0_R)$ from both sides to get $f(0_R) = 0$.
2. $f(-a) = -f(a)$**:** By definition, $-f(a)$ is the unique element such that:
$$f(a) + (-f(a)) = 0.$$
We need to show $f(-a) + f(a) = 0$:
$$f(-a + a) = f(0_R) = 0 \implies f(-a) + f(a) = 0.$$
Thus, $f(-a) = -f(a)$.
3. $f(a - b) = f(a) - f(b)$**:** Using $f(a - b) = f(a + (-b))$, we have:
$$f(a - b) = f(a) + f(-b) = f(a) - f(b).$$
4. S **has a multiplicative identity:** Since f is surjective, any $a \in S$ can be written as $f(b)$ for some $b \in R$. We need to show $f(1_R)a = a$ for all $a \in S$:
$$f(1_R)a = f(1_R)f(b) = f(1_R b) = f(b) = a.$$
Hence, $f(1_R) = 1_S$ is the multiplicative identity of S.
5. $f(u)$ **is a unit in** S**:** Let u be a unit in R with $u^{-1} \in R$ such that $uu^{-1} = 1_R$. Then:
$$f(u)f(u^{-1}) = f(uu^{-1}) = f(1_R) = 1_S.$$
Thus, $f(u)$ is a unit in S with $f(u^{-1}) = f(u)^{-1}$.

$\square$

2 Chapter 4: Polynomials

Definition (Extension Ring Construction)**.** Let R be a ring. Then there exists a ring T containing an element $x \notin R$ such that:

1. R is a subring of T.
2. $xa = ax$ for every $a \in R$.
3. The set $R[x]$ of all elements of T of the form
$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$
where $n \geq 0$ and $a_i \in R$, is a subring of T that contains R.
4. The representation of elements of $R[x]$ is unique: If
$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m,$$
where $n \neq m$, then $a_i = b_i$ for $i = 0, 1, \ldots, \min(n, m)$ and $b_i = 0$ for each $i > n$.
5. $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$ in $R[x]$ if and only if $a_i = 0$ for every i.

Theorem (Degree of a Product of Polynomials)**.** Let R be an integral domain, and let $f(x), g(x)$ be nonzero polynomials in $R[x]$. Then:
$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x).$$

Proof. Suppose
$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{and} \quad g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m,$$
where $a_n \neq 0_R$ and $b_m \neq 0_R$, so that $\deg f(x) = n$ and $\deg g(x) = m$. Then:
$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots + a_nb_mx^{n+m}.$$
The largest exponent of x that can possibly have a nonzero coefficient is $n+m$. Since $a_n \neq 0_R$ and $b_m \neq 0_R$, their product $a_nb_m \neq 0_R$ because R is an integral domain. Therefore, $f(x)g(x)$ is nonzero, and:
$$\deg[f(x)g(x)] = n + m = \deg f(x) + \deg g(x).$$
□

Theorem. If R is an integral domain, then so is $R[x]$.

Proof. Since R is a commutative ring with identity, so is $R[x]$ (by Exercises 7 and 8). The proof of Theorem 4.2 shows that the product of nonzero polynomials in $R[x]$ is nonzero. Therefore, $R[x]$ is an integral domain. □

Corollary. Let R be a commutative ring (not necessarily an integral domain). If $f(x), g(x) \in R[x]$ are nonzero and $f(x)g(x) \neq 0$, then in general we *cannot* guarantee $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$. Indeed, zero divisors in R can cause the leading term to vanish, so that
$$\deg(f(x)g(x)) < \deg(f(x)) + \deg(g(x)).$$

Corollary. Let R be an integral domain and $f(x) \in R[x]$. Then $f(x)$ is a unit in $R[x]$ if and only if $f(x)$ is a constant polynomial that is a unit in R.

In particular, if F is a field, the units in $F[x]$ are the nonzero constants in F.

Theorem (Division Algorithm in $F[x]$, 4.6)**.** Let F be a field and let $f, g \in F[x]$ with $g \neq 0$. Then there exist unique polynomials q, r such that

$$f = gq + r,$$

where either $r = 0$ or $\deg(r) < \deg(g)$.

Theorem (4.7)**.** Let F be a field and let $a(x), b(x) \in F[x]$ with $b(x) \neq 0$.

1. If $b(x)$ divides $a(x)$, then $cb(x)$ divides $a(x)$ for each nonzero $c \in F$.
2. Every divisor of $a(x)$ has degree less than or equal to $\deg a(x)$.

Definition (Greatest Common Factor)**.** Let F be a field, and let $a(x), b(x) \in F[x]$, not both zero. The **greatest common divisor (gcd)** of $a(x)$ and $b(x)$ is the monic polynomial of highest degree that divides both $a(x)$ and $b(x)$.

In other words, $d(x)$ is the gcd of $a(x)$ and $b(x)$ provided that $d(x)$ is monic and satisfies the following conditions:

1. $d(x)$ divides both $a(x)$ and $b(x)$, i.e., $d(x) \mid a(x)$ and $d(x) \mid b(x)$.
2. If $c(x)$ divides both $a(x)$ and $b(x)$, then $\deg c(x) \leq \deg d(x)$.

Theorem (4.8, Bezout's for Polynomials)**.** Let F be a field, and let $a(x), b(x) \in F[x]$, not both zero. Then there is a unique greatest common divisor $d(x)$ of $a(x)$ and $b(x)$. Furthermore, there exist (not necessarily unique) polynomials $u(x)$ and $v(x)$ such that

$$d(x) = a(x)u(x) + b(x)v(x).$$

Corollary (4.9)**.** Let F be a field, and let $a(x), b(x) \in F[x]$, not both zero. A monic polynomial $d(x) \in F[x]$ is the greatest common divisor of $a(x)$ and $b(x)$ if and only if $d(x)$ satisfies the following conditions:

(i) $d(x)$ divides $a(x)$ and $b(x)$.

(ii) If $c(x)$ divides both $a(x)$ and $b(x)$, then $c(x)$ also divides $d(x)$.

Definition (Relatively prime)**.** Polynomials $f(x)$ and $g(x)$ are said to be **relatively prime** if their greatest common divisor is 1.

Theorem (4.10)**.** Let F be a field, and let $a(x), b(x), c(x) \in F[x]$. If $a(x)$ divides $b(x)c(x)$ and $a(x)$ and $b(x)$ are relatively prime, then $a(x)$ divides $c(x)$.

Definition (Associates)**.** Let F be a field. A polynomial $f(x)$ is an **associate** of $g(x)$ in $F[x]$ if and only if

$$f(x) = cg(x)$$

for some nonzero $c \in F$.

Definition (Associates in a Ring)**.** Let R be a commutative ring with unity. Two elements a and b in R are said to be **associates** if there exists a unit $u \in R$ such that

$$a = ub.$$

We write $a \sim b$ to denote that a and b are associates.

Definition (Irreducible polynomial)**.** Let F be a field. A nonconstant polynomial $p(x) \in F[x]$ is said to be **irreducible** if its only divisors are its associates and the nonzero constant polynomials (units).

A nonconstant polynomial that is not irreducible is said to be extbfreducible.

Theorem (Reducibility Criterion 4.11)**.** Let F be a field. A nonzero polynomial $f(x)$ is reducible in $F[x]$ if and only if $f(x)$ can be written as the product of two polynomials of lower degree.

Theorem (Irreducibility Conditions 4.12)**.** Let F be a field and $p(x)$ a nonconstant polynomial in $F[x]$. Then the following conditions are equivalent:

1. $p(x)$ is irreducible.
2. If $b(x)$ and $c(x)$ are any polynomials such that $p(x) \mid b(x)c(x)$, then $p(x) \mid b(x)$ or $p(x) \mid c(x)$.
3. If $r(x)$ and $s(x)$ are any polynomials such that $p(x) = r(x)s(x)$, then either $r(x)$ or $s(x)$ is a nonzero constant polynomial.

Corollary (Divisibility Property of Irreducible Polynomials 4.13)**.** Let F be a field and $p(x)$ an irreducible polynomial in $F[x]$. If $p(x)$ divides the product $a_1(x)a_2(x)\ldots a_n(x)$, then $p(x)$ divides at least one of the $a_i(x)$.

Theorem (Unique Factorization of Polynomials 4.14)**.** Let F be a field. Every nonconstant polynomial $f(x)$ in $F[x]$ is a product of irreducible polynomials in $F[x]$. This factorization is unique in the following sense: If

$$f(x) = p_1(x)p_2(x)\cdots p_r(x)$$

and

$$f(x) = q_1(x)q_2(x)\cdots q_s(x),$$

where each $p_i(x)$ and $q_j(x)$ are irreducible in $F[x]$, then $r = s$ and there exists a permutation σ of $\{1, 2, \ldots, r\}$ such that

$$p_i(x) \text{ and } q_{\sigma(i)}(x) \text{ are associates for all } i.$$

Definition (Roots of a Polynomial)**.** Let R be a commutative ring and $f(x) \in R[x]$. An element a of R is said to be a **root** (or **zero**) of the polynomial $f(x)$ if $f(a) = 0_R$, that is, if the induced function $f : R \to R$ maps a to 0_R.

Theorem (Remainder Theorem 4.15)**.** Let F be a field, $f(x) \in F[x]$, and $a \in F$. The remainder when $f(x)$ is divided by the polynomial $x - a$ is $f(a)$.

By the Division Algorithm, we can write:

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

where the remainder $r(x)$ either is 0_F or has smaller degree than the divisor $x - a$. Thus, $\deg r(x) = 0$ or $r(x) = 0_F$. In either case, $r(x) = c$ for some $c \in F$. Hence,

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

so that evaluating at a gives:

$$f(a) = (a - a)q(a) + c = 0_F + c = c.$$

Theorem (Factor Theorem 4.16)**.** Let F be a field, $f(x) \in F[x]$, and $a \in F$. Then a is a root of the polynomial $f(x)$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.

Proof: First, assume that a is a root of $f(x)$. Then we have:

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

by the Division Algorithm. By the Remainder Theorem, this simplifies to:

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

Since a is a root of $f(x)$, we know $f(a) = 0_F$. Thus,

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

which shows that $x - a$ is a factor of $f(x)$.

Conversely, assume that $x - a$ is a factor of $f(x)$. That is, suppose:

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

Evaluating at $x = a$ gives:

$$f(a) = (a - a)g(a) = 0_F g(a) = 0.$$

Hence, a is a root of $f(x)$.

Corollary (Bound on Roots of a Polynomial 4.17)**.** Let F be a field and let $f(x)$ be a nonzero polynomial of degree n in $F[x]$. Then $f(x)$ has at most n roots in F.

Corollary (Irreducible Polynomials Have No Roots 4.18)**.** Let F be a field and let $f(x) \in F[x]$ with $\deg f(x) \geq 2$. If $f(x)$ is irreducible in $F[x]$, then $f(x)$ has no roots in F.

Corollary (4.19)**.** Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree 2 or 3. Then $f(x)$ is irreducible in $F[x]$ if and only if $f(x)$ has no roots in F.

Corollary (4.20)**.** Let F be an infinite field and let $f(x), g(x) \in F[x]$. Then $f(x)$ and $g(x)$ induce the same function from F to F if and only if $f(x) = g(x)$ in $F[x]$.

Theorem (Rational Root Test 4.21)**.** Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be a polynomial with integer coefficients. If $r \neq 0$ and the rational number r/s (in lowest terms) is a root of $f(x)$, then $r \mid a_0$ and $s \mid a_n$.

Lemma (4.22)**.** Let $f(x), g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$. If p is a prime that divides every coefficient of $f(x)$, then either p divides every coefficient of $g(x)$ or p divides every coefficient of $h(x)$.

Theorem (Integral Factorization Theorem 4.23)**.** Let $f(x)$ be a polynomial with integer coefficients. Then $f(x)$ factors as a product of polynomials of degrees m and n in $\mathbb{Q}[x]$ if and only if $f(x)$ factors as a product of polynomials of degrees m and n in $\mathbb{Z}[x]$.

Theorem (Eisenstein's Criterion 4.24)**.** Let

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

be a nonconstant polynomial with integer coefficients. If there is a prime p such that p divides each of $a_0, a_1, \ldots, a_{n-1}$ but p does not divide a_n and p^2 does not divide a_0, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Theorem (Irreducibility Modulo p Implies Irreducibility Over $\mathbb{Q}$ 4.25)**.** Let

$$f(x) = a_k x^k + \cdots + a_1 x + a_0$$

be a polynomial with integer coefficients, and let p be a positive prime that does not divide a_k. If $f(x)$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: Suppose, on the contrary, that $f(x)$ is reducible in $\mathbb{Q}[x]$. Then by Theorem 4.23, we can write:

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

where $g(x), h(x)$ are nonconstant polynomials in $\mathbb{Z}[x]$. Since p does not divide a_k, the leading coefficient of $f(x)$, it cannot divide the leading coefficients of $g(x)$ or $h(x)$ (whose product is a_k). Consequently,

$$\deg g(x) = \deg g(x) \quad \text{and} \quad \deg h(x) = \deg h(x).$$

In particular, neither $g(x)$ nor $h(x)$ is a constant polynomial in $\mathbb{Z}_p[x]$.

Verify that $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$ implies that $f(x) = g(x)h(x)$ in $\mathbb{Z}_p[x]$ (Exercise 20). This contradicts the irreducibility of $f(x)$ in $\mathbb{Z}_p[x]$. Therefore, $f(x)$ must be irreducible in $\mathbb{Q}[x]$.

Theorem (Fundamental Theorem of Algebra 4.26)**.** Every nonconstant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

Corollary (4.27)**.** A polynomial is irreducible in $\mathbb{C}[x]$ if and only if it has degree 1.

Corollary (4.28)**.** Every nonconstant polynomial $f(x)$ of degree n in $\mathbb{C}[x]$ can be written in the form

$$c(x - a_1)(x - a_2)\cdots(x - a_n)$$

for some $c, a_1, a_2, \ldots, a_n \in \mathbb{C}$. This factorization is unique except for the order of the factors.

Lemma (4.29)**.** If $f(x)$ is a polynomial in $\mathbb{R}[x]$ and $a+bi$ is a root of $f(x)$ in $\mathbb{C}$, then $a-bi$ is also a root of $f(x)$.

Theorem (4.30, Irreducibility in $\mathbb{R}[x]$)**.** A polynomial $f(x)$ is irreducible in $\mathbb{R}[x]$ if and only if $f(x)$ is a first-degree polynomial or
$$f(x) = ax^2 + bx + c \quad \text{with} \quad b^2 - 4ac < 0.$$

Proof: The proof that the polynomials described in the theorem are irreducible is left as Exercise 7.

Conversely, suppose $f(x)$ has degree at least 2 and is irreducible in $\mathbb{R}[x]$. Then by Theorem 4.26, $f(x)$ has a root ω in $\mathbb{C}$. Since $f(x)$ has real coefficients, its roots must occur in conjugate pairs, meaning $\overline{\omega}$ is also a root. Moreover, ω cannot be real, as that would imply $f(x)$ has a linear factor in $\mathbb{R}[x]$, contradicting irreducibility. Thus, $\omega \neq \overline{\omega}$.

By the Factor Theorem, $(x-\omega)$ and $(x-\overline{\omega})$ are factors of $f(x)$ in $\mathbb{C}[x]$, so we can write:
$$f(x) = (x-\omega)(x-\overline{\omega})h(x)$$
for some $h(x) \in \mathbb{C}[x]$. Now define:
$$g(x) = (x-\omega)(x-\overline{\omega}) = (x-(r+si))(x-(r-si)) = x^2 - 2rx + (r^2+s^2).$$
The coefficients of $g(x)$ are real numbers, meaning $g(x) \in \mathbb{R}[x]$.

By the Division Algorithm in $\mathbb{R}[x]$, there exist polynomials $q(x), r(x) \in \mathbb{R}[x]$ such that:
$$f(x) = g(x)q(x) + r(x), \quad \text{where } r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)).$$
However, since we already have $f(x) = g(x)h(x)$ in $\mathbb{C}[x]$, the uniqueness of the quotient and remainder in the Division Algorithm implies that $q(x) = h(x)$ and $r(x) = 0$. Thus, $h(x) \in \mathbb{R}[x]$.

Since $f(x) = g(x)h(x)$ and $f(x)$ is irreducible in $\mathbb{R}[x]$, it must be that $h(x)$ is a constant $d \in \mathbb{R}$. Therefore,
$$f(x) = dg(x),$$
meaning $f(x)$ is a quadratic polynomial of the form ax^2+bx+c for some $a,b,c \in \mathbb{R}$. Finally, since $f(x)$ has no real roots, the quadratic formula implies that its discriminant satisfies $b^2 - 4ac < 0$.

---

3 Chapter 5: Congruence in $F[x]$ and Congruence Class Arithmetic

Definition (Polynomial Congruence Modulo $p(x)$)**.** Let F be a field and let $f(x), g(x), p(x) \in F[x]$ with $p(x)$ nonzero. Then $f(x)$ is **congruent** to $g(x)$ modulo $p(x)$ (written $f(x) \equiv g(x) \pmod{p(x)}$) provided that $p(x)$ divides $f(x) - g(x)$, that is,
$$p(x) \mid (f(x) - g(x)).$$

Theorem (Theorem 5.1)**.** Let F be a field and let $p(x)$ be a nonzero polynomial in $F[x]$. Then the relation of congruence modulo $p(x)$ satisfies the following properties:

1. **Reflexivity:** $f(x) \equiv f(x) \pmod{p(x)}$ for all $f(x) \in F[x]$.
2. **Symmetry:** If $f(x) \equiv g(x) \pmod{p(x)}$, then $g(x) \equiv f(x) \pmod{p(x)}$.

3. **Transitivity:** If $f(x) \equiv g(x) \pmod{p(x)}$ and $g(x) \equiv h(x) \pmod{p(x)}$, then $f(x) \equiv h(x) \pmod{p(x)}$.

Theorem (Theorem 5.2)**.** Let F be a field and let $p(x)$ be a nonzero polynomial in $F[x]$. If $f(x) \equiv g(x) \pmod{p(x)}$ and $h(x) \equiv k(x) \pmod{p(x)}$, then:

1. $f(x) + h(x) \equiv g(x) + k(x) \pmod{p(x)}$.
2. $f(x)h(x) \equiv g(x)k(x) \pmod{p(x)}$.

Definition (Congruence Class of a Polynomial)**.** Let F be a field and let $f(x), p(x) \in F[x]$ with $p(x)$ nonzero. The **congruence class** (or **residue class**) of $f(x)$ modulo $p(x)$, denoted $[f(x)]$, is the set of all polynomials in $F[x]$ that are congruent to $f(x)$ modulo $p(x)$, that is,

$$[f(x)] = \{g(x) \in F[x] \mid g(x) \equiv f(x) \pmod{p(x)}\}.$$

Theorem (Theorem 5.3)**.** $f(x) \equiv g(x) \pmod{p(x)}$ if and only if $[f(x)] = [g(x)]$.

Corollary (Corollary 5.4)**.** Two congruence classes modulo $p(x)$ are either disjoint or identical.

Corollary (Corollary 5.5)**.** Let F be a field and let $p(x)$ be a polynomial of degree n in $F[x]$, and consider congruence modulo $p(x)$.

1. If $f(x) \in F[x]$ and $r(x)$ is the remainder when $f(x)$ is divided by $p(x)$, then $[f(x)] = [r(x)]$.
2. Let S be the set consisting of the zero polynomial and all the polynomials of degree less than n in $F[x]$. Then every congruence class modulo $p(x)$ is the class of some polynomial in S, and the congruence classes of different polynomials in S are distinct.

Theorem (Theorem 5.6)**.** Let F be a field and let $p(x)$ be a nonconstant polynomial in $F[x]$. If $[f(x)] = [g(x)]$ and $[h(x)] = [k(x)]$ in $F[x]/(p(x))$, then:

1. $[f(x) + h(x)] = [g(x) + k(x)]$.
2. $[f(x)h(x)] = [g(x)k(x)]$.

Theorem (Theorem 5.7)**.** Let F be a field and let $p(x)$ be a nonconstant polynomial in $F[x]$. Then the set $F[x]/(p(x))$ of congruence classes modulo $p(x)$ is a commutative ring with identity. Furthermore, $F[x]/(p(x))$ contains a subring F^* that is isomorphic to F.

Theorem (Theorem 5.8)**.** Let F be a field and let $p(x)$ be a nonconstant polynomial in $F[x]$. Then $F[x]/(p(x))$ is a commutative ring with identity that contains F.

Theorem (Theorem 5.9)**.** Let F be a field and let $p(x)$ be a nonconstant polynomial in $F[x]$. If $f(x) \in F[x]$ and $f(x)$ is relatively prime to $p(x)$, then $[f(x)]$ is a unit in $F[x]/(p(x))$.

Proof. By Theorem 4.8, there exist polynomials $u(x)$ and $v(x)$ such that

$$f(x)u(x) + p(x)v(x) = 1.$$

Rearranging, we get:

$$f(x)u(x) - 1 = -p(x)v(x) = p(x)(-v(x)),$$

which implies that

$$[f(x)u(x)] = [1]$$

by Theorem 5.3. Therefore,

$$[f(x)][u(x)] = [f(x)u(x)] = [1],$$

so that $[f(x)]$ is a unit in $F[x]/(p(x))$. □

Theorem (Theorem 5.10)**.** Let F be a field and let $p(x)$ be a nonconstant polynomial in $F[x]$. Then the following statements are equivalent:

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

Theorem (Theorem 5.11)**.** Let F be a field and let $p(x)$ be an irreducible polynomial in $F[x]$. Then $F[x]/(p(x))$ is an extension field of F that contains a root of $p(x)$.

Corollary (Corollary 5.12)**.** Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field K of F that contains a root of $f(x)$.

4 Chapter 6: Ideals and Quotient Rings

Definition (Ideal)**.** A subring I of a ring R is an **ideal** if, whenever $r \in R$ and $a \in I$, then:

$$ra \in I \quad \text{and} \quad ar \in I.$$

Theorem (Theorem 6.1)**.** A nonempty subset I of a ring R is an ideal if and only if it satisfies the following properties:

1. If $a, b \in I$, then $a - b \in I$.
2. If $r \in R$ and $a \in I$, then $ra \in I$ and $ar \in I$.

Proof. Every ideal certainly satisfies these two properties.

Conversely, suppose I satisfies properties (i) and (ii). Then I absorbs products by (ii), so we need only verify that I is a subring. Property (i) states that I is closed under subtraction. Since I is a subset of R, the product of any two elements of I must be in I by (ii). In other words, I is closed under multiplication. Therefore, I is a subring of R by Theorem 3.6. □

Theorem (Theorem 6.2)**.** Let R be a commutative ring with identity, let $c \in R$, and let I be the set of all multiples of c in R, that is,

$$I = \{rc \mid r \in R\}.$$

Then I is an ideal of R.

The ideal I in Theorem 6.2 is called the **principal ideal** generated by c and is denoted by (c). In the ring $\mathbb{Z}$, for example, (3) indicates the ideal of all multiples of 3.

In any commutative ring R with identity, the principal ideal (1_R) is the entire ring R because $r = r1_R$ for every $r \in R$.

It can be shown that every ideal in $\mathbb{Z}$ is a principal ideal (Exercise 40). However, there exist ideals in other rings that are not principal, meaning they do not consist of all the multiples of a particular element of the ring.

Theorem (Theorem 6.3)**.** Let R be a commutative ring with identity and let $c_1, c_2, \ldots, c_n \in R$. Then the set

$$I = \{r_1c_1 + r_2c_2 + \cdots + r_nc_n \mid r_1, r_2, \ldots, r_n \in R\}$$

is an ideal in R.

Definition (Congruence Modulo an Ideal)**.** Let I be an ideal in a ring R and let $a, b \in R$. Then a is **congruent** to b modulo I (written $a \equiv b \pmod I$) provided that $a - b \in I$.

Theorem (Theorem 6.4)**.** Let I be an ideal in a ring R. Then the relation of congruence modulo I satisfies the following properties:

1. **Reflexivity:** $a \equiv a \pmod I$ for every $a \in R$.
2. **Symmetry:** If $a \equiv b \pmod I$, then $b \equiv a \pmod I$.
3. **Transitivity:** If $a \equiv b \pmod I$ and $b \equiv c \pmod I$, then $a \equiv c \pmod I$.

Theorem (Theorem 6.5)**.** Let I be an ideal in a ring R. If $a \equiv b \pmod I$ and $c \equiv d \pmod I$, then:

1. $a + c \equiv b + d \pmod I$.
2. $ac \equiv bd \pmod I$.

Definition (Congruence class of ideal)**.** $a + I := \{b \in R \mid a \equiv b \mod I\}$.

Theorem (Theorem 6.6)**.** Let I be an ideal in a ring R and let $a, c \in R$. Then

$$a \equiv c \pmod I \quad \text{if and only if} \quad a + I = c + I.$$

Proof. Recall that by definition, $a \equiv c \pmod I$ if and only if $a - c \in I$.

(⇒) Assume $a \equiv c \pmod I$, i.e., $a - c \in I$. Then

$$a = c + (a - c),$$

which shows that $a \in c + I$. Thus, every element of $a + I$ can be written in the form

$$a + i = c + (a - c + i),$$

where $a - c + i \in I$ (since I is an ideal and hence closed under addition). This implies $a + I \subseteq c + I$.

(⇐) Conversely, assume $a + I = c + I$. Since $a \in a + I$, it follows that $a \in c + I$, so there exists some $i \in I$ such that

$$a = c + i.$$

Thus, $a - c = i \in I$, which means $a \equiv c \pmod{I}$.

Since both directions have been established, the equivalence is proved. □

Corollary (Corollary 6.7)**.** Let I be an ideal in a ring R. Then two cosets of I are either disjoint or identical.

Theorem (Theorem 6.8)**.** Let I be an ideal in a ring R. If $a + I = b + I$ and $c + I = d + I$ in R/I, then:

1. $(a + c) + I = (b + d) + I$.
2. $ac + I = bd + I$.

Theorem (Theorem 6.9)**.** Let I be an ideal in a ring R. Then:

1. The quotient R/I is a ring, with addition and multiplication of cosets defined as previously.
2. If R is commutative, then R/I is a commutative ring.
3. If R has an identity, then so does the ring R/I.

Theorem (Theorem 6.10)**.** Let $f : R \to S$ be a homomorphism of rings. Then the kernel $\ker f$ of f is an ideal in the ring R.

Theorem (Theorem 6.11)**.** Let $f : R \to S$ be a homomorphism of rings with kernel K. Then $K = \{0_R\}$ if and only if f is injective.

Theorem (Theorem 6.12)**.** Let I be an ideal in a ring R. Then the map $\pi : R \to R/I$ given by $\pi(r) = r + I$ is a surjective homomorphism with kernel I. The map π is called the *natural homomorphism* from R to R/I.

Theorem (Theorem 6.13 (First Isomorphism Theorem))**.** Let $f : R \to S$ be a surjective homomorphism of rings with kernel K. Then the quotient ring R/K is isomorphic to S, i.e., there exists a ring isomorphism

$$\varphi : R/K \to S$$

such that $\varphi(r + K) = f(r)$ for all $r \in R$.

Definition. An ideal P in a commutative ring R is said to be **prime** if $P \neq R$ and whenever $bc \in P$, then $b \in P$ or $c \in P$.

Theorem (Theorem 6.14)**.** Let P be an ideal in a commutative ring R with identity. Then P is a prime ideal if and only if the quotient ring R/P is an integral domain.

Definition. An ideal M in a ring R is said to be *maximal* if $M \neq R$ and whenever J is an ideal such that $M \subseteq J \subseteq R$, then either $M = J$ or $J = R$.

Equivalently, an ideal M in a ring R is said to be *maximal* if $M \neq R$ and whenever $M \subsetneq J$ is an ideal, then $J = R$.

Theorem (Theorem 6.15)**.** Let M be an ideal in a commutative ring R with identity. Then M is a maximal ideal if and only if the quotient ring R/M is a field.

Theorem (Additional Theorem)**.** Let $n \in \mathbb{N}$ be a positive integer with prime factorization

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Then the ring $\mathbb{Z}_n$ has exactly k maximal ideals, namely

$$(p_1), (p_2), \ldots, (p_k),$$

where for each i,

$$(p_i) = \{\overline{a} \in \mathbb{Z}_n : p_i \text{ divides } a\}.$$

Moreover, the quotient ring $\mathbb{Z}_n/(p_i)$ is isomorphic to the finite field $\mathbb{Z}_{p_i}$ for each i.

Definition (Hilbert's Nullstellensatz for Maximal Ideals)**.** Let $\mathbb{C}$ denote the field of complex numbers and consider the polynomial ring $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then every maximal ideal $\mathfrak{m}$ in $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is of the form

$$\mathfrak{m} = (x_1 - a_1,\, x_2 - a_2,\, \ldots,\, x_n - a_n)$$

for some point $a = (a_1, a_2, \ldots, a_n) \in \mathbb{C}^n$. Conversely, for every point $a \in \mathbb{C}^n$, the ideal

$$(x_1 - a_1,\, x_2 - a_2,\, \ldots,\, x_n - a_n)$$

is maximal in $\mathbb{C}[x_1, x_2, \ldots, x_n]$.